**Strengths and Weaknesses of Risk Management as the Primary Tool for US Military Strategic, Tactical and Operational Decision Making:**

**Will the Enterprise Risk Assessment Model, Composite Risk Management and Associated Techniques Provide the Predicted Benefits?**

Chris. W. Johnson,

Glasgow Accident Analysis Group,
Department of Computing Science, University of Glasgow, Scotland, UK.

Email: Johnson@dcs.gla.ac.uk; http://www.dcs.gla.ac.uk/~johnson

Keywords: Safety; Composite Risk Management, ERAM, Risk Assessment; Military Systems Engineering.

Abstract

Risk management provides the most important single framework for both strategic and tactical decision making across the US Military. The annual statement of the Chairman of the Joint Chiefs of Staff to Congress now uses notions of likelihood and consequence to assess the nation's military preparedness. At the same time, pressure from the US General Accounting Office and the Quadrennial Defense Review, has encouraged the Department of Defense to restructure its work around an Enterprise Risk Assessment Model (ERAM). At an operational level, Composite Risk Management (CRM) has been introduced as the main framework for decision making. For example, Field Manual 5-19 extends the scope of risk assessment to cover training exercises, combat and peacekeeping operations, as well as the hazards associated with off-duty activities including terrorist attack and the use of privately owned vehicles. This paper argues that risk management is not a panacea. For example, it is unclear whether the Department of Defense can achieve the culture shift that is necessary before risk analysis might 'revolutionize' their business strategy. At a tactical level, there is also a danger that enemy forces could learn to exploit systematic biases in decisions that are informed by particular risk assessment techniques. At an operational level, it is unclear whether leaders in the field can accurately collate and then communicate the products of a hazard analysis given the operational constraints of FRAGOs (Fragmentary Orders). Finally, there is a high-level concern over confirmation and attribution biases. These arise when the proponents of techniques like Composite Risk Management argue that adverse events would have been avoided if only personnel had used the new techniques. Such judgments under-estimate how difficult it is to apply new risk management methods in the hostile operational environments that often confront military personnel.

## Introduction

Risk management offers numerous benefits for resource allocation and for planning under uncertainty. It provides tools and techniques that have been validated across a range of safety-critical industries (Johnson, 2003). The concepts of hazards, of consequent and likelihood, of detection factors, exposure and of mitigation can all easily be applied to the military domain. Not only do they apply at the operational level, where leaders can analyze the hazards associated with tasks during a combat mission. The same concepts can also be applied to consider the risks associated with peacekeeping operations and with the hazards faced by off-duty personnel, including privately operated vehicles and terrorist attacks. At a more strategic level, risk management also provides a framework for acquisition and procurement policy. Rather than considering the hazards associated with particular operations, planners consider the hazards that might arise during particular development programs. They can evaluate project risks in terms of the likelihood and consequences of failing to meet service requirements on time and to cost. At the very highest level, risk management techniques can be used to analyze the threats posed by particular geo-political developments. Mitigation strategies can be devised to address these threats so that the necessary political support can be obtained to prepare for future challenges in an uncertain environment.

The 'Big Picture': Political Risk Mitigation

US military policy is strongly influenced by the risk assessments that are coordinated by the Chairman of the Joint Chiefs of Staff (CJCS) and presented to Congress each year. In 2005, General Richard B. Myers reported that the US was at "higher risk" of less swiftly and easily defeating potential foes. Commanders were reported to have increasing "difficulty meeting the higher standards imposed on them by conflicts around the world, including the military effort against terrorism" and that the overall "risk has increased but is trending lower" (White and Tyson, 2005). In 2007, General Peter Pace reported that the wars in Iraq and Afghanistan had increased the risks in defending the nation from 'moderate' to 'significant'. The importance of these high-level assessments does not stem from any underlying quantitative calculation but from their political and public impact. Defense Secretary Robert Gates was required to explain to Congress how the Pentagon would mitigate the increased risks identified in the statements made by Pace just as his predecessor had been required to report on Myers' assessment.

CJCS reports are drafted at an extremely high level of abstraction. They cannot easily inform more detailed aspects of US Defense policy (Frier, 2007). The US General Accounting Office (2005) have argued that is a need for more detailed risk-based approaches to strategic investment if the Department of Defense is to respond to increasing financial pressures in an uncertain security environment. They have identified the lack of comprehensive risk management strategies as 'an emerging challenge for the federal government'. Donald Rumsfeld made similar points in his most recent Quadrennial Defense Review (QDR). The Secretary of Defense must, by law, conduct the QDR at the start of each new administration. The purpose is to consider threats, strategy, force structure, readiness posture, military modernization programs, defense infrastructure, and information operations and intelligence. The 2006 QDR included the observation that "the unpredictable nature of Defense programs can be traced to instabilities in the broader acquisition system. Fundamentally reshaping that system should make the state of the Department's major acquisition programs more predictable and result in better stewardship of the U.S. tax dollar."

The US Department of Defense's Business Transformation Agency (2007) responded by developing the Enterprise Risk Assessment Model (ERAM) to identify and mitigate risks during acquisitions programs. A 'risk assessment team' spends two weeks reviewing existing project documentation. This analysis is then used to inform a series of more focused interviews with program stakeholder that last from two to three days. A further period of two weeks is then used to review material, formulate additional questions and devise a risk mitigation proposal. The program manager helps to review the initial findings before a final mitigation strategy is disseminated to program participants. ERAM outputs are intended identify vulnerabilities, propose solutions, and provide an action plan to reduce program risks. The intention is to ensure that DoD projects deliver *capabilities* rather than focusing on particular technologies. For example, several different approaches may be trialed in order to spreads the risks associated with the failure of any particular technological 'solution'.

A number of caveats can be raised about the ERAM approach. A capability-based program that spreads development risk between alternate technologies can also lead to resource starvation and under-investment in key areas. It can increase the uncertainty for companies deciding whether or not to invest in innovative approaches. It also remains to be seen whether or not individual initiatives can have the 'root and branch' impact advocated by the GAO. One reason for this is that ERAM is being introduced in a piecemeal fashion. In April 2006, the Under-Secretary for Defense (Acquisition, Technology, and Logistics) approved a trial of ERAM focusing initially on the Defense Integrated Military Human Resources System, General Fund Enterprise Business System, and Integrated Data Environment/Global Transportation Network Convergence projects. These initiatives were chosen because they are typical of the business critical ICT applications that often pose particular problems for public agencies acquisition. The validation bodies, the Investment Review Boards (IRBs) and the Defense Business Systems Management Committee (DBSMC), have still to publish their analysis of the risk-based approaches within ERAM. A number of further concerns center on the piecemeal introduction of such initiatives. For example, previous Department of Defense initiatives to introduce risk management into the security of ICT applications have failed to achieve 'critical mass':

> "…there is no specific Defensewide policy requiring vulnerability assessments or criteria for prioritizing who should be targeted first. This has led to uneven application of this valuable risk assessment mechanism. Some installations have been tested multiple times while others have never been tested. As of

> March 1996, vulnerability assessments had been performed on less than 1 percent of the thousands of defense systems around the world. DISA and the military services recognize this shortcoming, but state that they do not have sufficient resources to do more. This is a concern because vulnerabilities in one part of Defense's information infrastructure make the entire infrastructure vulnerable" (GAO, 2006b)

Although ERAM is arguably the most visible of the risk assessment projects within the US DoD acquisition program, it is not the only initiative that adopts this approach. In particular, it can be seen as part of a more general response to the principles encapsulated in Department of Defence Directive 5000.1 and Instruction 5000.2. These advocate the use of risk-based approaches across all procurement activities, including weapon systems and automated information systems (AISs). Instruction 5000.2 is intended to establish a management framework to translate 'mission needs and technology opportunities' into 'stable, affordable and well managed' acquisitions programs. Again, risk assessment is advocated as a key tool in achieving these objectives. The gradually development of 'evolutionary' prototypes or demonstrators will help end-users, testers and developers flush out any risks that were not identified during the inception stage. This was intended to satisfy address GAO (2006c) concerns that pilot programs should be limited to low-cost, low-risk prototypes. The evolutionary approach advocated in 5000.1 and 5000.2 helps to explain the piecemeal application of ERAM, described in previous paragraphs.

Lifecycle Risk Management from Procurement to Deployment and Decomissioning

Public and political attention also increasingly focuses on the ecological impact of military operations and this has created a role for risk assessment in the decommissioning of military systems. For example, the US army is responsible for restoring Formerly Utilized Sites Remedial Action Program (FUSRAP) sites. FUSRAP addresses radiological contamination generated by activities of the Manhattan Engineering District (MED) and the civilian Atomic Energy Commission (AEC) during the atomic weapons programs of the 1940s and 1950s. Responsibility for managing the clean-up of many of these sites was initially held by the MED and AEC on behalf of the Department of Energy. However, in October 1997, Congress transferred overall responsibility from the Department of Energy to the US Army Corps of Engineers. The Corp was faced with immediate actions to clean up low levels of uranium, thorium and radium that remained on FUSRAP sites. Under the 1997 legislation, responsibility for the long-term management of the sites can be returned to the Department of Energy once the all short-term clean-up has been completed. Risk assessment is a central element for the Corp, as it addresses the land use for former military sites under FUSRAP. These areas contain levels of radioactivity above current guidelines. However, they are not considered to pose an immediate health risk to the public or to the environment given *current land uses*. People should not suffer adverse effects because they are not exposed to the excess radiation levels for long periods of time. However, risk assessments have to be repeated each time there is any proposed change in the usage of a FUSRAP site. Under the program, each area is cleaned to levels acceptable for the projected future use for the land such as residential development, industrial operations, or recreational use.

The US Army Corp of Engineers provides a Factsheet for personnel that is intended to deliver a general introduction to the topic of risk assessment (US Army Corps of Engineers, 2007a). As might be expected from the previous paragraphs, the focus of this document is on redevelopment of former military sites. Hence, risk is defined in a very application specific way as: Risk = Exposure x Toxicity. In addition, the Corps guidance reinforces the previous comments about the difficulty of validating risk assessments in a section entitled 'Uncertainty'. This argued that risk assessment is not a perfect science and that there is a 'great deal of uncertainty associated with risk assessment'. The proposed solution is for Army engineers to deliberately adopt a conservative approach that errs on the side of safety when calculating potential risks to people. This introduces further problems because conservative approaches to risk assessment, typically, incur additional costs. In the long term, these costs cannot always be justified and are eroded by political and commercial pressure to justify risk assessments that are perceived to stand in the way of other interests.

The US Department of Defense recognizes the limited nature of such guidance and has, therefore, supported several initiatives to develop more sophisticated, risk based approaches to decommissioning (Rury et al, 2007). For example, Table 1 illustrates part of the Risk Based Decision Protocol for the reuse of military sites. As can be seen, a key element in this approach is to provide metrics for calculating the risks posed to human health in relation to the 'background levels' of risk that might be found in other comparable areas. This creates a host of ethical and

methodological issues. As can be seen from the column on the left, the financial benefits from reuse must also be considered in this risk-based approach. Full scale remedial actions would only be justified under this approach for former military sites that have a high reuse value and where the background risk was defined to be 'unacceptable'.

| | **Incremental Human Health Risk Relative to Background** | | |
|---|---|---|---|
| **High $$ Value Reuse: Benefits > 10x Cost of Site Remediation and/or Risk Management** | No Site Remediation: Implement Reuse Option without Prior Cleanup, unless Site Incremental Ecological Risks Drive Cleanup Requirements | Selective Remediation and/or Health Risk Management: Implement Reuse Option with Worker/Resident Protection and Monitor Public Health | Full Scale Remediation: Remediate Site, Attain Background Risk Levels, and Implement Reuse Option without a Public Health Risk Monitoring or Prevention Program |
| **Moderate $$ Value Reuse: Benefits < 10x Cost of Site Remediation and/or Risk Management** | No Site Remediation: Implement Reuse Option without Prior Cleanup, unless Ecological Risk Drives Cleanup Requirements | Selective Remediation and/or Health Risk Management: Refine Analysis of Economic Benefits versus Health Risks to Assess Need for Remediation and/or Health Risk Mitigation | Focus Remediation on Hot Spots: Selectively Remediate Hot Spots to Acceptable Levels of Residual Health Risk and/or Integrate Worker/Public Health Protection/Monitoring into Reuse Plan |
| **Low $$ Value Reuse: Benefits < Cost of Site Remediation and/or Risk Management** | No Site Remediation: Implement Reuse Option without Prior Cleanup, unless Ecological Risk Drives Cleanup | Manage Health Risks: Institutional Controls to Ban Residential Uses and Minimize Long-term Human Exposures from Commercial Activity | Prevention of Human Exposure: Physical and Institutional Controls on Access to Preclude Short and Longterm Human Exposures |
| | **Acceptable Risk: 1x to 5x Background Risk** | **Marginal Risk: 5x to 10x Background Risk** | **Unacceptable Risk: > 10x Background Risk** |

**Table 1:** Risk Based Decision Protocol for Reuse of Military Sites

The risk matrix in Table 1 determines the interventions and remediation actions that are considered to be 'cost effective' for a particular site. This is a controversial approach to ecological management. The assessment of monetary benefit from restoration projects is very subjective. Local populations often have very different perceptions of both the risk exposure and the reuse values that lie at the heart of this technique. In order to help ensure the consistency of any risk analysis, the U.S. Department of Defense through the Army's Installation Restoration Research Program (IRRP), the U.S. Army Engineer Research and Development Center (ERDC) and the US Army Center for Health Promotion and Preventive Medicine (USACHPPM) developed the Adaptive Risk Assessment Modeling System (ARAMS) (US Army Corps of Engineers, 2007). This software exploits land-use modeling facilities with a database of previous impact studies to estimate the human and ecological risks associated with Military Relevant Compounds (MRCs) and other contaminants. The challenges that arise during the development and use of ARAMS cannot be underestimated. Some of these relate to scientific uncertainty, for example over the long term effects of PCB contamination. It is difficult to estimate the level of uptake of contaminants given a level of exposure in redeveloped sites. In consequence both civil and military redevelopment plans often rely upon risk 'scenarios' or storyboards that describe particular, known uptake mechanisms without providing quantitative assessments of the extent of a potential problem either for human or wildlife exposure.

Operational Risk Management

The principles and language of risk management have influenced US strategic and political decision making. They are increasingly being used to regulate business engineering and military procurement. The same techniques also guide the planning and execution of tactical military operations. For example, US Army Field Manual 3-04.513 deals with the battlefield recovery and evacuation of aircraft (Department of the Army, 2000). Appendix D of the

Field Manual explicitly considers the risk management process and risk assessment techniques that must be used when planning and conducting such operations:

> "Risk management is a commonsense tool that leaders can use to make smart risk decisions in tactical and everyday operations. It is a method of getting the job done by identifying the areas that present the highest risk and taking action to eliminate, reduce, or control the risk. It is not complex, technical, or difficult. It is a comparatively simple decision making process, a way of thinking through a mission to balance mission demands against risks".

This 'common sense tool' can be deceptively difficult to use under the time pressures of combat. Under FM3-04.513 Commanders must: select the best risk-reduction options that their staff provide; accept or reject residual risk, based on perceived benefits; recommend appropriate control measures; train and motivate leaders at all levels to effectively use risk management concepts; ensure that risk controls are integrated into plans and orders; ensure that unnecessary safety restrictions are eliminated to maximize training and combat effectiveness; maintain a total commitment to mission accomplishment and the welfare of subordinates; use the risk management process to identify, assess, and control hazards for their mission; report risks beyond their control or authority to their superiors for resolution. At the same time, FM3-04.513 places responsibilities on all soldiers who must: understand, accept, and implement risk reduction guidance and the concept of risk management and assessment; maintain a constant awareness of the changing risks associated with the operation; make leaders immediately aware of any unrealistic risk reduction procedure and report risks beyond their control or authority to their superiors for resolution. In order to help personnel meet these requirements, FM3-04.513 provides a five step process for risk management:

1. *Identify hazards* to the force. Consider all aspects of current and future situations, environments, and known historical problem areas.
2. *Assess hazards* to determine risks. Assess the impact of each hazard in terms of potential loss and cost based on probability and severity.
3. *Develop controls and make risk decisions*. Develop control measures that eliminate the hazard or reduce its risk. As control measures are developed, risks are re-evaluated until the residual risk is at a level where the benefits outweigh the cost. The appropriate decision authority then makes the decision.
4. *Implement controls* that eliminate the hazards or reduce their risks. Ensure the controls are communicated to all involved.
5. *Supervise and evaluate*. Enforce standards and controls. Evaluate the effectiveness of controls and adjust/update as necessary. Ensure lessons learned are fed back into the system for future planning.

The field manual advocates the use of risk matrices in assessing hazardous operations. This can improve the objectivity of a risk assessment if the same matrices are shared between groups of assessors. Such an approach is 'nearly always more effective than intuitive methods in identifying the extent of risk', although 'each unit should develop its own risk assessment matrix with applicable major operational events'. Table 2 illustrates the generic risk matrix presented in Army Training Circular 1-210 (Department of the Army, 1995).

| | | **Hazard Probability** | | | | |
|---|---|---|---|---|---|---|
| | | **Frequent** | **Likely** | **Occasional** | **Seldom** | **Unlikely** |
| **Effect** | **Catastrophic** | Extremely High | Extremely High | High | High | Medium |
| | **Critical** | Extremely High | High | High | Medium | Low |
| | **Moderate** | High | Medium | Medium | Low | Low |
| | **Negligible** | Medium | Low | Low | Low | Low |

**Table 2:** US Army TC 1-210 Risk Assessment Matrix

The individual elements of the table are familiar to most engineers who have worked on safety-critical applications. In terms of effects, 'Catastrophic' is interpreted by the US Army to include outcomes that result in death or permanent total disability, system loss, major property damage. 'Critical' effects include permanent or partial disability, temporary total disability in excess of three months, major system, damage, significant property damage. 'Moderate' effects include minor injury, lost workday accident, compensable injury or illness, minor property damage. Finally, 'negligible' outcomes include first aid or minor supportive medical treatment, minor system impairment. The generic risk matrix presented in TC 1-210 is structured around similar qualitative statements about probabilities of adverse outcomes. The term 'frequent' relates to events that occur often in a soldier's career or in the service life of equipment. In addition, it is assumed that all soldiers or items are exposed to a hazard or that the hazard may be continuously experienced. 'Likely' refers to events that occur several times in a soldier's career or the service life of equipment. Again, it is assumed that all soldiers or inventory items are frequently exposed to a hazard. The term 'occasional' in the Army guidance is interpreted to refer to events that are expected to occur at some time in the career of an individual soldier or in the lifetime of an item of equipment. Again, it is assumed that all soldiers and items are exposed to the hazard but that this may occur 'sporadically or several time' during service. 'Seldom' refer to events which are possible during a soldier's military career or during the lifetime of equipment. All soldiers or items of inventory can be exposed to a hazard but the chances of occurrence for any individual are remote. However, such seldom events are 'expected to occur sometime in inventory service life'. The term 'unlikely' refers to events that are assumed not to occur during the service of an individual or item of equipment. They are possible but improbable and occur very rarely.

'Extremely high-risk' hazards prevent units from accomplishing a mission. The term 'high risk' in contrast, is used to describe hazards that significantly degrade 'mission capabilities in terms of the required mission standards'. 'Medium risk' hazards degrade mission capabilities in terms of the required mission. Finally, the term 'low risk' refers to hazards that have little or no impact on overall mission accomplishment. The terms for likelihood and consequence in Table 2 are intended to help leaders identify the risk levels for components of critical missions. In the case of TC 1-210, for example, the risk associated with securing a battlefield landing site might be assessed separately from the hazards associated with rescuing the crew and from the dangers associated with retrieving the aircraft. In addition, leaders must consider the interaction between these components and the mission as a whole. For example, one phase might be considered to be particularly high-risk but this assessment could be 'diluted' if the other components had little likelihood of adverse consequences so that the overall mission analysis might be at a more moderate level of risk.

US Army guidance stresses that the levels of risk shown in Table 2 should be calibrated for the operations and hazards faced by particular units. Tables 3 and 4 illustrate the more detailed risk assessment tools that have been proposed to support rotary wing operations. As can be seen, the first page identifies a number of factors that might contribute to the risks associated with any mission. For example, the first box labeled '1. Supervision CMD/CONTROL' provides a means of assessing the risks associated with operations involving personnel from the same unit or from an attached unit. Particular hazards stem from devolved lines of command hence a higher risk value is associated with operations involving crews from attached units than those for which all staff are drawn from the same command. This section of the form also associates a higher level of command and control risk with operations after dark. As can be seen, a mission involving attached units at night would be assigned an initial risk value of 4. In contrast, a mission that was conducted by an integrated unit in daylight would only score a risk value of 1. A companion paper explains the high-levels of risk associated with nighttime operations (Johnson, 2004). For now it is sufficient to observe that the US Army has identified 'human-error accelerator profiles' from its accident data. An example of a high-risk mission profile would be an NOE ('nap of the earth') flight using night vision goggles with less than 23% and 30 degrees of illumination. The accelerator in this case would be lack of illumination and limited visual field making crew scanning errors more likely to occur. Hence, these factors may be given a high risk value weighting within the matrix used by any unit that is likely to perform such an operation.

Complex missions can be assessed by breaking them down into a small number of activities using Mission Essential Task Lists (METL). Risk assessment matrices, such as those shown in Tables 3 and 4, help to identify the hazards associated with each sub-task. By summing the risk values for the hazards associated with each mission component, it is possible to form a partial ordering of those tasks that contribute most to overall risk. It is these sub-tasks that become the focus for risk reduction and mitigation. This relatively simple approach provides considerable flexibility. For example, an otherwise low risk mission might have a significant increase in the overall risk value if,

for instance, one of the crews had less than 25 hours in the area of operation. Leaders might then intervene , for instance, by introducing a highly experienced crew member into the operation.

The overall mission risk is obtained by summing the hazards for each stage of the mission. The total can then be assigned to a particular risk level. For example, Tables 3 and 4 associate 'Low Risk' with risk values less than 16. Medium risk operations range between 16 and 28. High risk operations are associated with scores of 29 and above. In each case, commanders must seek additional levels of authorization before embarking on a mission. For example, company level approval must be provided for medium risk operations, while battalion commanders must support high risk plans. In this example, extremely high-risk operations associated with the use of night vision equipment must be approved at brigade level.

It is clearly important to validate the risk values that are embedded within a risk matrix. If this were not the case then there is a danger that risk assessments would be unnecessarily conservative – in other words mission success might require an unnecessary level of resources in order to mitigate low levels of risk. These resources might have been better deployed on other operations. Alternatively, incorrect risk values might persuade commanders to accept hazards that threaten both mission success and the resources that are deployed to perform a particular operation. It is for this reason that risk matrices must be carefully monitored by comparison which outcome data from accident investigations and from training exercises, for example using the Army Safety Risk Management Information System and the Army Safety Management Information System-2 (ASMIS-2).

## ROTARY-WING RISK ASSESSMENT MATRIX

**1. SUPERVISION (Risk Value/Mission)**

| CMD/CONTROL | VALUE | TACTICAL DAY/NIGHT | |
|---|---|---|---|
| Parent Unit | 1 | 1 | 2 |
| Attached | 2 | 3 | 4 |

**2. PLANNING (Risk Value/Time)**

| GUIDANCE | IN-DEPTH | ADEQUATE | MINIMAL |
|---|---|---|---|
| Vague | 3 | 4 | 5 |
| Implied | 2 | 3 | 4 |
| Specific | 1 | 2 | 3 |

**3. CREW SEL/PC (Risk Value/Flt Hrs)**

| TIME IN AO* | TOTAL TIME >2000 | <2000 | <1000 | <500 |
|---|---|---|---|---|
| <25 | 3 | 4 | 5 | 6 |
| >50 | 2 | 3 | 4 | 5 |
| >50 | 1 | 2 | 3 | 4 |

**4. CREW SEL/PI (Risk Value/Flt Hrs)**

| TIME IN AO* | TOTAL TIME >2000 | <2000 | <1000 | <500 |
|---|---|---|---|---|
| <25 | 3 | 4 | 5 | 6 |
| >50 | 2 | 3 | 4 | 5 |
| >50 | 1 | 2 | 3 | 4 |

**5. CREW SEL/ADD (Risk Value/Flt Hrs)**

| TIME IN AO* | TOTAL TIME >2000 | <2000 | <1000 | <500 |
|---|---|---|---|---|
| <25 | 3 | 4 | 5 | 6 |
| 50 | 2 | 3 | 4 | 5 |
| >50 | 1 | 2 | 3 | 4 |

**6. ALL CREW MEMBERS ARE CREW COORDINATION TRAINED**

| | |
|---|---|
| No | +2 |
| Yes | 0 |

**7. ALL TASKS REQUIRED ON THIS MISSION ARE SUPPORTED BY THE UNIT MISSION ESSENTIAL TASK LIST (METL)**

| | |
|---|---|
| Yes | 0 |
| No | 5# |

#Requires bn cdr approval.

**8. CREW ENDURANCE (Risk Value/Flt Hrs)**

| QUALITY OF REST | >8 HRS | 6-8 HRS | <6 HRS |
|---|---|---|---|
| Field | 2 | 6 | 10 |
| Garrison | 1 | 4 | 10 |

Add 2 for missions flown during the last half of the duty day.

**9. COMPLEXITY (Value/Condition)**

| TYPE OF MISSION | VMC D | VMC N | NVG | IMC HOOD |
|---|---|---|---|---|
| Multiship | 2 | 6 | 4 | NA |
| Sling load | 2 | 3 | 5 | NA |
| Stabo/Rappel | 1 | 2 | 4 | NA |
| Terrain Flt | 1 | 3 | 2 | NA |
| Paradrop | 2 | 2 | NA | NA |
| Routine | 1 | 2 | 2 | 3 |
| NOE | 2 | 8 | 4 | NA |
| MTP | 3 | 5 | NA | NA |
| Maint Recovery | 3 | 5 | NA | NA |

**10. WEATHER****

(Risk Value/Ceiling/Visibility)

| | <1000/3 | <700/2 | <500/1 | >1000/3 |
|---|---|---|---|---|
| D | 3 | 4 | 6 | 1 |
| N | 4 | 6 | 10 | 2 |
| NVG | 3 | 4 | 8 | 1 |

**11. ADDITIONAL RISK FACTORS (D, N)**

Single Pilot +4

**ADDITIONAL COMMENTS**

* Area of operations.

** Visibility values are given in miles.

**Table 3:** Example of a suggested format for a rotary-wing risk assessment matrix (US Army TC 1-210)

## ROTARY-WING RISK ASSESSMENT MATRIX

| 12. NVG CREW SEL/PC (Total NVG Time) | 13. NVG CREW SEL/PI (Total NVG Time) |
|---|---|
| >150 <150 <100 <50 <25 | >150 <150 <100 <50 <25 |
| 1 2 3 4 5 | 1 2 3 4 5 |
| **14. NVG CREW SEL/ADD (Total NVG Time)** | **15. PERCENT OF ILLUMINATION (NVG)** |
| >150 <150 <100 <50 <25 | 100-80 79-60 59-40 30-23 <23 |
| 1 2 3 4 5 | 1 2 3 4 5 |
| **16. MOON ANGLE (NVG)** | **17. ADDITIONAL RISK FACTORS (NVG)** |
| 90-70 69-50 49-30 <30 | |
| 0 1 2 3 | |

| RISK VALUES: DAY/NIGHT MISSIONS | | RISK VALUES: DAY/NIGHT MISSIONS | |
|---|---|---|---|
| 1. Supervision | _____ | 12. NVG Crew Selection/PC | _____ |
| 2. Planning | _____ | 13. NVG Crew Selection/PI | _____ |
| 3. Crew Selection/PC | _____ | 14. NVG Crew Selection/Add | _____ |
| 4. Crew Selection/PI | _____ | 15. Illumination | _____ |
| 5. Crew Selection/Add | _____ | 16. Moon Angle (NVG) | _____ |
| 6. Crew Coordination Trained | _____ | 17. Additional Risk Factors | _____ |
| 7. METL Task | _____ | **TOTAL NVG MISSIONS** | _____ |
| 8. Crew Endurance | _____ | **TOTAL DAY/NIGHT MISSIONS** | _____ |
| 9. Complexity | _____ | | |
| 10. Weather | _____ | **TOTAL RISK VALUE NVG** | _____ |
| 11. Additional Risk Factors | _____ | | |
| **TOTAL** | _____ | | |

| COMPUTATIONS DAY/NIGHT MISSIONS | | COMPUTATIONS NVG MISSIONS | |
|---|---|---|---|
| Low Risk | <16 | Low Risk | <25 |
| Medium Risk | 16-28* | Medium Risk | 25-40* |
| High Risk | >29** | High Risk | 41-50** |
| | | Extremely High | >50*** |

* Medium-risk missions require approval of the company commander.
** High-risk missions require approval of the battalion commander.
*** Extremely high-risk missions require approval of the brigade commander.

ADDITIONAL COMMENTS

**Table 4:** Example of a suggested format for a rotary-wing risk assessment matrix (US Army TC 1-210 continued)

In order to be useful, risk management must inform the wider processes of decision making. Once leaders have identified critical tasks, using the METL approach mentioned in previous paragraphs, and critical hazards, such as crew inexperience, it is important to develop controls that reduce overall mission risks. It may be possible to eliminate unnecessary hazards, for example, by omitting tasks or by ensuring that an experienced crew is used on an otherwise hazardous mission. FM3-04.513 argues that commanders should be presented with a series of options for risk control. Before presenting such a list, it is necessary for staff to consider any negative side-effects. For example, allocating experienced personnel to reduce the risks associated with a hazardous operation can increase the risks associated with other missions that might otherwise benefit from their participation. Similarly, deploying experienced personnel may reduce the opportunities to increase the skill set of other staff while increasing the levels

of stress and fatigue on the crews who are allocated to the mission. US Army TC 1-210 urges commanders to think through the consequences of each potential risk control and then 'visualize what will happen once the option has been implemented'.

The implementation of risk controls can involve changes to operations orders (OPORDs), standing operating procedures (SOPs), and drills or rehearsals. As might be expected, considerable emphasis is placed on communicating information about the purpose of controls, 'from the commander down to the individual soldier' so that any attempts to mitigate a risk is not inadvertently undermined. Similarly, commanders must take steps to supervise the application of risk controls. As with previous stages in the risk management processes advocated by the US Army, the superficial simplicity of the approach hides numerous detailed problems. For example, too close a monitoring may alienate staff, if they feel that their actions are under close supervision. Time may be wasted in providing evidence of controls to the point where supervision begins to undermine core mission objectives.

FM3-04.513 provides leaders with three further, general principles for guiding the management of risk during military operations:

- *Never accept an unnecessary risk.* The leader who has the authority to accept or reject a risk is responsible for protecting his soldiers from unnecessary risks. If he can eliminate or reduce a risk and still accomplish the mission, the risk is unnecessary.

- *Make risk decisions at the appropriate level.* The leader who must answer for an accident is the person who should make the decision to accept or reject the risk. In most cases, he will be a senior officer, but small-unit commanders and first-line leaders might also have to make risk decisions during combat. Therefore, they should learn to make risk decisions during training.

- *Ensure that the benefits of a prudent risk outweigh the possible cost of the risk.* Leaders must understand the possible risk and have a clear picture of the benefits to be gained from taking that risk.

The risk management process advocated in FM3-04.513 and TC 1-210 has a number of important benefits; the instantiated forms in Tables 3 and 4 are well tailored to support the missions performed by particular units. They can also be easily extended should new hazards arise. The association of risk values with particular hazards also provides considerable flexibility in identifying mitigating factors – commanders can identify and respond to those aspects of a mission that contribute most to the overall risk. Finally, by calculating the overall mission risk in terms of individual hazards, TC1-210 provides a relatively intuitive means of integrating risk assessments into the decision making processes that are associated with different levels of command.

There are also limitations with this approach to risk management. The assessment matrices are subjective. There are few guarantees that different personnel will associate the same risk values with similar hazards or that they will identify similar hazards for the same mission elements. There are further limitations. In particular, the instantiated forms in Tables 3 and 4 take little account of risk exposure either in terms of the length of mission elements or the number of personnel involved. Finally, the existing provision does not easily enable leaders to offset the risk exposure against mission benefits – where for instance, the costs to an opposing force may be so great as to justify limited exposure of friendly forces to elevated levels of risk. In other words, the straightforward approach ignores the complexity of many military operations where decisions are often guided by concerns that can be formalized within prospect theory.

Training Related Risks

Previous sections have drawn on the guidance provided by TC 1-210 to illustrate the general approach to risk management that has been adopted across many military organizations. Risk matrices provide a framework for identifying the likelihood and consequences of hazards that are associated with mission components. Most techniques rely upon subjective assessments that are then linked to particular risk values that are calculated as the sum of risk assessments associated with individual hazards. There are some differences between this overall framework and civilian counterparts. For instance, US Army guidance helps to ensure that high risk decisions are validated by higher tiers in the command structure. It is rare to find such explicit links between risk assessment

techniques and management hierarchies in other industries; one reason for this might be that it creates an explicit line of responsibility in the event of mission failure. Further differences stem from the inherent risks in many military operations. In order to prepare staff to make tactical decisions and execute complex plans under a wide range of environmental pressure, military organizations rely upon training and simulation tasks that carry their own degree of risk:

> "Tough, realistic training conducted to standard is the cornerstone of Army warfighting skills. An intense training environment stresses both soldiers and equipment, creating a high potential for accidents. The potential for an accident increases as training realism increases, just as it does in combat. The end result is the same; the soldier or asset is lost. Commanders must find ways to protect individuals, crews, teams, and equipment from accidents during training and combat. How well they do this could be the decisive factor in winning or losing." (US Army Field Manual 3-04.513)

In other words, there is a need to simulate risk. This creates tensions because it can be difficult to justify the use of hazardous training exercises that result in military fatalities each year, for example from heat stress, accidental discharge of weapons, or from military vehicles turning over during night exercises. These accidents can, however, be justified because of the longer term benefits that they provide for individuals and for the operational effectiveness of the unit undergoing the training.

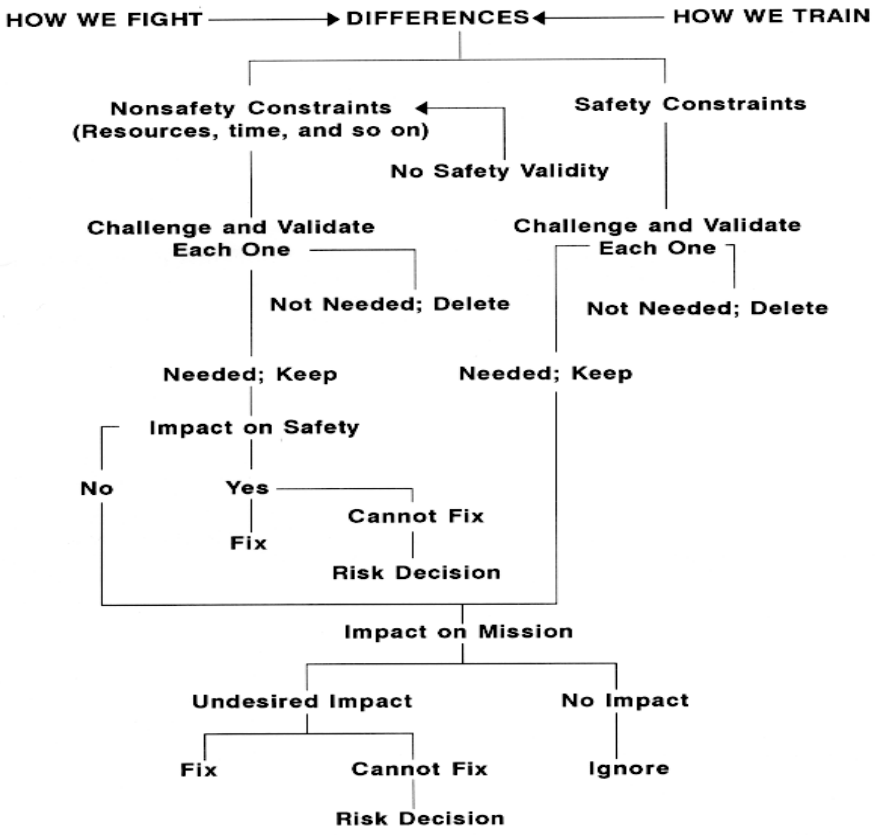


**Figure 1:** Training realism assessment process

Figure 1 is taken from TC 1-210 and summarizes the US Army's approach to risk assessment during training. The intention is to minimize differences between simulated exercises and operational challenges. These differences can be due to safety constraints. For example, the hazards of exposing troops to Multiple Launch Rocket System fire may outweigh eventual mission benefits. Differences between training and operations may also be due to other practical constraints. For example there was insufficient time for all of the troops that were issued with Night Vision Devices during Desert Shield to train with those devices before deployment. Figure 1 argues that each of these safety or functional constraints that create differences between training and operations should be challenged.

If possible, they should be removed to increase the veracity of the training program; 'With proper controls in place, these restrictions can be reduced or eliminated'. If the constraints cannot be removed then they should be subject to risk assessment following the approach outlined in previous paragraphs.

The process described in Figure 1 shows two different ways in which the US Army have embedded risk assessment within their tactical planning. Firstly, by reducing the differences between operations and training exercises, personnel are exposed to situations and pressures that simulate risk-based decision making under uncertainty prior to deployment. Secondly, in order to protect personnel in both operational deployments and in simulated exercises, risk assessment is used to mitigate or avoid any unnecessary risks. However, a number of caveats remain. The subjectivity of risk management techniques often makes it difficult for individuals to challenge decisions where they believe that undue risks are being taken during training exercises. For example, commanders can, and have been, relieved of duty within the US Army when soldiers suffer from avoidable heat-related injuries. Even so 13 died from these causes during 2005, there were more than 500 cases of heat stroke and 2,200 of heat exhaustion. These figures illustrate that many of the hazards associated with training exercises are often only apparent in retrospect.

A number of accidents involving improvised explosive devices (IEDs) can also be used to illustrate the difficulty of using risk management to maintain safety while at the same time reducing the differences between operational and training exercises. IEDs are one of the biggest threats currently facing many armed forces around the globe. In an effort to prepare personnel, many US Army units have constructed 'makeshift' IEDs for use in pre-deployment training. In particular, several variants have been developed using ad hoc extensions to the M21 (Hoffman) Artillery Flash Simulator. This device is responsible for more explosives accidents and personnel injuries than any other simulator. Other improvised IEDs rely upon flour mixtures with military grade munitions that often have extremely unpredictable results. The US Army Combat Readiness Center (2006b) observes that 'although their intentions are good, the risks associated with using homemade IEDs might be worse than the potential training benefits'. These devices contravene both Federal laws and Army regulations (eg AR385-63, Range Safety, paragraph 2-2). However, the continuing number of accidents involving ad hoc IEDs during pre-deployment training illustrates clear differences in perception within the Army between the operational benefits and the training risks of using such devices.

Composite Risk Management

The US Army's first published doctrine on risk management was published in April 1998. Field Manual 100-14 was intended to help leaders make specific operational decisions about force protection. However, the attacks of 2001 revealed significant omissions in FM100-14. In particular, there was a perception that it failed to adequately consider the terrorist threat to military personnel both on and off duty. Other criticisms were levied at the additional guidance in FM3-04.513 and TC 1-201. It was argued that these documents created arbitrary distinctions between the methods used to identify hazards in tactical and non-tactical operations. Such concerns led to the introduction of Army Field Manual 5-19 on Composite Risk Management (Department of the Army, 2006). A primary motivation behind this document was to coordinate the military response to a changing operational context. FM5-19 states that personnel should "Accept no level of risk unless the potential gain or benefit outweighs the potential loss. (Risk assessment) is a decision making tool to assist the commander, leader, or individual in identifying, assessing, and controlling risks in order to make informed decisions that balance risk costs (losses) against mission benefits (potential gains)". However, it also urges staff; "Do not be risk averse. Identify and control the hazards; complete the mission".

FM5-19 embodies the same five stages of risk management that were embodied in FM3-04.513, mentioned above. The risk assessment stage also relies upon risk matrices. However, FM5-19 advocates a more 'holistic approach' rather than following the traditional military distinctions between accidental and tactical hazards embodied in the divide between training and operations in Figure 1. This integrated policy led to the new term 'Composite Risk Management' (CRM). The motivation stemmed, in part, from initiatives at a strategic level to introduce risk assessment as a key tool to inform decision making throughout the military. It also stemmed from dissatisfaction with previous methods reflected in the change of name from the US Army's Safety Center to the new US Army Combat Readiness Center. This field operating agency located at Ft. Rucker, Alabama is the main agency for

promoting operational risk management throughout the US Army. Senior staff leading this transformation summarized the need for change to CRM:

> "…the Army was still operating under a 1970's paradigm for safety, relying on lagging indicators, consequence management, and a compliance orientation… Mishaps behind the wheel accounted for nearly ¾ of the deaths in the past 2 years, the same proportion as reflected in the Army Safety Center's 1984 review…Such data make it clear that traditional safety has been unable to provide permanent solutions for chronic issues but simply has supplied superficial, temporary fixes. Thus, the (new) offensive on loss prevention has elements for the close fight and the deep fight. The plans consider the main effort (CRM in Army operations) and the flanks (CRM in off duty activities)". (Smith and Yaeger, 2007)

As might be expected, the move from a separation of concerns between accidental and tactical risks towards a holistic Composite Risk Management approach required a significant cultural change. In particular, the traditional boundaries between safety management and operational planning were deliberately blurred in FM5-19 so that any tactical decisions had to be assessed in terms of the overall risks that personnel might face.

Under FM5-19 a hazard is interpreted to be any "condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation". They include "a situation or event that can result in degradation of capabilities or mission failure". However, the holistic nature of Composite Risk Management introduces important differences that reflect the US military concern to look after personnel on and off-duty. Hazards are defined to exist in all environments, including but not limited to "combat operations, stability operations, base support operations, training, garrison activities, and off-duty activities". The revised field manual also advocated the METT-TC mnemonic (Mission, Enemy, Terrain and weather, Troops and support available, Time available, and Civil considerations). METT-TC can be used to identify hazards irrespective of whether units are on or off-duty. FM5-19 also extended the scope of previous guidance by arguing that all Army personnel should be trained in the principles of risk management. In consequence, Composite Risk Management doctrine has been institutionalized in the Risk Management Chain Teaching program created by the Chief of Staff of the Army (US Army Combat Readiness Center, 2007).

The CRM doctrine emphasizes that commanders must identify those enemy capabilities that pose hazards to an operation or mission. Key to this hazard analysis of enemy capacity is the Intelligence Preparation of the Battlefield (IPB). The IPB is intended to support 'threat based risk assessments by identifying opportunities and any constraints the battlefield environment offers to both enemy and friendly forces' and hence must explicitly capture 'enemy capabilities and vulnerabilities'. However, FM5-19 also recognizes the temporal constraints that create considerable pressures for the field commanders who must make key tactical decisions. The more considered quantitative approaches to likelihood and consequence assessment are ill suited to the rapidly changing context that many commanders must address:

> "In these situations, they perform hasty risk assessments. A hasty risk assessment may be performed mentally. It may be transmitted verbally or in writing via a FRAGO (Fragmentary Order)…Only the essential information necessary to complement the FRAGO and forward the risk guidance received from the battalion commander are included. As in the example, an overlay may be included with the risk assessment to clearly portray the location of hazards. The hasty risk assessment (can be) a separate document. However, it may be included within the FRAGO issued by the company to the platoon" (FM5-19).

The time limited nature of these situations and the critical nature of their decisions makes it essential that FRAGOs are successfully communicated to their intended recipients. FM5-19, therefore, provides detailed guidance on how hazard assessments can be passed in annotated form within these orders. The integration of 'ad hoc' risk assessments in fragmentary orders again illustrates the holistic approach advocated in the new Field Manual. Even where time is strictly limited, commanders should explicitly take the opportunity to consider potential hazards as part of the Military Decision Making Process (MDMP).

The closing sections of the Field Manual summarize the motivation for the holistic approach to military risk assessment; 'the death of a Soldier in combat or due to an accident can have a devastating effect on a unit's morale

and effectiveness…the effects of criminal acts, suicide, sexual assault, and reckless behavior can also cripple an organization's morale and destroy its combat effectiveness'. The CRM process is intended to help military personnel identify behaviors or activities that threaten a unit's morale and combat effectiveness. Hence it follows that the same CRM techniques should support suicide prevention and POV accidents as well as reducing exposure to, or mitigating the consequences of, tactical risks.

As with ERAM, it is too soon to judge whether CRM will provide the anticipated benefits. Some caution is necessary because there is only limited evidence to suggest that training personnel in the principles of risk management will have any longitudinal impact on accident rates (Johnson, 2003). There is a concern that attribution bias will impair the critical and unbiased assessment of risk assessment initiatives across the US military. Attribution bias refers to inferences that are made by observers often with the benefit of information or resources that were not available to the individuals involved in an incident. This can be illustrated by a recent accident report that describes how two M1A2 Abrams tanks were assigned to escort an explosive ordnance disposal (EOD) team to an enemy weapons cache site. Neither the tank crews nor the EOD team was familiar with the location of the weapons cache. Maps and imagery provided insufficient detail to plan the mission. A process of trial and error led them the cache and the EOD team completed their task after dark, around 18:45. The leaders decided to return using the route over a sandy, clay road that ran alongside a canal. The trail tank crossed a bridge over the canal and turned right over a berm. It's rear began to shake violently and the track commander (TC) told the driver to go left as the right edge of the road collapsed under the tank's weight. The crew heard the TC announce "rollover, rollover, rollover" as the tank overturned into the water-filled canal. The TC's death was attributed to blunt-force trauma suffered during the rollover and a lack of oxygen after the tank settled in the water. The subsequent investigation identified two primary causes: a failure to adequately plan the mission and a failure to execute proper rollover procedures because the TC did not immediately drop inside the turret. Attribution bias can be seen in the commentary that accompanies the account of this accident:

> "Had the tank crews used CRM when they were trying to identify alternate routes, they might've realized the hazards they faced on the unimproved roads they ultimately selected. This instance wasn't the first time a canal road collapsed under a tactical vehicle in theater; similar roads have caved in under vehicles weighing far less than an M1 tank, including HMMWVs. The bottom line is every Soldier must take into account all the hazards, both tactical and accidental, that can hurt or kill them or their buddies. We need each one of you, so use CRM to stay ready and Own the Edge!" (Countermeasure, 2006b)

The key term here is 'might' – without significant additional operational experience in the application of CRM, considerable questions must remain as to whether the ad hoc risk assessments recommended in FM5-19 could really have helped the leaders and their crews to identify the hazards at the end of a long day, filled with other earlier missions as they made their way back to base through a potentially hostile environment.

Discussion and Conclusions

Previous sections have argued that risk assessment now dominates both strategic and tactical thinking across the US military. We have seen how the annual statements from the Chairman of the Joint Chiefs of Staff to Congress now explicitly embody the language of risk management. The concept of risk mitigation is also captured in the expectation that the Defense Secretary will respond with appropriate interventions. At a more tactical level, the Enterprise Risk Assessment Model (ERAM) has been developed to help mitigate the risks associated with procurement and with the management of large scale military contracts. At the other end of the lifecycle, the ARAMS tool provides the key strategic tool for managing decommissioning and redevelopment of military resources.

Field Manual 3-04.513 and Army Training Circular 1-210 provide further examples of the dominance of risk assessment within US military doctrine. These documents provide detailed guidance on the techniques to be used when planning hazardous operations. A central preoccupation in these documents is to develop training exercises that simulate operational, combat conditions without exposing personnel to undue risk. More recently, however, it has been recognized that the 'war on terror' blurs traditional boundaries between combat and non-combat situations. It has, therefore, been argued that the same risk assessment methods should be used irrespective of whether personnel are being trained, or are serving in the field or are off-duty, where they may be potential terrorist targets.

As a result, FM5-19 advocates a Composite Risk Management in which hazard analysis and risk management have become the dominant decision making strategies across the US military. As we have seen, FM5-19 institutionalizes the ideas of likelihood and consequence, of mitigation and exposure reduction within all levels of operational planning.

Does the dominance of risk assessment techniques create any concerns? It is difficult to answer this question in any definitive way, given that techniques like the Enterprise Risk Assessment Model and Composite Risk Management are relatively novel. Their impact on operational effectiveness has yet to be studied, for instance across operational units that are still undergoing training in the doctrines embodied in FM5-19. However, at other levels within the military, experience has shown the difficulty of using risk assessment techniques to reliably inform decision making. For example, the US General Accounting Office surveyed risk assessment practices relating to US preparations for chemical and biological attacks and argued that:

> "DOD's assessment process is unreliable for determining the risk to military operations; as a result, in its 2000 report to the Congress, the Department inaccurately reported the risk in most cases as "low." The report is inaccurate because it includes erroneous inventory data and wartime requirements. More important, the process for determining risk is fundamentally flawed because (1) the Department determines requirements by individual pieces of protective equipment rather than by the number of complete ensembles that can be provided to deploying service members, and (2) the risk-determining process combines individual service requirements and reported inventory data into general categories, masking specific critical shortages affecting individual service readiness. Had the Department assessed the risk on the basis of the number of complete ensembles it had available, by service, the risk would rise to "high" in all cases. Inadequate management of inventory is an additional risk factor because readiness can be compromised by DOD's inventory-management practices, which prevent an accurate accounting of the availability or adequacy of its protective equipment. These practices can also undermine efforts to mitigate the risk".
>
> (GAO, 2001)

In technical areas, such as the preparation for chemical and biological attacks, it is impossible to accurately assess the residual risk to national defense without relatively complete and accurate information on existing control measures. Simply implementing risk assessment techniques as a framework for decision making will not eliminate the underlying requirements for accurate information about military and civil defense inventories. These specific comments have recently been reiterated in more general criticisms of the implementation of risk-based decision making across the Department of Defense:

> "DOD faces four challenges that have affected the implementation of the framework. First, DOD's organizational culture resists department-level approaches to priority setting and investment decisions. Second, sustained leadership, adequate transparency, and appropriate accountability are lacking. Further, no one individual or office has been assigned overall responsibility or sufficient authority for the framework's implementation. DOD also has not developed implementation goals or timelines with which to establish accountability, or measure progress. Finally, integrating the risk management framework with decision support processes and related reform initiatives into a coherent, unified management approach for the department is a challenge that DOD plans to address during the 2005 QDR". (GAO, 2006a).

These criticisms reinforce the GAO's previous observations about the organizational challenges that the Department of Defense faces in implementing risk assessment as a basis for decision making across such a complex organization. This should not be interpret as a criticism of risk assessment in itself, given that GAO-05-207 explicitly advocated the adoption of this approach. However, there remain significant concerns about whether it is possible to sustain the organizational changes that are envisaged for the Department of Defense:

> "The unpredictable nature of Defense programs can be traced to instabilities in the broader acquisition system. Fundamentally reshaping that system should make the state of the Department's major acquisition programs more predictable and result in better stewardship of the U.S. tax dollar." Additionally in January 2006, the Defense Acquisition Performance Assessment (DAPA) Project provided an independent review of and recommendations for how to improve the DoD acquisition process. Similar recommendations in the

> past had not been able to produce lasting change; however, a new concept led by the BTA called ERAM shows promise". (DOD, 2006)

There are further concerns. In particular, there is a miss-match between the simplified forms of risk assessment that are being taught at most levels of the US Army command structure and the complexity of the decisions that they are being called to make. The concept of exposure is often poorly dealt with. Although this might seem to be an abstract concern, it has critical practical consequences. For example, consider a leader who must decide between two plans in which a unit either has to cross a river using a bridge or must make a significant detour to cross at a fording point. In the former case, there may be a relatively short exposure to an extremely high risk while in the latter case there would be prolonged exposure to a lower level of risk. Simply decomposing mission plans into a Mission Essential Task List will not help much to balance the relative risks here. Research in prospect theory has developed a series of techniques to help decision makers evaluate different outcomes with relative risks in the form described above. However, it remains to be seen whether or not these approaches could be translated into the Army doctrine in field manuals. Until more sophisticated methods are developed, leaders continue to face considerable problems in mapping between the simple techniques that they have been trained to use and the complex, dynamic decisions that they must make every day.

Previous sections have described how lightweight risk assessments are to be integrated into FRAGOs (Fragmentary Orders) when leaders must make complex decisions against hard deadlines. The Composite Risk Management proposals are also intended to ensure that these assessments are communicated to the units involved in particular mission components. The precise format for both the FRAGOs and the communication of risk based decisions must be tailored to the particular situations facing individual units. Only time will tell if this emphasis results in the development of appropriate tools and techniques that can be used in the field. One concern is that many military staff are pre-selected and then trained for decision-making characteristics that are very different from those in the civilian population. There seems to be very little direct evidence today that CRM techniques will be able to compensate for the risk preference biases that are often seen in military personnel. This concern can be illustrated by an article in a recent edition of the US Army's Countermeasure – a risk management publication from the Center for Combat Readiness, where the author describes the risk seeking nature of many soldiers and then raises an, as yet, unsubstantiated hope that Composite Risk Management will help to address some of the consequences in military activities:

> "Have you ever deliberately put yourself in a situation you didn't think you'd get out of alive, only to survive and vow never to do the same thing again? … Playing football on a semi-thawed lake, passing traffic uphill in a no-passing zone, driving drunk and boating in a lightning storm—none of these are sound decisions, but I've done them all. When you're young, it's hard to distinguish risk from what we perceive as adventure… We can step back and make smart decisions, which is the beauty of Composite Risk Management. Even in combat, Soldiers of all ranks have the authority to stop unsafe acts and implement controls to ensure everyone makes it home from the fight. Please take advantage of this great tool and apply it to everything you do, especially if you see some idiot pulling charges out of a powder pit!" (Andree, 2006).

Such assertions arguably underestimate the problems of 'groupthink' and 'risky shift' that are well known to affect team-based decision making in combat operations (Johnson, 2003). The term 'group think' refers to the way in which co-workers will reinforce mutual beliefs and discount lateral thinking if it contradicts accepted norms within the group. 'Risky shift' refers to a process by which team members will gradually adopt the position of more risk seeking individuals even if they would normally reject those positions if they were not in that team. More work is urgently required to determine whether the implementation of CRM across many diverse units will have the operational benefits envisaged in the Combat Readiness Center publications.

Further problems affect risk management for military systems that rely upon the operation of software components or interventions by human operators. Traditionally risk assessment techniques have been applied in safety-critical systems to represent and reason about the reliability of hardware components. It is possible to derive evidence to validate failure rates by observing the performance of these components over prolonged test periods. This approach is embodied within the approaches documented within US Military Handbook MIL-HDBK-338B. However, these statistical approaches do not work well with models of human behavior. A range of performance

shaping factors include the level of training and motivation of enemy forces make it dangerous to rely too much on subjective risk assessments of any hazards that involve predictions of their behavior. It is equally difficult to make accurate predictions about the likelihood of hazards that stem from 'human error' on the part of friendly forces, including other coalition members. Similarly, the deterministic nature of software undermines attempts to use risk assessment with more complex distributed systems. Code does not wear out so the likelihood of failure does not increase over time, if software contains a bug when it is written then that fault will remain there until the code is executed. Hence, risk management techniques that have been developed to assess the likelihood and consequences of hardware failure cannot easily be applied to most, modern military applications (Johnson, 2003).

One of the most vibrant areas of research within risk management and decision theory has focused on the development of models that explain opponents' behavior in various forms of games. These models assume that competitors make complex decisions with uncertain outcomes in order to maximize their returns while, typically, minimizing the rewards for competitors in the game. Considerable benefits are to be gained if one player understands the decision making processes employed by their opponent. These theoretical outcomes have direct applications in the military domain. For example, previous sections have reiterated the guidance to leaders that all 'unnecessary risks must be avoided'. This enables opponents to make direct inferences about the risk adverse behavior of the US military that are being applied by the insurgents' use of IEDs and snipers in Baghdad. In this case, the opponents are reacting on the basis of direct observations of risk-based decision making in the field. In the future, however, opposing forced could make strategic decisions based directly on the risk averse statements in public documents such as FM5-19. If Composite Risk Management is effectively employed in the manner envisaged by the Department of Defense then this document and its successors will provide opposing forces with a 'blue print' for US military operational decision making.

## Biography

Chris.W. Johnson, DPhil, MA, MSc, FBCS, CEng, CITP, Department of Computing Science, University of Glasgow, Glasgow, G12 8RZ, Scotland, UK, telephone +44 (141) 330 6053, facsimile +44 (141) 330 4913, e-mail – Johnson@dcs.gla.ac.uk, web page http://www.dcs.gla.ac.uk/~johnson

Chris Johnson is Professor of Computing Science at the University of Glasgow in Scotland. He heads a small research group devoted to improving the reporting and analysis of incidents and accidents across safety-critical domains ranging from healthcare, to the military to aviation and rail. He has led a number of studies into military incidents and accidents, most recently this involved a study of mishaps involving night vision equipment.

## References

R. Andree, Personnel Injury: Great Flying Stoves!, US Army Countermeasure, Centre for Combat Readiness, Volume 27:10/06:10-11, October 2006.
https://crc.army.mil/MULTIMEDIA/magazines/countermeasure/2006_issues/cmoctober06.pdf

N. Freier, In Defense of Rational Risk Assessment. Technical report, Strategic Studies Institute of the US Army War College, Carlisle, Pennsylvania, 2007.
http://www.strategicstudiesinstitute.army.mil/Pdffiles/Pub763.Pdf

C.W. Johnson, A Handbook of Accident and Incident Reporting, University of Glasgow Press, Glasgow, Scotland, 2003. http://www.dcs.gla.ac.uk/~johnson/book

C.W. Johnson, The Role of Night Vision Equipment in Military Incidents and Accidents. In C.W. Johnson and P. Palanque (eds.) Human Error, Safety and Systems Development, Kluwer Academic Press, Boston, USA, 1-16, 2004.

P. M. Rury, V. Baitchorov, A. F. Sculimbrene, A Risk-Based Decision Protocol For The Reuse Of Military Sites,

Institute of Zoology, Belarussian, Academy of Science, Minsk, Belarus and Environmental Management Restoration
Branch, Wright-Patterson Air Force Base Ohio, USA, April, 2007.
http://www.hatchmott.com/documents/adobe/decommission.pdf

J.A. Smith and B.R. Yaeger, Tansforming Army Safety: Enhance Combat Readiness through Composite Risk Management, Technical Report, US Army Combat Readiness Center, 2007.
https://crc.army.mil/CRC/transforming_army_safety.pdf

US Army Combat Readiness Center 2006, Composite Risk Management: Hot Brass in the Summertime, Countemeasure, 27:09/06:9-10, 2006.
https://crc.army.mil/MULTIMEDIA/magazines/countermeasure/2006_issues/cmseptember06.pdf

US Army Combat Readiness Center 2006a. Loss Investigation: A Map but No Direction, Countemeasure, 27:09/06: 14-15, 2006. https://crc.army.mil/MULTIMEDIA/magazines/countermeasure/2006_issues/cmseptember06.pdf

US Army Combat Readiness Center 2006b. Simulated IEDs: Real Problems, 27:06/06: 10-11, 2006.
https://crc.army.mil/MULTIMEDIA/magazines/countermeasure/2006_issues/cmjune06.pdf

US Army Combat Readiness Center 2007, U.S. Army Accident Information; Ground Accident Statistics for the Current Fiscal Year, as of 3 April 2007. US Army Combat Readiness Center,
https://rmis.army.mil/stats/prc_ground_stats#POV

US Army Combat Readiness Center 2007a, Composite Risk Management Chain Teaching Training Packet. US Army Combat Readiness Center, April 2007.
https://crc.army.mil/RiskManagement/detail.asp?iData=2&iCat=710&iChannel=25&nChannel=RiskManagement

US Army Corps of Engineers, Adaptive Risk Assessment Modeling System (ARAMS), April 2007.
http://el.erdc.usace.army.mil/arams/

US Army Corps of Engineers, Fact Sheet: Risk Assessment, April 2007a.
http://www.lrb.usace.army.mil/fusrap/docs/fusrap-fs-risk.pdf

US Department of Defense, Evolving Investment Review and Accelerating Systems Acquisition, Technical report, Defense Business Transformation Unit, Washington DC, USA, April 2006.
http://www.defenselink.mil/dbt/manage_inv-review.html

US Department of Defense, FAQ: Enterprise Risk Assessment Methodology (ERAM), Technical report, Defense Business Transformation Unit, Washington DC, USA, April 2007.
http://www.dod.mil/dbt/faq_eram.html

US Department of the Army, TC 1-210: Aircrew Training Program Commander's Guide to Individual And Crew Standardization, Headquarters, Department Of The Army, Washington, DC, 3 October 1995.
http://www.cavalrypilot.com/tc1-210/chg1toc.html

US Department of the Army, FM 3-04.513: Battlefield Recovery and Evacuation of Aircraft, Headquarters, Washington, DC, 27 September 2000.
http://www.army.mil/usapa/doctrine/Active_FM.html

US Department of the Army, FM 5-19: Composite Risk Management, Headquarters, Washington, DC, August 2006.
https://crc.army.mil/riskmanagement/fm5-19.pdf

US Government Accountability Office (GAO), Chemical and Biological Defense: Improved Risk Assessment and

Inventory Management Are Needed, Technical Report GAO-01-667, Washington DC, USA, 2001. http://www.gao.gov/new.items/d01667.pdf

US General Accounting Office (GAO), High-Risk Series: An Update, Technical Report GAO-05-207, Washington DC, USA, 2005.

US Government Accountability Office (GAO), Business Systems Modernization: DoD Continues to Improve Institutional Approach, but Further Steps Needed, Washington DC, USA, May, 2006.

US Government Accountability Office (GAO), Additional Actions Needed to Enhance DOD's Risk-Based Approach for Making Resource Decisions, Technical Report GAO-06-13, Washington DC, USA, 2006a.

US Government Accountability Office (GAO), Information Security: Computer Attacks at Department of Defense Pose Increasing Risks, Technical Report GAO/AIMD-96-84, Washington DC, USA, 2006b.

US Government Accountability Office (GAO), Business Systems Modernization: DoD Continues to Improve Institutional Approach, but Further Steps Needed, Technical Report Washington DC, USA, 2006c.

J. White and A.S. Tyson, Wars Strain U.S. Military Capability, Pentagon Reports, The Washington Post, Tuesday, May 3, 2005; A06.
http://www.washingtonpost.com/wp-dyn/content/article/2005/05/02/AR2005050201504_pf.html