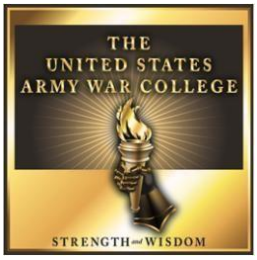
Strategy Research Project

Risky Business: Implementing Risk Management in National Security Decision-making

by

Lieutenant Colonel Ryan McCormack
United States Army

Under the Direction of:
Professor Albert Lord



United States Army War College
Class of 2017

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01-04-2017	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Risky Business: Implementing Risk Management in National Security Decision-making

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Ryan McCormack
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Professor Albert Lord

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT Distribution A: Approved for Public Release. Distribution is Unlimited.
To the best of my knowledge this SRP accurately depicts USG and/or DoD policy & contains no classified information or aggregation of information that poses an operations security risk. **Author:** ☒ **PA:** ☒

13. SUPPLEMENTARY NOTES
Word Count: 7537

14. ABSTRACT
The United States security policy decision-making process crosses multiple constituencies in an environment characterized by ambiguity and complexity. There is no formalized decision-making process that ensures a rigorous interagency outcome-oriented risk assessment when making national security policy and strategy. The process of national security policy decision-making is inherently unstructured and, as a result, introduces risk that if left unmanaged can involve the commitment of vast resources and lead to questionable and often disastrous outcomes. This study attempts to identify and overcome the impediments to decision-making methods that introduce risk and ways to promote outcome-oriented risk management in future national security policy and strategy development.

15. SUBJECT TERMS
National Security Council, Strategic Decision-making

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(w/ area code)*
UU	UU	UU	UU	37	

Risky Business: Implementing Risk Management in National Security Decision-making

(7537 words)

Abstract

The United States security policy decision-making process crosses multiple constituencies in an environment characterized by ambiguity and complexity. There is no formalized decision-making process that ensures a rigorous interagency outcome-oriented risk assessment when making national security policy and strategy. The process of national security policy decision-making is inherently unstructured and, as a result, introduces risk that if left unmanaged can involve the commitment of vast resources and lead to questionable and often disastrous outcomes. This study attempts to identify and overcome the impediments to decision-making methods that introduce risk and ways to promote outcome-oriented risk management in future national security policy and strategy development.

Risky Business: Implementing Risk Management in National Security Decision-making

> The challenge of conceptualizing national security in today's unpredictable world is exacerbated by the contingent nature of many of the most serious problems. Many things that could harm U.S. interests are potential, rather than actual. The risk that they will harm U.S. interests cannot be eliminated, but only managed.
>
> – Project on National Security Reform[1]

Mark Twain once stated, "History does not repeat itself – at best it often rhymes."[2] Throughout history the United States developed policies and subsequent strategies for military conflicts in order to answer challenges to its national security. During these conflicts, the complexity and challenges associated with decision-making across multiple governmental constituencies often occurred without an adequate consideration of the risks associated with strategic decisions. Some argue that the decision-makers were unable to identify, assess, and manage risks introduced by the apparent misalignment of strategic objectives, the methods identified to achieve them, or the resources available to attain strategic success. In this context, risk is the probability and severity of something bad happening that prevents or limits the ability to achieve a strategy. Similarly, risk management is the process of appraising and assuaging the potential negative consequences affecting desired political outcomes.[3]

The concept of *risky business*, the practice of risk management in strategic decision-making, is not new. History is replete with examples in business and government where strategic advisors and decision-makers participate in a "rigorous, disciplined dialogue about the possible implications of various options" before making decisions, and improve the likelihood of achieving acceptable outcomes.[4] What *is* relatively new is the seeming failure of security decision-makers to apply a formal risk management methodology into national policy and strategy development. Additionally,

there appears to be a growing aversion by U.S. Presidents to engage their strategic advisors in detailed discussions of the risks associated with national security strategies, how risks might best be managed, and their consequences for security.

Today's national security leaders must overcome two specific impediments to adopting risk management into strategic-level decision-making. The first impediment is the use of faulty decision-making models that introduce cognitive biases and limit, exclude, or prevent a discussion of the risks associated with achieving strategy outcomes. To overcome this obstacle, the National Security Council (NSC) should adopt a prescriptive decision-making model that reduces bias and defaulting to heuristics when making judgments. Additionally, the process should integrate a risk management methodology that provides the President with a comprehensive risk assessment and related mitigation measures from across the interagency team.

The second impediment is the lack of a comprehensive national-level risk management methodology focusing on desired national security outcomes across all governmental departments. Currently there is no framework or requirement for departments to provide risk management input into national security decision-making. The NSC should implement a risk management methodology that helps security advisors to identify, assess, manage and communicate risk associated with national security policy decisions.

The consideration of risk is perhaps the most important aspect of formulating suitable and attainable national security policy and strategy. The challenge is to openly communicate risks, identify and incorporate mitigation measures to limit potential

consequences, and routinely identify and incorporate normative national security decision-making models used by the NSC.

National Security in a Complex Strategic Environment

Security in the 21st Century is arguably more complex and challenging than any other in history because strategic decisions must be formulated and disseminated in an increasingly rapid manner. Today, threats to security are multi-dimensional and dispersed, affecting domestic politics, external state and non-state actors, technology, interdependence, and globalization. The challenge with the current environment is found in its complexity and dynamic security changes. Moreover, policy makers often do not adapt their national security strategies, policies, or capabilities to deal with the changing security challenges and associated risks. Here lies the true *risky business.*

A recent assessment by the Center for Strategic and International Studies expands the scope of the strategic environment by identifying the main national security, energy, and economic challenges in its annual report. The document identifies three important national security challenges that, if left unaddressed, will threaten the nation's security strategy. The first challenge is the fragile and increasingly contentious US domestic situation with regard to national politics, a stagnant economy, large budget, and increasing debt. The effects of sequestration on defense spending and the reduction of capabilities will also continue to limit US national security objectives. Next, the rise of assertive regional adversaries looking to challenge US primacy and national interests is a significant challenge. Competitors' use of hybrid warfare and "gray zone" activity blur the lines "between defense, diplomacy…between overt activity and espionage; and between security and economics."[5] Finally, the challenges associated with cyber threats, the vulnerability of information, and the speed of which related

security decisions are required in response to stay ahead of the news cycle, and counter disinformation is increasingly problematic.

One of the most comprehensive summaries outlining the future strategic environment is found in a recent Joint Staff publication, *Joint Operating Environment 2035*. This document highlights how the dual aspects of *contested norms* and *persistent disorder* will define the future strategic environment.[6] It contends that the environment and future conflicts will most likely be violent and potentially occur simultaneously in multiple domains. With this as its foundation, future conflict can be summarized across six contexts or trends: a proliferation of violent ideological competition, continued threats to US territory and sovereignty, uncertain geopolitical balancing, disruption within the global commons, and a contested cyberspace.[7] Finally, persistent disorder will yield shattered and reordered regions from cumulative political fractures and environmental challenges.[8] As these trends develop, an effective approach toward managing risk must also evolve to meet the demands of this dynamic security development.

The Chairman of the Joint Chiefs of Staff (CJCS), General Joseph F. Dunford, elaborated on the environment's complexity by identifying the transregional, multi-functional and multi-domain (TMM) aspect of today's threats. The world order will continue to evolve under the pressure of rising powers and TMM threats such as violent extremist organizations, criminal networks, and other non-state actors. This evolution will change current strategic relationships, give rise to new regional powers with global reach, modify the role of existing international institutions, and empower new actors pursuing regional primacy.[9] Collectively, the challenges require near real-time decision-making, further complicating the formulation and implementation of risk management

strategies. Decision-makers must engage this *risky business* head on by considering ways to manage risk as threats and adversaries proliferate.

To be effective in the emerging, complex, and dynamic strategic environment requires the establishment of relatively stable strategic national objectives. *The US National Security Strategy* (NSS) "outlines the major national security concerns of the US and how the administration plans to address them using all the instruments of national power."[10] It provides the broad direction and policy guidance for the government to direct activities supporting national interests and attain strategic aims. Security activities include the use of diplomatic, informational, economic, and military power to protect from harm one's physical, ideological, political, and economic interests, "the loss of which could threaten the fundamental values of the state."[11]

Strategy is widely understood as a function of ends, ways, and means. When these three elements are not aligned, risk is introduced to the equation. Nations must not only have a strategy to be successful in ensuring security, but must have a strategy that is congruent with its security policy objectives and available resources. Nations that align policy objectives and capability ultimately achieve their national aims; those that do not usually fail to achieve their policy goals.

Often at the strategic-level a candid identification, analysis, and discussion of risk is obscured by several dynamics associated with decision-making methods, group dynamics, individual biases, and politics. The success and failure of any strategy is also dependent upon a comparative assessment of associated risk for the viable option. This is normally accomplished by conducting a thorough risk analysis. In order to discuss the ways of overcoming the impacts of faulty decision-making processes through a feasible

risk management process, one must have a firm understanding of risk and the ways it might be managed in the national security arena.

Risk and the Impediments to Proper Risk Management

Defining risk in the national security policy and strategy development process is a significant step toward managing the potential negative outcomes in light of achieving policy objectives. This step is often ignored or avoided because the process to manage or discuss risk is complicated, unstructured, or not integrated into decision-making processes. This introduces the possibility of strategic failure or even worse, national disaster. Michael J. Mazarr reinforces this reality by stating, “The biggest national security disasters and risk calamities often stem from a willful disregard of consequences.”[12] National security strategy-makers often fail to acknowledge the misalignment of ends, ways, and means during the decision-making process as a result of “satisficing” where the decision-makers identify a “good enough solution” that assumes or ignores quantified risk.[13] Satisficing introduces a multitude of decision-making biases and heuristics that can lead to failure, or at worst, an incremental, ad hoc approach toward policymaking at best.

Additionally, there is a growing trend that decision-makers omit the hard discussion of risk in order to move the process along to reach consensus. Often individuals in groups avoid recognizing and discussing risk, insulating themselves from outside advice and counsel because they value their position in the group and do not want to become an outsider.[14]

In today’s strategic environment there are multiple definitions of risk as it pertains to policy and its underlying strategy. Risk may be viewed as the strategic threats to overall policy objectives. It can also be defined as the gaps that develop between

identified policy objectives and the resources allocated to attain the ends.[15] Former Secretary of Defense Donald Rumsfeld identified risk in two famous categories, “known unknowns” and “unknown, unknowns” as a basis for operating in the strategic environment.[16] An expanded definition states, “Risks involve threats to outcomes that we value. Defining risks means specifying those valued outcomes clearly enough to make choices about them.”[17] Making choices is a fundamental component of strategic military risk that includes the probability that a military capability or force is unable to achieve strategic objectives. It is very difficult to eliminate risk; therefore a process to measure and manage it is imperative.

Risk management cannot focus on one dimension but must strike a balance across a range of functions.[18] The multifaceted aspect of the threats and challenges requires risk management to be comprehensive and multidimensional. Additionally, there are many stakeholders within the national security system that have diverse and often conflicting perspectives and interests. It is not uncommon to have multiple departments coming together to identify and overcome many of the TMM threats facing the nation. The challenge lies with the range of sometime disjointed and divergent processes used by multiple national security players. The national security system can overcome these challenges by “creating processes and structures that facilitate this diverse group of players [and] enable government with the capacity to make effective and informed [risk] decisions efficiently.”[19] A comprehensive national-level risk management methodology should begin with a basic risk management framework.

Risk Management Framework

Of all the components of national power – diplomatic, informational, military, and economic – the military has developed the most useful, normalized methodology to

manage risk in the strategic environment. Faced with the realities of increasingly constrained resources and the imperative to maintain capabilities, the military must strike a difficult balance of choices and prioritization to achieve strategic objectives and minimize risk.[20] The recently published CJCS Manual 3105.01, *Joint Risk Analysis,* provides the most in depth and holistic approach to identifying, assessing, and managing strategic risk in our government.

This new document highlights the Joint Risk Analysis Methodology (JRAM), a comprehensive process for appraising and managing risk. It allows the CJCS to give the best military advice to the President, Congress, and Secretary of Defense in the areas of developing, managing, and employing the joint force to attain national security policy and strategy objectives.[21] The JRAM is divided into three fundamental components as part of cycle: risk appraisal, risk management, and risk communication as part of the Joint Risk Framework (Figure 1).

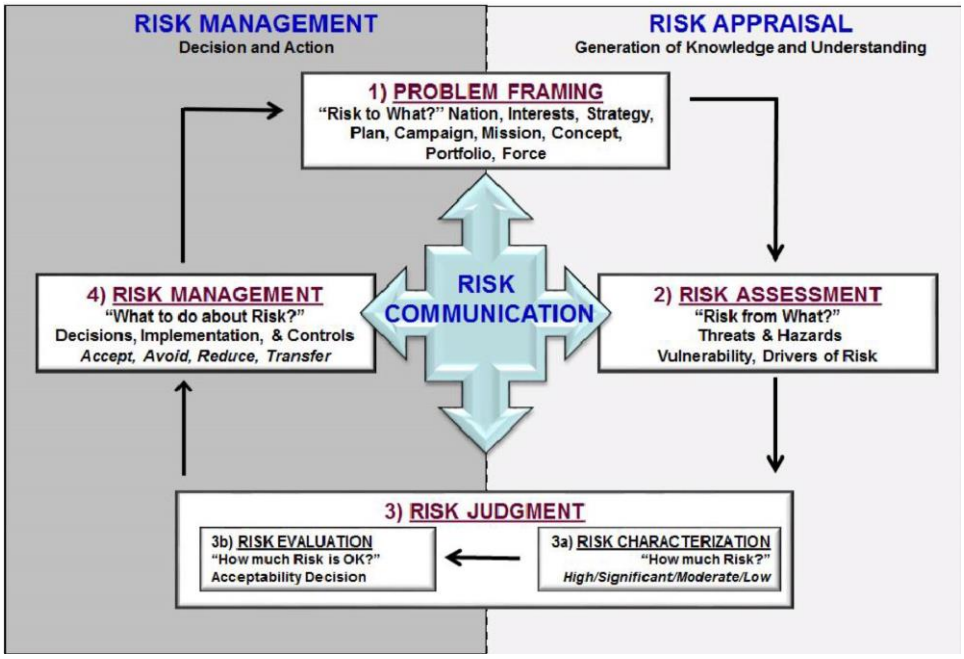


Figure 1. The Joint Risk Framework[22]

The first element of the cycle, risk appraisal, is the development of risk specific knowledge and understanding within the environment. Risk management is the process of making decisions and taking actions to mitigate, avoid, or accept risks based on their impact on desired outcomes. Risk communication is the dialogue that occurs between strategic advisors and decision-makers on risk perspectives and establishes a culture of "risk mindedness" and priorities for objective achievement. As time passes or conditions in the strategic environment change, the risk management cycle continues with another iteration starting with risk appraisal.

Within the cycle there are four steps that include framing the problem, assessing risk, providing a quantitative and qualitative judgment of the risk, and the ability to manage the risk.[23] The *problem-framing* step allows strategic leaders and advisors to better define the risk and answer the question, "What is at risk?" At the national security level, this step references core national interests, national security policies, supporting

security strategy, military strategy, military forces, or mission. This step is the starting point for determining what might be at risk and the implications of adverse actions. For example, as national security leaders look at policies and specific strategies to respond to a security challenge, they begin a detailed analysis of the problem and the environment. Additionally, leaders then define the probability an event might occur, and the consequential impact to the objective.[24]

Risk *assessment*, identifies specific hazards and the overall vulnerabilities associated with threats to the strategic objective. This step answers the question, "What is causing risk in this situation?" Here the process identifies possible threats and hazards that have the potential to cause harm to US interests or policy goals. Also, this step looks to identify any drivers of risk – the "factors that act either to increase or decrease the probability, frequency, or consequence of risk arising."[25] An example of this might be a decrease in capability or limitation in resources due to budget cuts that may increase assessed risk. The critical output of this step is the determination of the expected probability and consequence of an event occurring.

The third step, *risk judgment*, is the process used to determine the national security decision-maker's degree of acceptable risk. To make a risk judgment the leader must first identify the risk level through an assessment of the probability that a negative event may occur and consequence if it actually occurs. The next action is for the leader to make a risk evaluation by determining if the risk is acceptable or unacceptable based on the characterization of risk.[26] The process of risk judgment allows the leader to make a qualitative decision about the acceptability of the risk and provide some initial guidance on how to manage it while moving forward.

During the *risk management* step, the leader creates, applies, and monitors risk decisions by accepting, avoiding, reducing, or transferring risk.[27] Once risk is identified, the national security leader must determine the level of acceptable risk. The acceptable level of risk is the threshold that the leader determines when a risk of failure for an action transitions from acceptable to unacceptable. At the strategic level, the President should articulate this broadly in his strategic guidance during discussions with staff, as the strategy is developed, and as conditions change.

If unacceptable, decision-makers may prescribe mitigation measures that reduce the consequence or probability a negative event will occur, or transfer the risk. The leader may make an informed decision to take action despite being in the “unacceptable zone” as it may yield bigger gains than being avoided altogether. General Martin Dempsey referenced the opportunistic aspect of risk stating, "Probability and consequence are not easily measured, and they do not paint the whole picture. It is just as important to think about how risk changes over time and what opportunities may be available if we accept risk.”[28]

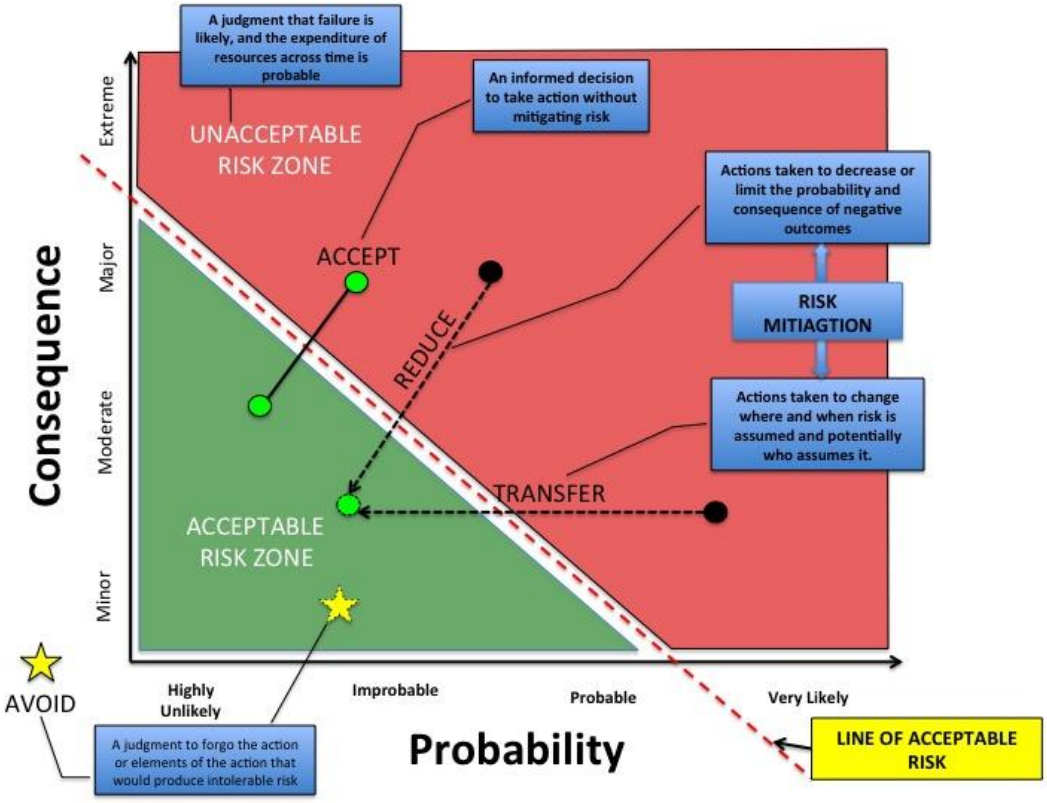


Figure 2. Risk Management Application Graph[29]

The risk communication aspect of the JRAM is arguably the most important because it connects each step of the process, and addresses the outputs of the process that initiate risk dialogue and enable the decision-making process. “Effective communication between risk stakeholders reduces misunderstandings and potential surprise and is critical to enhancing dialogue and creating confidence in outcomes.”[30] The JRAM espouses that effective communication builds on professional trust and is a fundamental aspect of providing the best military advice. Therefore, it is important that risk management outputs be communicated so there is a clear understanding of the threat likelihood and consequence, what could be done to mitigate it, and enable a further discussion among advisors and decision-makers before, during, and after action.

The JRAM is the most comprehensive risk management framework in the national security policy and strategy-making process. It provides a normalized process to manage the multitude of risks encountered in the strategic environment. It could easily be transferred to the many other governmental departments. Additionally, it could be easily integrated into any national security decision-making process and prevent history from rhyming.

History Rhyming

There are two examples in US history that briefly demonstrate how previous Presidents failed to incorporate an assessment and discussion of risk when making national policy and strategy decisions. These examples are demonstrated in President John F. Kennedy's decision to invade Cuba and, similarly, President George W. Bush's decision to invade Iraq.

During the planning and deliberations for the Bay of Pigs invasion of Cuba in 1961, President Kennedy implemented a collegial decision-making process in lieu of a more standardized national security bureaucratic process used by President Eisenhower. In this collegial decision-making process, Kennedy received advice and information from multiple informal channels of competing advisors rather than a single bureaucratic process or organization.[31] This informal process never incorporated a viable discussion of the risk associated with the Cuban invasion, nor did it attempt to include any dissenting opinions on the overall strategy.

Throughout the planning and assessment process there was an "over consensus of 'groupthink'" during the opportunities set aside for deliberations preventing an outcome-oriented assessment of risk.[32] Since an informal group, not a dedicated committee attended all the meetings, there was little coordination or detailed staff work

across the departments to provide assessments of success or the probability and consequence of negative outcomes of the invasion. While Kennedy did ask the Joint Chiefs of Staff (JCS) to conduct a review of the CIA's plan to invade Cuba, the results did not provide any significant assessment of risk.[33] After a limited review due to a lack of plan specifics, the JCS published JCSM-57-61 titled *Military Evaluation of the CIA Paramilitary Plan – Cuba* and found initial success of the invasion was likely. The report stated that there was "a fair chance of ultimate success" and even if it does not, it would contribute to the "eventual overthrow of the Castro regime."[34]

In reality, Kennedy and his advisors never considered any significant details or risks associated with the plan. It appears Kennedy spent more effort in assessing the "possible political consequences of abandoning the invasion plans … [T]hey did not, however, give much weight to the interests and consequences which would be involved if the plan was tried and failed."[35] The JCS gave their assessment with limited availability to the actual details of the CIA plan, and was initiated tacitly under the belief that the President already supported the invasion decision. Thus it did not want or need further analysis. This prompted the National Security Advisor (NSA), McGeorge Bundy, to assert that "those who offer serious advice on major issues must themselves do the necessary work", as a significant decision-making lesson learned from the Bay of Pigs.[36]

The combination of Kennedy's collegial decision-making model and loose organizational structure had an adverse impact on the President's deliberative process. It limited dissent among group members and prevented a holistic assessment of what could go wrong with the Cuban invasion. The failure outlined during the Bay of Pigs

decision process is just one indication that supports a more codified decision-making approach that incorporates risk management.

Likewise in 2003, President Bush and his NSC found themselves in a similar scenario where policy-makers and strategic advisors failed to candidly discuss risk as they examined strategy options for achieving regime change in Iraq. During an interview with Bob Woodward, President Bush explained his perspective on making decisions informed by risk. He stated, “I am the kind of person that wants to make sure that all the risk is assessed. But a president is constantly analyzing, making decisions based upon risk, particularly in war – risk taken relative to what can be achieved.”[37] In contrast to this statement, it appears that President Bush did not actively manage the risks associated with the decision to invade Iraq in 2003. Instead, his overconfidence prevented him from fully assessing the risks associated with the invasion and the requirement for a subsequent stabilization effort.

Similarly, when discussing the plan and strategy for the invasion of Iraq, President Bush never engaged his advisors in any deliberative decision-making process. Richard Haass, the Director for Policy Planning at the Department of State (DOS) recalled that, “there was no meeting or set of meetings at which the pros and cons were debated and a formal decision taken.”[38] At no point did he or his advisors explicitly engage in or discuss risk associated with an invasion or the possibility of a sustained occupation.

In an attempt to identify and assess risk, Donald Rumsfeld identified several “unknown unknowns” in a memo to President Bush in October 2003, some five months before the invasion, called the “Parade of Horribles”. In this memo Rumsfeld confided

that he was, “uneasy that, as a government, we had not yet fully examined a broad enough spectrum of possibilities…there was never a systematic review of my list to the NSC.”[39] Some of the most compelling risk possibilities that remained unmanaged by the NSC were that the US would fail to find WMD, the US could fail to manage a post-Saddam Iraq that would destabilize the region and increase ethnic strife among the Sunnis, Shiites, and Kurds, the post-Saddam efforts could take up to ten years to be successful, and most significantly, the US could lose it stature as a world leader.[40]

Rumsfeld’s “spectrum of possibilities” was essentially a list of unmanaged risk that the NSC failed to address which ultimately led to the catastrophic chaos that extended the war and taking it to the brink of failure. According to Rumsfeld, the other members of the NSC were not prepared to address the risks and Bush refused to discuss anything that detracted from obtaining support for an invasion.[41]

These two examples briefly demonstrate the potential disastrous outcomes when leaders fail to institutionalize strategic-level risk management within their decision-making process. They also provide an opportunity to identify specific impediments in greater detail.

The Impediments to Conducting Risky Business in Security Decision-making

Today’s national security leaders should work to overcome two impediments to inculcating risk management into their strategic-level decision-making processes. The use of faulty decision-making models and the lack of a comprehensive national-level risk management methodology limit the attainment of national security policy objectives.

Faulty Decision-making Model and Processes

Decision-making at the strategic-level is inherently challenging due to the complexity of the environment, and the problems faced are abstract and commonly fail

to have easy solutions. Generally, important national security decisions are non-routine and encompass the integration of the art of leadership and the science of management. Additionally, these types of decisions involve interdependent assessments and actions by a diverse group of stakeholders requiring a broader assessment of the risk.[42] There are two decision-making models commonly used at the presidential-level that tend to introduce bias and prevent the incorporation of risk management and undermine even the most robust attempts to discuss or address risk.[43]

The first decision-making model that limits risk management in decision-making is the intuitive decision-making model. The process of intuitive decision-making involves the ability of an individual to tap into a "reservoir of recognized patterns" based on experience that allow the decision-maker "to go with their gut".[44] It explains how, for relatively simple problems, individuals "can make effective decisions without conducting a deliberate analysis" of the problem, options, or how they lead to achieving an objective.[45] Gary Klein explains, in his summary of the theory, that individuals use a recognition-primed decision process when facing new situations or decisions. Their initial understanding of the situation generates cues that allow the decision-maker to recognize patterns of activity that initiate "action scripts."[46] Klein explains that these action scripts then initiate a process of mental simulation and mental modeling that allows an individual to "know what to expect" before implementing a decision so they know if they are getting the correct results.[47]

This intuitive approach allows the decision-maker to make quick decisions that are generally "good enough". But with more complex, strategic-level decisions, going with "good enough" inevitably introduces significant amounts of risk. If followed blindly,

intuition tends to lead to disastrous results if not balanced with some sort of oversight or assessment process to limit potential negative outcomes. Intuitions are “inherently biased” and introduce unreliable information and thought processes that overlay on top of already complex decisions. This makes the process of intuitive decision-making itself unreliable and risky. Therefore one could make the argument, “we shouldn’t simply follow our intuitions” as they are generally unreliable and tend to limit any formalized risk management process. [48]

Often leaders incorporate biases and exclude a disciplined dialogue that identifies risk, assesses its impacts on objective outcomes, and identifies ways to manage it. Biases and other cognitive traps and logical fallacies play a large part in decisions made by policy makers and strategic advisors. Most often, cognitive traps, fallacies, and biases cloud the decision-makers judgment by allowing them to be misled by others, their environment, and most importantly, themselves.[49]

When applying the intuitive model, as decision-makers begin to understand the situation, they generate cues from initial familiar impressions. These cues allow them to recognize similarities in the situation and encourage them to follow previously developed cognitive courses of action or options that are often suboptimal. In effect, they become “wedded” to this initial information and use it for future decision-making despite the known danger of making tenuous connections in highly uncertain and complex situations. This tendency to overly rely on initial information and situational impressions is called “anchoring.”[50] Anchoring prevents leaders from applying a risk management framework because it limits their ability to actively frame the problem. Since the leader already has a vision of the situation and problem, they immediately

transition to developing possible actions without conducting a deliberate analysis of the negative consequences.

Another bias often demonstrated in national security decisions is overconfidence. History and multiple studies indicate, “that people overestimate their ability to influence events” or strategic actions.[51] Generally, decision-makers become overconfident about their appraisals of the situation and are either too narrow in their risk assessment or fail to do one at all. Overconfidence has negative impacts on national security decision-making and generally fails to incorporate a quality discussion of risk and often predispose leaders to take military action vice diplomacy.[52] This bias is common in national security issues due to the relative strength of the US and its ability to use all the elements of its national power.

Finally, availability heuristic often limits a leader’s ability to incorporate risk management in intuitive decision-making. An availability heuristic is where “an individual tends to interpret the frequency or probability of an event based upon what instances” are available in their memory.[53] Availability heuristic not only creates problems that arise from these traps in intuitive decision-making, but are often compounded with confirmation bias. Confirmation bias causes decision-makers to search for and interpret information “that confirms our conscious and unconscious expectations” and suppresses information that contradicts them.[54]

The most significant challenge with the intuitive decision-making model is it lacks a risk management function within the process. Cognitive biases and use of heuristics limit the decision-makers ability and desire to identify, assess, manage, and discuss the negative consequences associated with national security choices. President Bush,

during the lead up to the Iraq invasion, clearly demonstrated many aspects of the intuitive decision-making model. Bob Woodward identified in his book *Bush at War*, that Bush was maintained a strong predilection for his “secular faith in his instincts” as the Commander in Chief.[55]

The second model that limits or prevents the incorporation of risk management in decision-making is the collegial decision-making model. As referenced earlier, when the collegial model is applied strategic decision-making, the President is the center of the policy-making and decision cycle. This model is marked by a flexible and informal approach for sharing information between competing advisors, as opposed to a more bureaucratic and structured method. There are considerable limits to this approach including an excessive demand on the President’s time and attention, lack of a staff process and routine oversight on decision process inputs and outputs, and susceptibility for advisors and the President to engage in groupthink.[56]

Groupthink is a concurrence-seeking phenomenon that people engage in as they lean toward unanimity and agreement and “override their motivation to realistically appraise” alternatives or upset the process toward a decision.[57] As a result, there is little or no judgment of the risks involved. The dark side of groupthink is that members providing input into the decision-making process often feel safety in the group. This safety inevitably allows members to “be more inclined to behave in risky and even reckless ways in groups” because accountability is often diffused or shifted among others.[58] This notion of the “risky shift” is codified in the famous quote by President Kennedy that, “success has a thousand fathers, but failure is an orphan.”[59]

Since the collegial model is highly susceptible to the groupthink phenomenon, it fails to provide the routine oversight necessary to ensure that the risk management process is being followed after the problem is framed. The decision-maker never faces the dilemma of determining the “line of acceptable risk” nor understands how much risk is associated with the decision and what if anything can be done about it. Since the President is the driving force behind making a decision, the aspects of risk assessment and risk judgment may not occur. Many times, once the problem is framed and a decision is made, *groupthink* generally prevents an accurate assessment of the threats and hazards associated with the decision.

Decisions leading up to the Bay of Pigs and Iraq invasions suffered from bias and other cognitive traps introduced by faulty intuitive and collegial decision-making models. These biases and models prevented each President from identifying, assessing, and managing the risks associated with these invasions. However, these identified risks could have been, in some form or another, been better managed through the NSC as a result of careful analysis. The first step is to use a decision-making process that limits cognitive biases and promotes the identification and discussion of risk.

Lack of a National-level Risk Management Process

The second impediment is the lack of a comprehensive national-level risk management process focused on attaining national security outcomes across all governmental departments.

There are three aspects to this impediment. First, there is neither a framework nor requirement for all governmental departments to provide risk appraisals or management measures to the national security decision-making process. Second, there are multiple definitions of risk across government. Third, there is a general lack of “risk-

mindedness” across government that limits a serious discussion of what can go wrong with security policy and how to prevent it.

The Department of Defense, through the JRAM, has the most comprehensive approach toward objective oriented risk management. Other departments either do not have a risk management framework aligned with their ability to meet NSS requirements, or only focus on very specific events not necessarily tied to national security. For example, the Department of Homeland Security (DHS) identifies broad risks to the homeland such as natural disasters, spread of highly infectious disease, and even WMD events from homegrown or foreign terrorists. DHS does not comprehensively address the challenges to national security found in the NSS. While it does emphasize the importance of risk communication, it mainly focuses on communicating risk only within DHS and externally to the public as risk events become intolerable or unacceptable.[60] Additionally, similar to other governmental departments, within the limited DHS risk management framework, there is no reference on specific deliverables to the President or the NSC decision-making process.

Another aspect to the problem is there are multiple definitions of risk across the national security enterprise, several methods to attempt to identify it, and no process to integrate each of the disparate assessments.[61] In order for national security leaders to gain a comprehensive understanding of risk in this environment, there must be a standardized framework that each department can use to make and communicate risk judgments. A well-defined concept of risk management contributing to policy decisions along with an “institutionalized, routinized” decision-making process will adequately address and manage risks and achieve policy objectives.[62]

The final aspect to the problem is the lack of a risk-minded culture whereby the President and advisors avoid risk discussion. Many times the Chief Executive, and other NSC decision-makers view attempts to discuss the probability and consequence of bad events happening as being overtly negative or non-supportive of the policy or strategy. Often the "honest broker" or "devil's advocate" who attempts to discuss risk is shunned or limited in their participation, as their input is deemed overly pessimistic of the plan. These decision-making groups must be "risk minded" and work to establish a culture that embraces risk dialogue between decision-makers and advisors. The President plays a large role in "creating a risk-aware culture – one that values dissent and warning, promotes transparency and demands candor" from his advisors.[63] Therefore, he should embrace these discussions, and view them as critical elements of decision-making that enables his ability to manage risk.

Taking *Risky Business* Head On

To overcome the impediments to managing risk in national security decisions, strategic leaders must take *risky business* head on. In the US governmental system, "the President is ultimately the decision-maker, the nominator of his team, and architect of his process for making decisions."[64] Therefore, any process to make better national security decisions, manage the risks associated with those decisions must originate with the Commander in Chief.

Roles, responsibilities, and processes could be specified in a National Security Policy Memorandum (NSPM) directing NSC processes and adapted structures.[65] Specifically, the President could modify the NSPM in three ways. First, the NSPM should require the NSC to codify a prescriptive planning and decision-making process limiting the use of cognitive traps, biases, and fallacies that limit quality decision-

making. Second, the NSPM should require the NSC to implement a risk management methodology similar to the JRAM. Additionally, the President should direct all departments to adopt a similar risk management methodology requiring the outputs to be integrated into NSC planning process.[66]

Codified National Security Decision-making Framework

An improved NSPM specifies two efforts establishing a codified national security decision-making process. First, it requires the NSC to adopt a prescriptive planning and decision-making process following an established, more rational-model framework. The NSC/IPC should implement a rationally based planning and decision-making model similar to the Joint Operations Planning Process (JOPP). The JOPP is an orderly, analytical process, consisting of a set of logical steps to examine a problem; develop, analyze, and compare alternative options; select the best option; and then produce a plan or strategy.[67] A rational decision-making framework helps achieve “de-biasing” where planning and decision-making groups follow a more controlled mode of thinking.[68]

Included in any initiative to making better national security decisions, the President should then implement certain measures to address poor decision-making structures once rational options are brought to him for decision. The President should have the NSC identify if the results of planning efforts have a unanimous recommendation from the NSC/PC. If not, the President should be made aware of “how many, who, and how strong” the dissenting opinions were amongst the group and the qualities of any alternative recommendations.[69] Next, the President should understand if any recommendations have any unmitigated risk associated with the options, or if he is being asked to accept risk. If asked to accept risk, he must understand the nature of the consequences and the probability of associated events or outcomes.

These measures would ensure the President is not only privy to dissent, but also guarantees a risk dialogue takes place early in the decision cycle. They also encourage debate throughout the process at all levels of the NSC. In the end, these discussions allow the NSA to be the honest broker, as many of these debates "occur before they reach the President, but some should occur in front of the President."[70] Candid divergence among advisors and decision-makers is a valuable part of the process. The ability to reconcile disagreements is the President's responsibility and makes leadership a critical element in security policy formulation and execution.[71]

Utilizing a NSPM to formalize the decision-making process allows the President and the NSC to maintain control of the process, tailor it to his/her leadership style, and accommodate the different personalities and capabilities of NSC members. This process also provides flexibility to department leaders' contribution to the risk management methodology. A prescriptive, formalized decision-making process encourages rational decision-making, limits bias, and provides the President with viable policy options.

Implementing an Institutionalized Risk Management Methodology

The first step to implementing a risk management methodology is to create a culture of "risk-mindedness" within the NSC.[72] The President should be the standard-bearer for establishing this culture and demand that risk management is a central part of the policy and strategy development process. Additionally, due to the volatile aspect of the strategic environment, the President should be open to repetitive risk dialogues with his advisors. These dialogues occur throughout the development of national security alternatives and through the point he makes a final decision. This is difficult because

policy makers often want to move the process forward and not over-analyze policy details, especially those that could go wrong.

A lack of a risk minded culture was evident during the lead up to President Bush's decision to invade Iraq. Rumsfeld's attempt to have a dialogue with Bush and NSC principles received little enthusiasm.[73] Thus Rumsfeld's illustrative list of potential problems with an Iraq invasion fell mostly in deaf ears. The repetitive aspect of risk discussion must not be a revolving dialogue about hazard identification, but should be a discussion about how previous and new risks are being managed across all departments. A culture of "risk-mindedness" ensures members of the decision-making process are part of the solution when it comes to risk management.

By establishing a risk-minded culture within the NSC and across government, the decision-making body avoids several pitfalls normally associated with poor decisions. First, the President and other members of the NSC process would tend to be less overconfident in a selected strategy alternative.[74] An open dialogue of the potential risks and management options is a sobering process that opens the aperture scope of risk and generates an understanding of what might go wrong. Additionally, members of the process are exposed to more relevant facts and evidence. This provides a wider perspective and limits the likelihood of becoming anchored to only certain elements of information, and also avoids confirmation bias that tends to lead groups poorly informed decisions. Perhaps if the Bush NSC/PC embraced a culture supporting repetitive risk discussion, the decision to invade Iraq might have gone in another direction.

The second step to implementing a risk management process is to formalize the national security risk management methodology across all governmental departments.

Since the conduct of “risk management is painful – not a natural act for humans to perform”, only a compulsory, standardized risk management process can yield the results necessary for today’s national security decision-making.[75] The CJCS approach toward risk management, in his role as presidential advisor, provides an in depth method to manage military strategic and operational risk. Unfortunately, it does not necessarily fill the requirement for management and communication of risk in the NSC decision-making process. National security risk analyses should attempt to integrate an interagency approach with multiple perspectives, and provide holistic input required to make better decisions. To accomplish this, governmental departments involved in security decisions should adopt a compulsory, institutionalized risk management methodology similar to the JRAM.

The outputs of departmental risk assessments are provided to the NSC Interagency Policy Committee (NSC/IPC) where collective risk is appraised and managed at the lowest level. Any unmitigated risk or recommendations to accept risk would rise to the NSC Deputy Committee (NSC/DC) where it would be assessed again to determine further opportunities to manage and address. Again, unmitigated risk, unresolved issues or disagreements are brought to the NSC Principle Committee (NSC/PC) where any final disagreements are resolved. Finally, unmitigated risk and recommendations to accept or avoid risk are brought to the President as part of a candid discussion or decision recommendation. The President has the last say to accept, avoid, or identify other management options not discussed.

The final step to implementing a risk management methodology is to establish a cadre of embedded inter-agency risk experts or “risk czars” in the NSC. These risk

experts, representing their respective department or agency, would be key players in the developing policy and strategy outcomes and responsible for following the aforementioned institutionalized national security risk management methodology. To ensure risk experts are given the appropriate authorities and consistent staff billets within the NSC/IPC, their positions should be mandated through law. These positions should be authorized and appropriated in legislation, whereby each department and agency identified, is a key player in the NSDM. As such, each department would have at least one staff position solely dedicated to national security risk management.

Robert Kaplan and Anette Mikes recommend risk czars work “side by side” with policy-makers and “continuously monitor and influence” the strategic risk profile for each strategy development initiative.[76] These risk experts would best serve the process by participating in all NSC/IPC planning sessions, and in NSC/DC and PC meetings as required. The “risk czars” would have the independence to report their findings directly to the NSA, who would fill the role of “senior risk officer”. Kaplan and Mikes identify the potential for these risk czars to “go native” as a danger of being embedded in the NSC planning process. They run the risk of being “deal makers rather than deal questioners.”[77] To avoid this, the NSA should simultaneously be the senior risk officer and honest broker to the President mitigating any danger.

Establishing a risk management methodology alone will not yield better national security decisions. It is but one significant component that must be integrated into a codified national security decision-making framework in order to yield the strategic success outlined as a policy outcome. As part of the NSPM, the President should require all national security decisions incorporate an institutionalized risk management

methodology.[78] This formalization would embed and reinforce a risk minded culture required for better strategic decisions. Additionally, the NSPM should require participating departments to adopt a formalized risk management process. This process could be the foundation for identifying and assessing risks in each entity's specific enterprise, appraising their ability to support the NSS similar to the CJCS process. Each departmental risk assessment would then be brought forward as an input into the NSC's interagency risk management process supporting Presidential decision-making. This would be a part of a comprehensive approach where the NSC holistically looks at risk as it applies to achieving policy objectives.

Conclusion

The NSC remains ill equipped to make risk-informed decisions despite attempts to improve interagency planning and coordination. The current national security decision-making process does not incorporate a holistic quantitative and qualitative appraisal of risk. These attempts are generally ad hoc in nature and do little to avert the impediments to incorporating risk into decision-making.

To facilitate the development of effective national security strategy, the NSC should adopt a formalized an interagency risk management methodology that adequately identifies, appraises, manages, and then communicates risk to the President before, during, and after strategic decisions. Standardizing the methodology for risk management in decision-making will not guarantee success. It provides decision-makers and their strategic advisors a framework to consider all the relevant risks associated with national security decisions. Such a methodology also facilitates the iterative process of managing risk throughout strategy. It is clear that a formal decision-

making process must implement a risk management process across the interagency effort in the NSC.

Incorporating a risk management methodology into a formalized national security decision-making process is required in the current strategic environment. The question is - can national security policy makers meet the requirement to conduct *risky business*? Will individual and organizational biases continue to plague strategic decision-makers, preventing them from making quality decisions informed by the very risks that might bring strategic failure? Is history destined to rhyme? The answers to these questions are – *perhaps*. When the United States acts in the national security arena it must avoid repeating history and have the rigorous, disciplined dialogue of risk before making strategic decisions.

Endnotes

[1] Project on National Security Reform and Center for the Study of the Presidency, *Forging a New Shield* (Arlington, VA: Center for the Study of the Presidency, Project on National Security Reform, 2008), 9.

[2] This quote is attributed to Mark Twain but there is no specific source or published work that identifies him as the author. There are several different versions, but for the sake of connecting the notion of "repeated history", I use this version for facilitation.

[3] Michael J. Mazzar, "Rethinking Risk in Defense," *War on the Rocks*, April 13, 2015, http://warontherocks.com/2015/04/rethinking-risk-in-defense (accessed October 9, 2016).

[4] Ibid.

[5] Craig Cohen and Josiane Gabel, eds., *2017 Global Forecast* (Washington, DC.: Center for Strategic and International Studies, 2017), 7, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/161219_GlobalForecast_2017.pdf (accessed January 24, 2017

[6] U.S. Joint Chiefs of Staff, *Joint Operating Environment JOE 2035: The Joint Force in a Contested and Disordered World* (Washington, DC: U.S. Joint Chiefs of Staff, July 2016), ii, http://www.dtic.mil/doctrine/concepts/joe/joe_2035_july16.pdf (accessed October 5, 2016).

[7] Ibid., iii.

[8] Ibid.

[9] Ibid., 5–9.

[10] U.S. Joint Chiefs of Staff, *Joint Operations Planning,* Joint Publication 5-0 (Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011), II-2, http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf (accessed October 11, 2016).

[11] Amos A Jordan, William J Taylor, and Michael J Mazarr, *American National Security* (Baltimore, MD: Johns Hopkins University Press, 1999), 3.

[12] Ibid.

[13] David Patrick Houghton, *The Decision Point: Six Cases in U.S. Foreign Policy Decision Making* (New York: Oxford University Press, 2013), 74.

[14] Ibid., 50–51.

[15] Mazzar, "Rethinking Risk in Defense."

[16] Donald Rumsfeld, *Known and Unknown: A Memoir* (New York: Sentinel, 2011), xiii–xiv.

[17] Baruch Fischhoff and John David Kadvany, *Risk: A Very Short Introduction* (New York: Oxford University Press, 2011), 66.

[18] Project on National Security Reform and Center for the Study of the Presidency, *Forging a New Shield*, 10.

[19] Ibid.

[20] National Defense University, *QDR 2001: Strategy-Driven Choices for America's Security* (Washington, DC: National Defense University Press, 2001), 195.

[21] Chairman of the Joint Chiefs of Staff, *CJCSM 3105.01 Joint Risk Analysis*, Chairman of the Joint Chiefs of Staff Manual (Washington, DC: U.S. Joint Chiefs of Staff, October 14, 2016), A-2.

[22] Ibid., B-2.

[23] Ibid., B-1.

[24] Ibid., B-2-B-3.

[25] Ibid., B-3.

[26] Ibid., B-4.

[27] Ibid., B-5.

[28] Martin E. Dempsey, "Risky Business," *Joint Force Quarterly : JFQ*, no. 69 (Second Quarter 2013): 3.

[29] This graph reflects a hybrid of concepts outlined in the CJCSM 3105.01, dated 14 October 2016, and aspects of risk management discussed during the Theater Strategy and Campaigning core course at the U.S Army War College during Academic Year 2017.

[30] Chairman of the Joint Chiefs of Staff, *CJCSM 3105.01*, B-6.

[31] R. Gordon Hoxie, Ryan J Barilleaux, and Center for the Study of the Presidency, *The Presidency and National Security Policy* (New York: The Center for the Study of the Presidency, 1984), 207.

[32] Ibid., 210.

[33] On January 28, 1961 during his initial briefing on the invasion plans, President Kennedy requested a Defense Department review of CIA proposals for the deployment of anti-Castro Cuban forces on Cuban territory with the results of the analysis reported to the President promptly.

[34] Rebecca R. Friedman, "Crisis Management at the Dead Center: The 1960-1961 Presidential Transition and the Bay of Pigs Fiasco," *Presidential Studies Quarterly* 41, no. 2 (June 2011): 319.

[35] Hoxie, Barilleaux, and Center for the Study of the Presidency, *The Presidency and National Security Policy*, 215.

[36] Peter Kornbluh, *Bay of Pigs Declassified: The Secret CIA Report on the Invasion of Cuba* (New York: The New Press, 1998), 14.

[37] Bob Woodward, *Bush at War* (New York: Simon & Schuster, 2003), 343.

[38] Richard Haass, *War of Necessity: War of Choice* (New York: Simon & Schuster, 2009), 234.

[39] Rumsfeld, *Known and Unknown*, 481.

[40] Ibid., 482.

[41] Ibid., 481.

[42] Charles D. Allen, Breena E. Coates, and Goerge J. Woods III, *Strategic Decisionmaking Paradigms: A Primer for Senior Leaders* (Carlisle Barracks, PA: U.S. Army War College, 2012), 36–37.

[43] Michael J. Mazzar, "Fixes for Risk Assessment in Defense," *War on the Rocks*, April 22, 2015, http://warontherocks.com/2015/04/fixes-for-risk-assessment-in-defense (accessed October 9, 2016).

[44] Gary Klein, *The Power of Intuition: How to Use Your Gut Feelings to Make Better Decisions at Work* (New York: Doubleday, 2007), 21.

[45] Ibid., 22.

[46] Ibid., 27.

[47] Ibid.

[48] Ibid., 3.

[49] Steven A Yetiv, *National Security through a Cockeyed Lens: How Cognitive Bias Impacts U.S. Foreign Policy* (Baltimore: Johns Hopkins University Press, 2013), 95.

[50] Ibid., 117.

[51] Robert S. Kaplan and Anette Mikes, "Managing Risks: A New Framework," *Harvard Business Review*, June 1, 2012, 5, https://hbr.org/2012/06/managing-risks-a-new-framework (accessed November 28, 2016).

[52] Yetiv, *National Security through a Cockeyed Lens*, 96.

[53] Redd and Mintz, "Policy Perspectives on National Security and Foreign Policy Decision Making," S27.

[54] Yetiv, *National Security through a Cockeyed Lens*, 117.

[55] Woodward, *Bush at War*, 342.

[56] Hoxie, Barilleaux, and Center for the Study of the Presidency, *The Presidency and National Security Policy*, 219–21.

[57] Houghton, *The Decision Point*, 50.

[58] Ibid., 43.

[59] Ibid.

[60] U.S. Department of Homeland Security, *Risk Management Fundamentals: Homeland Security Risk Management Doctrine* (Washington, DC: U.S. Department of Homeland Security, 2011), 25–28, https://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf (accessed November 28, 2016).

[61] Mazzar, "Rethinking Risk in Defense."

[62] Ibid.

[63] Mazzar, "Fixes for Risk Assessment in Defense."

[64] Robinson et al., *Improving Strategic Competence*, 33–34.

[65] Mazzar, "Rethinking Risk in Defense."

[66] Each NSC department and agency would be given the latitude to adapt the Joint Risk Assessment Methodology used by the CJCS to determine the risks in their specific enterprise.

The only caveat is the outputs of the process must assess, evaluate, characterize, and then manage risks specifically associated with obtaining national security strategy.

[67] U.S. Joint Chiefs of Staff, *Joint Operations Planning, Joint Publication 5-0*, xxv.

[68] Yetiv, *National Security through a Cockeyed Lens*, 97.

[69] Thomas Sheppard and Bryan Groves, "Post 9/11 Civil-Military Relations: Room for Improvement," *Strategic Studies Quarterly* 9, no. 3 (January 1, 2015): 81, https://www.hsdl.org/?abstract&did=786763 (accessed January 12, 2017).

[70] Ibid.

[71] Sarkesian, Williams, and Cimbala, *U.S. National Security*, 124.

[72] Kaplan and Mikes, "Managing Risks," 5.

[73] Rumsfeld, *Known and Unknown*, 481.

[74] Kaplan and Mikes, "Managing Risks," 5.

[75] Ibid., 8.

[76] Ibid., 10.

[77] Ibid., 11.

[78] Mazzar, "Rethinking Risk in Defense."