FACULTY PAPERS ON DEFENSE MANAGEMENT
DEPARTMENT OF COMMAND, LEADERSHIP, AND MANAGEMENT

SCHOOL OF STRATEGIC LANDPOWER
U.S. ARMY WAR COLLEGE, CARLISLE, PA 17013

THE CHALLENGES OF MANAGING STRATEGIC RISK: SETTING A FOUNDATION FOR JOINT DECISION-MAKING

FACULTY PAPER EK-001 – ORIGINALLY RELEASED OCTOBER 2018

Thomas P. Galvin[1] and Jay Rouse

Risk management in the context of enterprise decision-making differs from the operational context. Risk, defined as "the potential for something adverse to happen," is an inherent part of any strategic decision pursued within the defense enterprise. What is meant by 'potential' and 'adverse' is often subjective. Pursuing the capability and capacity to meet current and emerging requirements is constrained by uncertainty in both the global and domestic security environments, forcing senior leaders to make decisions and manage defense programs with incomplete information.

Measuring the risk of any course of action is a highly complex and dynamic problem, sometimes resulting in the superb programming choice of two years ago to appear foolish today. Designing and implementing risk management systems requires a framework to help harmonize the terms used and calibrate assessments, so that the categorization of risk as 'high' or 'low' can be trusted. The framework must also address the changing nature of the environment and its longitudinal effects on risks, along with how best to articulate risks to help in the decision-making process.

Risk, "the potential for something adverse to happen," [2] is an inherent part of any strategic decision pursued within the defense enterprise. What is meant by 'potential' and 'adverse' is often subjective. Pursuing the capability and capacity to meet current and emerging requirements is constrained by uncertainty in both the global and domestic security environments, forcing senior leaders to make decisions and manage defense programs with incomplete information. Measuring the risk of any course of action is a highly complex and dynamic problem, sometimes resulting in the superb programming choice of two years ago to appear foolish today.

Moreover, the demand for capabilities (in quantity, time, and space) will always exceed national resources or will. Annual budgets, even when less constrained, are still finite, creating inherent tensions among actors within the enterprise competing for resources to perform their part of the mission of providing combat-ready forces. Decisions on developing, sustaining, or mobilizing those capabilities involve tradeoffs, and tradeoffs induce risk. Consider the question of investing more of the defense budget in people (e.g., training, equipping, compensation and benefits) versus modernizing weapons systems. If one cannot do both completely, then anything not undertaken may present risk. Additionally, the defense

[1] Corresponding author. U.S. Army War College, ATTN: DCLM, 122 Forbes Avenue, Carlisle, PA 17013. Thomas.p.galvin.civ@mail.mil

[2] Paul K. Davis, *Lessons from RAND's Work on Planning under Uncertainty for National Security* (Santa Monica, CA: RAND Corporation, 2012), 1.

enterprise faces a unique and very difficult challenge in calibrating risk assessments across strategic, operational, and tactical levels. For these reasons, the services and the joint community have developed and employed decision support systems known as *risk management systems* to identify, assess, and control[3] risks in clear and consistent ways to aid strategic decision making.

Designing and implementing risk management systems requires a framework to help harmonize the terms used and calibrate assessments, so that the categorization of risk as 'high' or 'low' can be trusted. The framework must also address the changing nature of the environment and its longitudinal effects on risks, along with how best to articulate risks to help in the decision making process. To this point, the defense and joint communities and the services have successfully employed risk management systems independently, leaving open the question of a framework to calibrate risk management across the enterprise. The recent implementation of the Joint Risk Assessment System (JRAS) is a step in that direction, but it is only a step.

The purpose of this paper is to present a foundation for discussion of strategic risk management and risk management systems as they apply in the defense enterprise. Included is a presentation of the JRAS' underlying framework developed by the International Risk Governance Council. Our goal is to open dialogue to promote common shared understanding of risk management, potentially leading to a single robust enterprise-wide architecture that will improve the incorporation of risk in strategic decisions. The paper will first explore the meaning of strategic risk, then present a foundational understanding of risk management (or risk governance as it is also called), and conclude with an introduction to JRAS and brief comparison with other risk management activities in DoD.

Meaning of Risk at Strategic Level

There are different ways that *risk* is applied across government, finance, and other sectors. The security sector tends to view it as a combination of the consequences of an adverse event and its probability of occurrence. The financial sector, however, uses volatility as measure of risk, such as using past price fluctuations in the market as a gauge for future variance.[4] For example, the risk assumed by an investor is the potential of the portfolio to lose value, and thus the risk analysis considers past performance (which likely includes both gains and losses over time), weighing the likelihood of gaining value over the timeframe set by the investor (short or long-term). In government contexts, risks tend to be expressed as vulnerabilities – the inability to respond to a situation, rather than the situation itself. That is, if a particular system is underfunded, the risk is associated with the lost or unrealized capability. The following subsections clarify other terms that tend to be conflated or combined with risk – hazards, uncertainty, and opportunity.

Risk vs. Hazards and Threats

A *hazard* is something, either persons or situations, which could cause harm.[5] However, the mere existence of the hazard does not constitute a risk. The hazard must act or be acted upon to create harm. Consideration of the probability that harm would occur due to the hazard is what constitutes *risk*. Scheer et al (2014) offers the following illustration.

To illustrate, one example is the toadstool that contains a fatal poison for human beings. As long as no one eats the toadstool there is no risk, merely a hazard. However, knowledge about the probability of how often mushroom pickers mistake the toadstool for an edible mushroom combined with data related to the probability of the ingestion of a toadstool (exposure) makes it possible to calculate the risk of the related ingestion of a certain amount of poison and the

[3] Drawn from definition of 'risk management' in Chairman of the Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, 2010), 208. Hereafter *DoD Dictionary*.

[4] Davis, *Lessons from RAND's Work*, 2.

[5] Dirk Scheer, et al., "The Distinction Between Risk and Hazard: Understanding and Use in Stakeholder Communication," *Risk Analysis*, Vol. 34, No. 7 (2014): 1270-1285, doi: 10.1111/risa.12169, 1271.

expected health impact from the ingested amount (dose-response relationship).[6]

In the defense enterprise, this difference is often encountered when addressing a *threat*, in the form of an adversarial state or non-state actor. This view is shared among some other government agencies such as the Department of Homeland Security that also measures risk in terms of identified threats.[7] The adversary is the hazard, and the likelihood that the adversary will take action, and the nature of scope of such action, informs the risk assessment. Adversaries are adaptive, and actions to reduce risk may spur adversarial responses that increase it or change its nature.[8] Natural disasters are also hazards, and the likelihood and scope of future events, which can be estimated from historical patterns, helps calculate risk.

A challenge for strategic decision makers is the diversity of hazards in the environment, and overemphasizing one category over others could produce poor decisions. The 2010 Quadrennial Defense Review offered an example of how categorizing hazards (operational, force management, institutional, and future challenges[9]) can help ensure completeness in the analysis.

Risk vs. Uncertainty

It is important to delineate risk from uncertainty because they are often confused, and there are different types of uncertainty.[10] Uncertainty is "the inability to know everything about a situation and the difficulty of predicting the nature of effect of change."[11] Risk is therefore uncertainty combined with a probability of occurrence. If one assesses that an adversary has a 10% chance of invading a neighboring state and causing catastrophic damage, that's a statement of risk. If the adversaries' intentions are not known or knowable and therefore probability cannot be determined, then this is a statement of uncertainty, and efforts at strategic planning attempt to shape the environment around the adversary and deal with the potential surprises until risk can be judged.[12] In the case of acquisition, there is considerable uncertainty in the cost of developing new technologically-advanced capabilities. Risk is difficult to assess when the probabilities of cost are incalculable and technical readiness levels impossible to forecast accurately. Therefore additional effort must be expended to develop sufficient understanding of the technology and cost drivers so that probabilities of success and cost consciousness can be weighed in the acquisition decision.

Risk vs. Opportunity

Although not ordinarily discussed in defense contexts, many risk management systems combine assessments of risks with opportunities, "proactive decisions that can have a large upside"[13] such as alternatives for cutting costs or pursuing investment. *Opportunity costs*, which is the cost incurred by not taking an alternative action, is important to defense managers as these represent the value of trade-offs in making decisions affecting the enterprise. For example, choices of platforms that are less capable, but perhaps less expensive and with a shorter fielding time, may incur opportunity costs that are relevant in matters of risk.[14]

Paradoxes of Risk in the Defense Enterprise Context

Paradoxically, the assessment of risk and its articulation to decision makers is itself fraught with risk.[15] How risk is described to external

[6] Scheer, "The Distinction," 1271.

[7] Clark A. Murdock (Dir.), *Risk Management in Non-DoD U.S. Government Agenices and the International Community: Best Practices and Lessons Learned* (Washington, DC: Center for Strategic and International Studies, March 2011), 6.

[8] Gregg M. Burgess and Thomas D. Clark, Jr., "The Defense Acquisition System: A Meta-Organizational Analysis," *Systems Research*, Vol. 7, No. 3 (1990): 169-191.

[9] U.S. Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, February 2010), 89-95. Although titled a "Defense Risk Management Framework," the categorization given in these pages is more properly called a hazard identification framework.

[10] Davis, *Lessons from RAND's Work,* 3.

[11] Stephen J. Gerras (ed.), *Strategic Leadership Primer*, 3rd ed. (Carlisle, PA: Department of Command, Leadership, and Management, 2010), 11.

[12] Davis, *Lessons from RAND's Work,* 10.

[13] Murdock, *Risk Management in Non-DoD*, 12.

[14] Murdock, *Risk Management in Non-DoD*, 10 presents this as a trade-off between "program risk" and "institutional risk," whereby programs incur risk within their own purview while the enterprise sees risk across programs.

[15] C. W. Johnson, "The Paradoxes of Military Risk Assessment," in A. G. Boyer and N. J. Gauthier (eds.), *Proceedings of the 25th International Systems Safety Conference* (Baltimore: International

stakeholders has an influence on the strategic environment and affects how government leaders provide resources for military activities, short and long term. With this in mind, Johnson (2007) presented thirteen paradoxes of military risk assessment, a few of which are elaborated here.[16]

The link between perceived levels of risk and increased expenditure has left the military vulnerable to claims that threats have been over estimated. In other words, if the risk is not perceived by the stakeholder as significant enough, then a favorable decision might not be reached. Note that Johnson only commented on the perception, which is fueled by the fact that risk assessments of strategic issues tend to be expressed categorically (e.g., low, moderate, significant) and not as a probability, which raises the question about what is being discussed – risk or uncertainty.

In military acquisitions there is a tension between accepting sufficient risk to create innovative systems that exceed enemy capabilities and yet rejecting those projects that are so innovative that they are unlikely to yield operational benefits within a fixed timescale and to a specified budget. This stems from a cultural paradox that the military faces between its pursuit of long-term visions (often expressed with a target year like Joint Force 2020) against the exigencies of an budget process. It has also been charged that defense managers are driven to forsake the future in favor of short-term objectives whereby they can make their 'mark' so they can be promoted. As such, 'safer' alternatives with guaranteed results would be favored.

Military risk assessments are usually validated by reference to the hazards that were realized in previous missions, this makes them overly conservative given that few records are maintained of successful operations where hazards were avoided. Put another way, the military weighs risk according to what has been learned from previous experience and tends to ignore uncertainties. According to Johnson, this leads to "unnecessarily conservative" assessments whereby "an unnecessary level of resources [are needed] in order to mitigate low levels of risk."[17]

The final paradox chosen for this paper provides a good segue into the challenges of risk management and how to model it. *The enthusiasm for [risk management] techniques … in some sections of the military may create a hostility and cynicism amongst those personnel who are faced with the application of simple risk assessment techniques under complex, time limited constraints with incomplete information.* While the context of this paradox was the so-called Composite Risk Management doctrine used in the U.S. Army in the 2000s, it applies equally at the enterprise level in reporting strategic risk. If the model assumes the availability of more and better information than is possible, the outcomes of the risk assessment may be flawed. Moreover, if the assessment model does not sufficiently account for the varied hazards that one must account for, the users of the model will introduce bias when plying the data to fit the model, in addition to increased hostility and cynicism.

Risk Management Frameworks

The purpose of a risk management framework is to provide defense managers with a systematic approach to collecting the necessary data and exercising thorough and consistent analysis with minimal bias, so that the outcomes can be useful for decision makers. By "thorough and consistent," it is also understood that risk is inherently multi-level, and manifests itself differently at the tactical, operational, and strategic levels. It is important that the model appreciate the differences and synthesize them together, rather than choose one level over another, such as articulating tactical risk as though it were strategic.[18]

Using a simplified version of Clarke and Varna's (1999) model, there are three essential elements to the strategic risk management

Systems Safety Society, Unionville, VA, 2007), original pages 859-869. Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.62.1988&rep=rep1&type=pdf (accessed 31 August 2015).

[16] These represent paradoxes 1, 2, 4, and 12 in Johnson, "The Paradoxes."

[17] Johnson, "The Paradoxes," 862.

[18] Christopher J. Clarke and Suvir Varma, "Strategic Risk Management: The Competitive Edge," *Long Range Planning*, Vol. 32, No. 4 (1999): 414-424, see 415-416.

process – gathering data, appraising risk, and taking action.[19]

Gathering Data

Collecting the data to which to assess risk involves two discrete steps – framing the environment and collecting the relevant information. Framing the environment (also called "setting the context"[20]) determines what kinds of information about the strategic environment and the organizational posture are relevant to the assessment. Organizations with a narrow core mission are more likely to consider more narrow categories of risk in their models. The U.S. defense enterprise, whose core defense missions are diffuse and who has a wide range of collateral missions in support of other U.S. government agencies and international partners, will tend to need a broader array of information to assess risk. The organization may elect to widen or narrow the scope as deemed necessary.

The organization's objectives typically drive what data is gathered and what risks are considered most relevant.[21] In the military, these might include threat analysis, stakeholder analysis, and opportunity costs. What is at stake for the organization in steady-state conditions is also critical, such as its fiscal posture, sense of competitive advantage, image, and its relationships with stakeholders.[22]

Appraising Risk

Next is the act of conducting the analysis or appraising risk. This constitutes the identification and prioritization of the hazards and determination of probabilities and scope. Again, probabilities at the strategic level may be a categorical scale of 'low' to 'high' rather than a number or percentage. The choice of scale used depends on the context, data, and available organizational energy. Numeric scales may appear more precise but may be too expensive and time-consuming for the informational benefit over a simpler 'high-medium-low' scale employing only one's judgment. The scale should also be sufficient flexible to address emerging challenges.

Once done, there is a synthesis and evaluation step that determines tolerance and acceptability. This serves to highlight potential mitigation strategies or prioritizations among them. The models should be appropriately sensitive so that special or unusual hazards can be appropriately addressed. For example, a risk may be low probability but extremely devastating, such as a nuclear event, or utterly intolerable, such as a repeat of the problematic response to Hurricane Katrina. When such risks influence the core mission of the organization, the low probability becomes less a factor and the organization is more likely to choose mitigating actions (however, Johnson's first paradox on overestimating risk applies).

Taking Action

Organizations then act to mitigate intolerable risks and ignore the others based on available strategies and resources and communicate those actions to stakeholders. Risk management frameworks may categorize the resultant strategies differently so to help aid decisions makers and channel organizational energy more efficiently. For example, to segregate and prioritize 'simple' actions that can be taken using the organization's existing structure and processes and 'complex' actions that demand substantive organizational changes. Another example is where within the organizational structure that the risk mitigation strategies are governed, with many delegating responsibilities to lowest feasible levels.[23]

An important caution comes from a study of risk management frameworks from across the U.S. government and globally, that "risk management should seek to inform decision-making, not replace it."[24] Senior defense managers face a significant number of enterprise-level decisions, and for whom the rigor of a quality risk assessment affords them the opportunity to take the recommendations as is.

---

[19] Clarke and Varma, "Strategic Risk Management.", 416.
[20] Murdock, *Risk Management in Non-DoD*, 4.
[21] Murdock, *Risk Management in Non-DoD*, 15.
[22] Clarke and Varma, "Strategic Risk Management.", 416. Private sector firms would also be concerned about organizational survival, something that is not treated similarly in defense, but certainly the defense role in national survival is relevant.
[23] Murdock, *Risk Management in Non-DoD*, 15.
[24] Murdock, *Risk Management in Non-DoD*, 16.

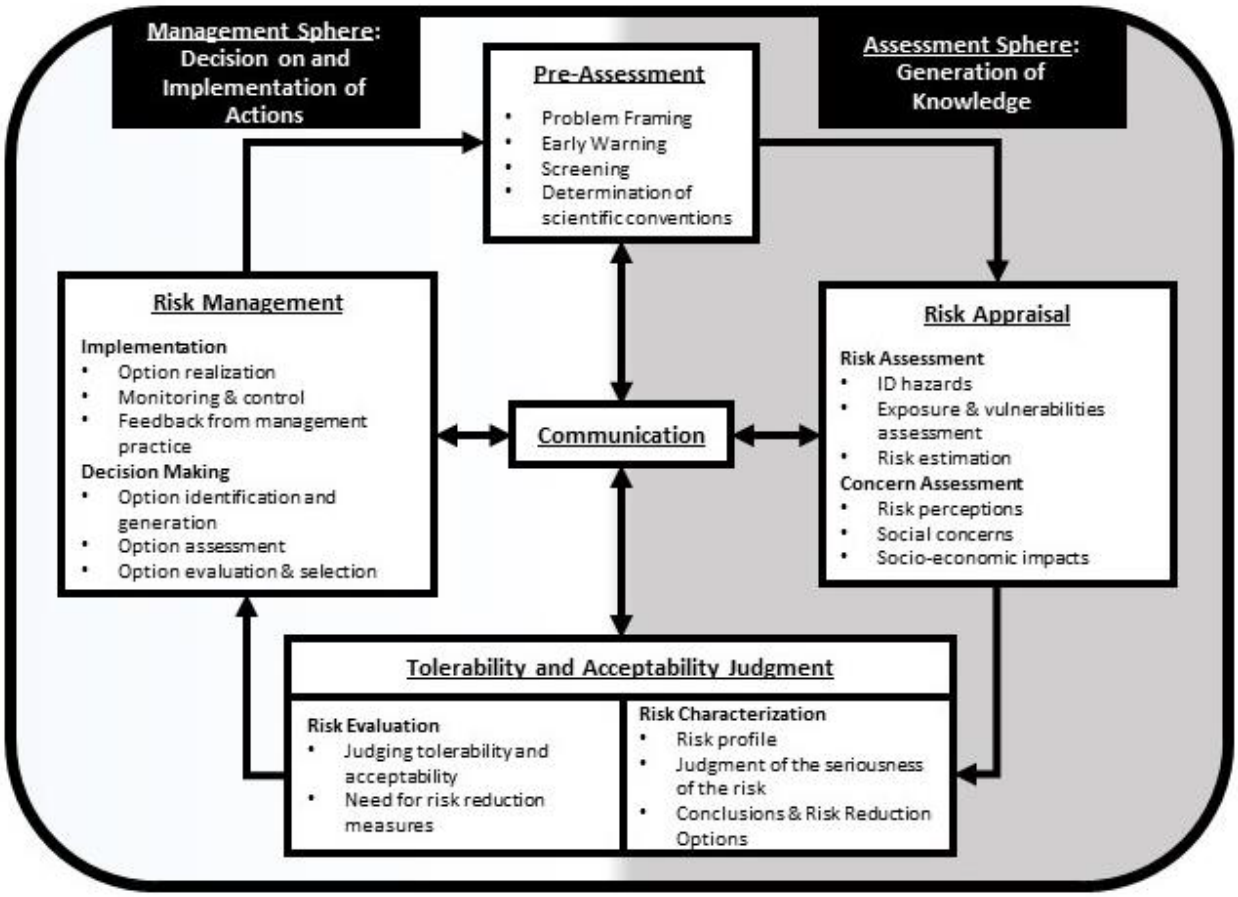

Figure 1. International Risk Governance Council Framework (adapted from IRGC 2006)

Risk-based decision-making only serves to aid judgment based on determination of probability and scope of a risk but does not consider all other factors that are critical to a decision.[25]

Example – the International Risk Governance Council Framework

Of the numerous risk management frameworks and models available in the literature, the one chosen as the example for this article is the International Risk Governance Council (IRGC) framework as it is in the public domain and elements of it have been incorporated into defense enterprise-level risk management activities. The main elements are presented in the risk governance framework shown in Figure 1.[26]

The IRGC Framework's four phases mirror the data gathering-appraising-taking action cycle expressed in the previous section, with the greatest difference being that appraisal is divided into two distinct phases of assessing and judging. Additionally, the framework separates the roles and responsibilities between decision makers (*management sphere*) and support elements or subject matter experts (*assessment sphere)*. The four phases are as follows. The *pre-assessment* incorporates both framing the context of a potential course of action and then gathering the data internally and externally to the organization. *Risk appraisal* takes the data and identifies both linkages to potential sources of harm (risk assessment) and indirect perceptions and implications (concern assessment) related specifically to the course of action. This is done

[25] Murdock, *Risk Management in Non-DoD*, 17..

[26] International Risk Governance Council (IRGC), *White Paper on Risk Governance: Towards an Integrative Approach* (Geneva, Switzerland: IRGC, Reprinted 2006).

by subject matter experts of the course of action itself to reduce bias and ensure objectivity. Strategic concerns will be incorporated later.

The third phase, *tolerability and acceptability judgment*, is broken down into two actions – *characterization* followed by *evaluation* – that signal the shift from assessment sphere to management sphere. During characterization, risks are initially judged as acceptable or tolerable. 'Acceptable' means that action's negative consequences are not of concern even if no risk mitigation strategies are taken. 'Tolerable' means that the action's benefit outweighs the consequences so long as mitigation actions are pursued. Thus, for a risk to be deemed tolerable, the mitigation strategies must be considered with it. As the judgment is passed to the risk evaluation phase, whereby the decision makers take over, the broader strategic perspective of the action is synthesized to produce a final judgment of tolerability or acceptability and the associated mitigation strategies.

The final phase is *risk management* that constitutes the final course of action taken along with risk mitigation actions, monitoring, and feedback.

The IRGC framework is also interesting in how it depicts two feedback mechanisms. The first, represented by the outer arrows, is the feedback inherent to the assessment process. At each cycle, the environment is evaluated anew to inform adjustments to the chosen action. The middle of the diagram includes a continuous stream of *risk communication* that goes across the organization at all phases of the risk assessment. This action enables the organization to articulate risk with external stakeholders and helps "balance factual knowledge about risk with personal interests, concerns, beliefs, and resources."[27] This is intended to help the broader society cope with statements of risk and potentially react more favorably to crises and disasters if they occur (see Appendix for an example of assessing and communicating risk).

The IRGC framework also classifies risk-related problems into four levels, each requiring more intense strategic approaches and higher levels of organizational energy. *Simple risk problems* are characterized as routine because sufficient data and knowledge are available, and thus the problem can be addressed using the organization's extant decision-making processes. *Complex risk problems* are characterized as lacking sufficient available data or knowledge to make an appropriate risk assessment, or that there is significant disagreement (at a broader scientific level, not differences of opinion within the organization) on how to conduct the appraisal. *Risk problems due to high unresolved uncertainty* must consider a wide range of additional criteria such as reversibility, persistence, and ubiquity. For example, if the hazard is a 'dirty bomb' but there is considerable uncertainty over the probability of occurrence and the course of action (e.g., significant increase in law enforcement posture) could have negative effects of its own, then the Framework guidance recommends a cautious approach that allows for reversal if the action causes harm. Such approaches should be geared toward "learning" about the environment so to reduce the uncertainty. *Risk problems due to ambiguity* relates to problems where different stakeholders in society harbor vastly different perspectives on the risk, making decision making difficult due to the potential for conflicting priorities. These problems require further exploration through societal discourse toward finding an acceptable solution, while decision makers must seek to synthesize the disparate views during the risk management phase.

Conclusion

Risk management is a vitally important function in the defense enterprise and is arguably one of the most difficult and controversial because of all the unknowns, uncertainties, and ambiguities in the strategic environment. Developing high-quality, objective assessments of the risks facing the nation is complex and must avoid undue influence from political or other concerns. Thus, the risk management system must afford defense managers at all levels the ability to systematically frame the hazards, threats, and opportunities available. Tools such as the IRGC Framework have been successfully used in other venues and have been adapted for

[27] IRGC, *White Paper on Risk Governance,* 15.

defense enterprise use. Regardless of which tool is used, however, it is crucial to account for how risk assessment can lead organizations to poor solutions, such as offered in Johnson's (2007) paradoxes. Risk management does not replace decision making, it is only a supporting mechanism. But a powerful one it is, as it helps decision makers make sense of the complex and adaptive strategic environment and provides a rigorous look at difficult choices facing senior defense officials.

Thomas P. Galvin is an Associated Professor with the Department of Command, Leadership, and Management whose research interests include change management, strategic communication campaigns, national preparedness and military readiness management, and military organizational design. He has served at the U.S. Army War College since 2011.

Jay Rouse was formerly a contractor working with the Joint Staff J-5 on updates to the Chairman's Readiness System.