



Lt. Col. Thomas Sacchieri (*right*), commander of 1st Battalion, 16th Infantry Regiment, 1st Armored Brigade Combat Team, 1st Infantry Division, speaks to the battalion S-3, Maj. Michael Anderson (*center*) while others listen in during a battalion combined armed rehearsal on 18 February 2025 at the National Training Center at Fort Irwin, California. Post-rehearsal commander-to-commander dialogue should include a thorough risk assessment. (Photo by Pvt. 1st Class Christopher Bailey, Operations Group, National Training Center)

# Eyes Up

## Reframing Risk Dialogue for Improved Decision-Making

Maj. Christopher Zaczyk, US Army

*It's day three of an armored brigade combat team's rotation at the National Training Center. As the sun sets on the desert, the battalion commanders collect their thoughts after the brigade operation order brief and prepare for commander-to-commander dialogue. Chief*

*among the topics of conversation is their assessment of risk to inform the way ahead before operations commence. Within the next hour, the brigade commander will, without a doubt, make decisions that will affect the outcome of the following day's operations.*

*Three hours up the road, a professional poker player takes her seat at the table. The opening hand is dealt, and she reviews her cards, eyeing her opponents for tells and contemplating her next move.*

*Halfway across the country, an offensive coordinator is under the lens of the Monday Night Football camera as his team moves back to the huddle. The score is close, and analysts in the box provide inputs for him to consider as he weighs whether to punt or keep his offense on the field for a fourth-down attempt at a three-yard gain.*

On the surface, these scenarios couldn't be more different. However, when viewed through the lens of assessing risk, several similarities emerge. The key players in all three vignettes are informed by years of experience. They must work with incomplete information against a determined opponent. Most importantly, they are painfully aware that their decision could result in tremendous success or catastrophic failure. They all have decisions to make, and none have the luxury of time with which to make it.

The key difference between the characters above is that only one of them is forced to make their decision in isolation—the poker player. The brigade commander and offensive coordinator are surrounded by experts who are responsible for cutting through the noise and bringing out the best possible decision.

When commander-to-commander risk dialogue is effectively executed, commanders operate like offensive coordinators. Their decisions are informed, risk is mitigated, and the richness of the dialogue opens the aperture of the conversation to move beyond reactive and defensive decisions to aggressive, offensive-minded opportunity seeking. Regardless of the outcome, leaders can trust that they've weighed consequences and aligned resources toward the best possible course of action. When risk dialogue fails, commanders are forced to act as poker players—alone at the table, armed with only their experience and intuition.

Risk dialogue can fail in two scenarios. First, when subordinates overemphasize and become hyperfocused on hazards and threats and second, when a senior commander cannot clearly articulate a desired outcome.

An environment where subordinate commanders overemphasize threats to their senior commander misrepresents the balance of threats and capabilities in

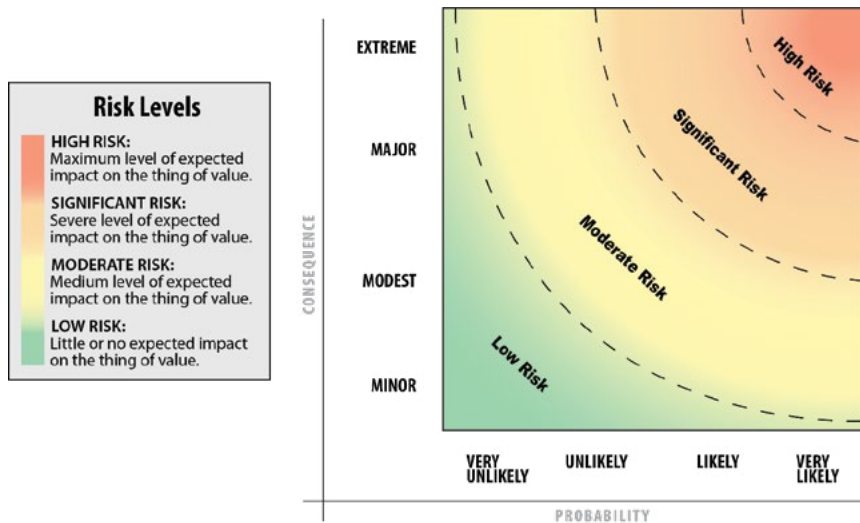
the pursuit of desired outcomes. Fixation with environmental factors best demonstrates this and often results in lackluster analysis limited to comments like “Temperatures will be high, so we need to ensure soldiers are drinking water.” At best, threat-centric discussion provides commanders with little more than an obvious list of potential problems they alone are left to synthesize and assess. At worst, identified threats overwhelm the decision cycle and result in gridlock or brushing off potentially significant problems in favor of smaller, more solvable issues. Commander's risk dialogue is too significant a component of the planning, preparation, and execution framework to settle for a nonsubstantive conversation.

In the second scenario, subordinates cannot provide adequate risk assessments because they cannot envision the larger context surrounding the desired outcome being threatened. The cognitive linkage of operations within the unit and how they nest within the objectives of headquarters one and two levels up is integral to successful dialogue. When the organization understands the desired outcome of the operation and the arrangement of tactical actions in time, space, and purpose toward that end, an effective dialogue and better decision-making follow. Just as the offensive coordinator relies on the head coach to provide the context of a desired end state for the drive in the wider context and atmospherics of the game, so too must subordinates understand their role and what success or failure in their operation means in the wider scope of the mission.

Clearly articulating risk, what mitigating risk means, and how opportunities are conveyed to enable commanders to make informed decisions requires a change. This change demands a refocusing of risk dialogue, from hazards and threats to desired outcomes and command decisions at echelon. A mindset shift, grounded in desired outcomes, is fundamental to creating shared understanding for commanders on the battlefield.

The benefits of effective risk dialogue aren't limited to shared understanding and improved commander decision-making, however. Risk dialogue is a key

**Maj. Christopher Zaczyk, US Army,** serves with US Northern Command. His previous assignment was as executive officer for 1st Brigade, 1st Infantry Division.



(Figure from CJCSM 3105.01B, *Joint Risk Analysis Methodology* [US Government Publishing Office, 2023], B-6)

## Figure 1. Baseline Risk Levels and Generic Risk Contour

states, “Risk is the probability and consequence of an event causing harm to a thing that is valued.”<sup>2</sup> These definitions are too narrow and miss the integration of a directed or desired outcome in the assessment of risk. In short, these definitions assist with the assessment of the magnitude of a threat. Fully understanding risk demands broadening the understanding of its components and their relationship to the end state.

First, risk analysis must recognize that threats and hazards persist whether a desired outcome is present or

forum in the doctrinal process of commander-to-commander dialogue where a subordinate commander can negotiate with their senior commander. Commanders who can convey risk and opportunity are commanders who win additional resources for their formations and build trust and respect with their higher headquarters. In time-constrained environments like at training centers and during combat operations, the ability to concisely convey risk creates decision space for commanders when needed most.

This article seeks to facilitate better risk dialogue by offering an updated definition of risk and related topics, reframing the lens through which leaders approach risk assessment, and providing a structure for delivering risk assessments that drives decisions. Instead of keeping an eye downward for potential threats, leaders at all echelons can reframe their risk dialogue with an eyes-up approach—deriving risk assessments from their desired end states, identified threats, and capabilities.

## Decoupling Risk, Threats, and Hazards

Current risk doctrine conflates threats and risks by asserting that a negative event’s severity and probability constitute the risk. The Army defines risk as “probability and severity driven chance of loss, caused by threat or other hazards.”<sup>1</sup> Moreover, joint doctrine

not. The severity of impact and the likelihood of occurrence do not solely constitute a risk; they define the magnitude of the threat. The world is full of hazards. Identifying hazards that *threaten* the achievement of an acceptable outcome, and the extent to which they threaten it, is the only relevant objective of threat analysis. Delineating between a threat and a hazard produces unnecessary complexity in analysis. A passive negative factor like weather and an active negative factor like an enemy massing are both valuable considerations because they *threaten* mission accomplishment. There is no need to separate them. It’s important to note existing risk analysis tables remain an effective tool in this endeavor, as demonstrated in figure 1.

Second, risk is a function of the balance between threats to mission accomplishment and available resources to allocate against that threat. This distinction is critical in facilitating risk dialogue. Commanders make decisions on the allocation of resources on the battlefield. In much the same way as the likelihood of occurrence and magnitude of impact dictate the weight of the threat identified, those criteria apply to the strength of the capability available. Effective risk analysis must weigh the balance between what the unit has, what it is attempting to accomplish, and what threatens the acceptable outcome.

Finally, to accept that risk is connected to, but not the same as, threats and capabilities is to acknowledge

that risk is outcome dependent. If there is no desired outcome, there is no risk to assess and accept. In simple games like poker, this is easily understood. A player's hand will always have a mathematical probability of winning and losing. To play a hand with a 70 percent chance of winning (acceptable outcome) still incurs a 30 percent risk of loss (unacceptable outcome). While the likelihood of drawing a bad card in the river contributes to the assessment, it isn't the sole factor on which the player decides. There are no mathematical solutions in combat operations. Commanders and staffs must strive toward sufficient information and the minimization of assumptions to make holistic assessments on whether to move forward with their current course of action.

With these factors in mind, *risk* is better defined as *the imbalance between capabilities and threats signaling an operation may result in an unacceptable outcome*. A commander—based on training, education, and experience—determines how much risk they are willing to tolerate. Figure 2 illustrates these relationships. It's important to note that there is a graduated color scale on the double-sided arrow expressing a commander's risk

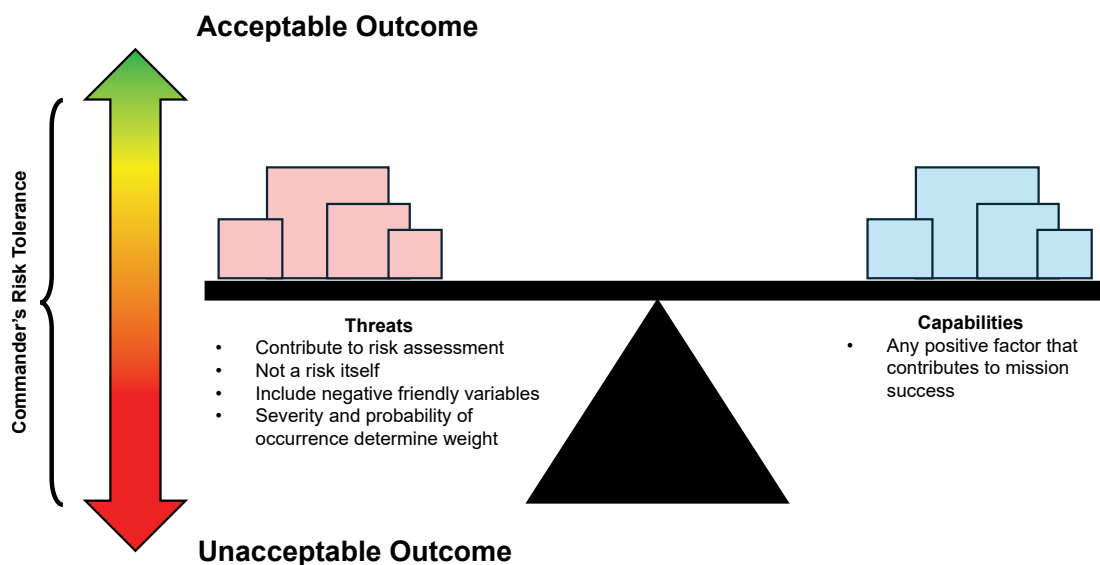
tolerance. *Risk tolerance* is defined as *the commander's willingness to move forward with a given course of action given its potential to result in an unacceptable outcome*. Risk tolerance will change based on the mission, the operational environment, and different commanders. The color scale, like risk-seeking or risk-averse decisions, is situationally dependent.

In this framework, risk mitigation is accomplished in three ways. First, action can be taken to reduce the severity of the impact or likelihood of the occurrence of a particular threat. For example, if a unit is concerned with enemy signals intelligence collecting on radio traffic and implements a communications window to limit traffic, they reduce the severity of the impact of the threat.

Second, a risk can be mitigated by increasing a capability to counterbalance the threat. Using the previous example, if the unit opted to move their communications to an alternate system that the enemy did not have the capability to intercept, they've mitigated the risk by increasing the impact of an existing capability.

**Risk:** The imbalance between capabilities and threats signaling an operation may result in an unacceptable outcome.

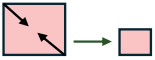
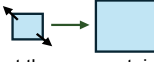

**Risk Tolerance:** The willingness to move forward with a given course of action given its potential to result in an unacceptable outcome.

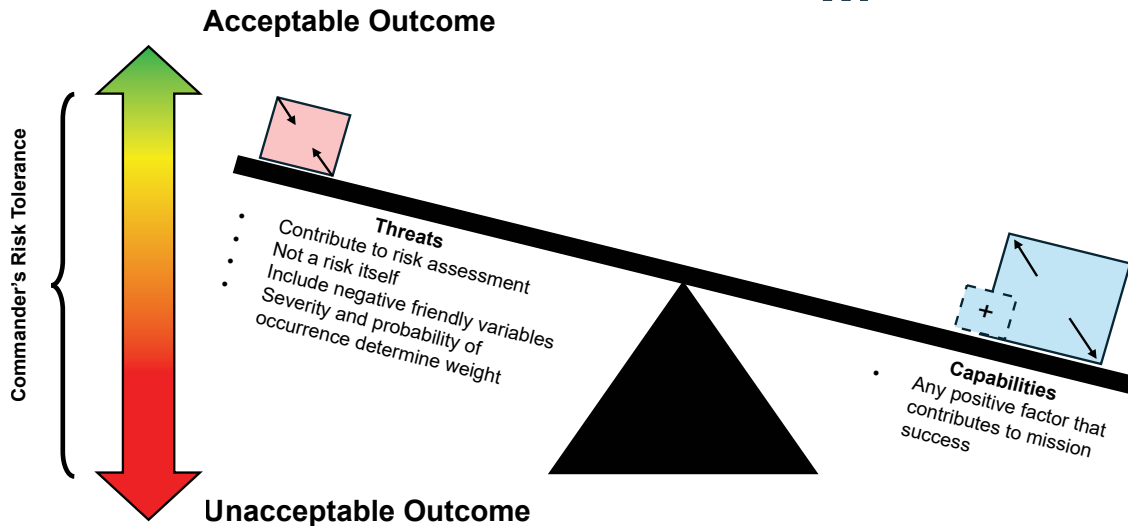


(Figure by author)

**Figure 2. The Risk Scale**

To mitigate risk is to:

1. Reduce the severity of the impact or likelihood of occurrence of a particular threat. 
2. Increase a capability to counter-balance the threat. 
3. Deceive an enemy about the effectiveness of a threat they present, increase the perceived capability of a friendly force, or present the appearance of a capability that does not exist. 



(Figure by author)

**Figure 3. Risk Mitigation**

Third, tactical or military deception can be employed to change enemy perceptions of the effectiveness of their own capabilities (threat to friendly forces) or to overemphasize a friendly capability. Commanders can employ deception in many ways, most commonly by tasking a subordinate unit to achieve a desired effect on the enemy. If deception assets, like decoys, are available, they can be employed to achieve that end.

Finally, the identification of opportunities is an essential outcome of successful analysis. As presented in figure 3, opportunities are identified in four ways. First, the leader can identify the features of a threat that can be leveraged as a capability. For example, if the enemy begins to mass forces on a friendly unit's boundary line, they threaten friendly maneuver. However, the same mass that threatens friendly forces also presents a valuable target for indirect fires. In this instance, a portion of the threat's weight is carved out and seized by friendly forces.

Second, a unit can add a capability that provides an advantage that wasn't previously available. Using the previous example, the threatened unit can request

additional long-range precision fires or priority for air support to tip the scale in their favor.

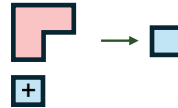
Third, an opportunity can be derived by identifying a threat common to both friendly and enemy forces that a friendly capability can better overcome. The emphasis on "owning the night" is rooted in the sense of opportunity derived from superior night sensing technology.

Finally, the commander can employ deception to provide a false read of capabilities or to misdirect the enemy's attention. Enemy deception operations can also tip the scales toward a perceived unacceptable outcome. Commanders and their staffs must take careful note of their assumptions (both friendly and enemy) and fight to make them facts. A perceived threat may be smaller in magnitude than assumed due to enemy deception operations. It's important to note that all opportunities have a temporal component. An opportunity cannot be permanently exploited. Figure 4 illustrates this relationship.

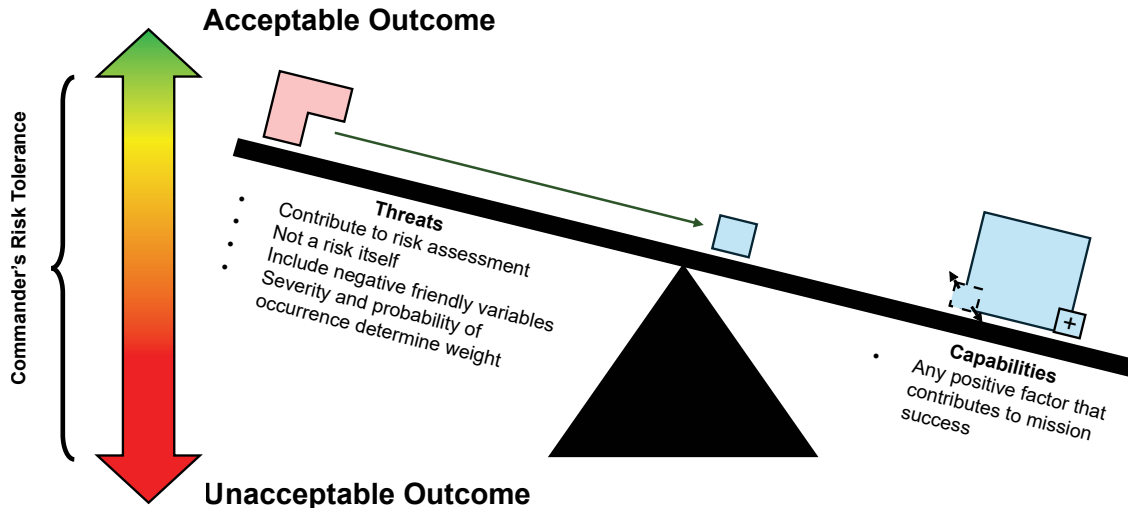
Reframing the model employed to analyze risk is the first step toward clarifying risk dialogue. By establishing a balanced lens through which to engage with

To identify an opportunity is to:

1. Identify the features of a threat that can be leveraged as a capability.
2. Add a capability that provides an advantage not previously available.
3. Identify a common threat that a friendly capability can better overcome.
4. Deceive an enemy to increase the perceived effectiveness of a friendly capability or convince the enemy of a capability that does not exist.



\*Note — there is a temporal component to all opportunities. You cannot permanently exploit an opportunity.



(Figure by author)

**Figure 4. Opportunity Seeking**

the concept of risk—accounting for outcomes, threats, and capabilities—leaders at echelon better understand and engage with the complexities and uncertainties of the modern battlefield. The next challenge is employing the risk framework in practical scenarios.

## Integrating the Risk Framework into Commander Dialogue

As previously stated, risk dialogue is a critical forum for commanders to negotiate with their higher headquarters to gain resources, create shared understanding, and synchronize assets to maximize their value against the enemy. Accomplishment requires recognizing two concepts. The first concept is an established set of criteria for the decisions that only commanders can make. The second requirement is a clear delineation of which leader owns the risk at each echelon.

Commanders are ultimately responsible for making decisions that control the allocation of resources across their formations. It's important to recognize that this statement isn't a complete representation of what commanders do. They have incredible responsibility and authority. But when a commander decides, they are

deciding on resource allocation to accomplish an objective and achieve a desired outcome. To *decide*, then, is to *align and allocate resources in the pursuit of achieving a future state more acceptable than the current one*. When organizing and synchronizing operations across time, space, and purpose; a commander can make five types of decisions:

1. Change a subordinate unit's mission by modifying the task and purpose they have been given.
2. Change a boundary within their battlespace.
3. Change the task organization of a subordinate unit.
4. Reallocate a finite commodity between subordinate units (e.g., repair parts, funding).
5. Remove a subordinate leader from position.

Categorizing command decisions is important for three reasons. First, categorizing decisions simplifies the risk assessment process. It takes risk conversations from the realm of the conceptual to the practical. Second, categorization sets expectations for which threats contribute to legitimate risk for subordinate staffs. It allows staff identification of the most critical problem the unit must solve. Uneven terrain and environmental considerations may certainly be threats, but if a commander's decision

cannot address them, then the subordinate wasted an opportunity to bring forward a legitimate issue. Finally, categorizing a commander's decisions allows for risk segmentation at echelon. This formalizes and clarifies the doctrinal categories of risk to mission and risk to force.

Joint planning doctrine defines risk to mission (operational risk) as "the current force's ability to achieve objectives in the national military strategy (NMS) with acceptable human, material, and financial costs" and risk to force (force management risk) as "a Service or joint FP's [force provider] ability to generate trained and ready forces within established rotation ratios and surge capacities to meet mission requirements."<sup>3</sup> At the operational and strategic level, these definitions are suitable and clear. However, the risk-to-mission and risk-to-force framework do not scale down to the tactical level. These terms also become too easily intertwined, leading to difficulty in differentiating and developing compelling risk statements for both categories. At some point, every meaningful risk to force becomes a risk to mission.

To clearly delineate between the risk categories, the following definitions would be more helpful. First, *risk to force* should be defined as *the most significant threat to the subordinate unit's mission accomplishment that a commander can resolve with a decision made at their level and without additional resources from their higher headquarters*. In this definition, the commander has resolved the threat to an acceptable outcome but still briefs their higher headquarters on the risk to give the senior commander the opportunity to weigh in on the decision with guidance or to provide additional resources held at their level to better reduce the risk. To provide a nontactical example, if division-level training guidance directed that all companies be live-fire certified but there were not enough available training days to accomplish all gates to live fire, an effective risk to force statement follows:

*The risk to force is a shortfall of available training days to complete all live-fire gates prior to achieving company live-fire certification. To overcome this risk, we removed section-level qualifications from the training progression. This modification to the training schedule is not assessed to degrade crew proficiency and frees up the necessary time required to achieve company-level live-fire certification.*

Second, *risk to mission* is better defined as *the most significant threat to the higher headquarters' mission accomplishment that a commander cannot resolve without a decision made by the senior commander*. With this definition, the risk cannot be resolved by the commander at their level. If left unresolved, the risk to mission threatens the achievement of an acceptable outcome for the senior headquarters. The senior commander must make a decision at their echelon to resolve it. The subordinate commander is responsible for providing a recommended decision to their senior for consideration. If the senior commander cannot mitigate the risk with their resources, the risk aggregates up to the next echelon. An example of a risk to mission under this definition is provided:

*The assessed risk to mission is a lack of available forces to execute the battalion's specified tasks of seizing Objective Bears and Objective Chargers. Recommend a change of task to securing Objective Bears in order to allocate additional personnel to the seizure of Objective Chargers.*

Categorizing decisions and using them as the criteria to delineate levels of risk provides a logical framework with which to enrich a commander's risk dialogue. In the examples provided, the subordinate commander informs their senior commander in real time, enabling the senior commander to work through the proposed mitigation strategy. Outcomes are at the forefront of the dialogue, and threats are balanced against capabilities.

## Conclusion

The current approach to risk assessment lacks the necessary depth and focus to facilitate effective dialogue between commanders at echelon. By adjusting focus from a downward perspective on the threats a unit faces to an eyes-up approach oriented on the desired outcome, the definition of risk and its components can be clarified for leaders at all levels to understand. Extending this approach to the clear articulation of risk at each echelon provides a framework for more useful dialogue that creates shared understanding and ensures resources are properly aligned to achieve desired outcomes. ■

*The author would like to extend sincere gratitude to the leaders and colleagues who dedicated time to the development of the ideas presented.*

## Notes

1. Field Manual (FM) 1-02.1, *Operational Terms* (US Government Publishing Office [GPO], 2024), 66.
2. Chairman of the Joint Chiefs of Staff Manual 3105.01B, *Joint Risk Analysis Methodology* (US GPO, 2023), B-1.
3. Joint Publication 5-0, *Joint Planning* (US GPO, 2025), I-16.

US ISSN 0026-4148