Chapter 9

Mission Oriented Risk Analysis and Prioritization of Research Activities

Introduction

Information Assurance (IA) is defined as the practice of protecting and defending information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. The focus on IA now has a network-centric component. In addressing Defense-in-Depth, we have moved away from systems and platforms and our focus is now more on the network. IA is still a major concern, but network defense has become an important part of an IA layered defense.

Risk Management Review

Risk management is the total process of identifying, controlling and mitigating information system related risks. Identifying the risks to existing system security and determining their probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact are components of traditional risk analysis. When the system is large, the risk analysis is both complex and time consuming. In the research and technology (R&T) arena when the system doesn't exist, when dealing with emerging technologies that haven't transitioned, or when dealing with complex and divergent ideas, risk management involves developing a means whereby these multi-faceted ideas can be visualized in a consistent way.

Risk analysis, it's a technique whereby we can apply consistent criteria against each risk element so the resultant values can be directly compared and prioritized on an equal basis in terms of the risk each represents to a mission or operation. Then, depending on the strengths and needs of the sponsoring organization soliciting the work, the potential for solving the issue with existing technologies, and of course the budget actually available to spend on research and development, these organizations prioritize the list of problem areas using risk analysis. From these final prioritized lists, solicitations and announcements emerge.

Risk Mitigation in R&T Requirements

Risk management decisions in R&T require determining the proper balance between the costs and benefits of functionality and security from among the available alternatives that best satisfy the operational objectives in a potentially hostile environment. Risk Managers, system owners, policy and budget authorities, and other stakeholders need a more detailed understanding of how risk mitigation approaches may be employed to accomplish the network defense trade-offs required for R&T technology transition decisions. This section addresses a multi-attribute utility model applicable to analyzing options in terms of mission-based risk avoidance. The model described in this paper is based on the technique called Mission Oriented Risk Analysis (MORA).

MORA is an analysis and reasoned judgment (case law) approach that attempts to identify the multiple parameters that are important in answering a specific question, establishes the scales from which estimates for each parameter will be selected, establishes the weighted average relationship between the relevant parameters, and uses the results to provide equivalent insights into the pros and cons of various decision alternatives. For R&T decisions, the form of the

MORA model and the estimates on variables herein have been tailored to the basic questions being addressed at each stage and the data that is available.

The MORA based approach to risk management has the following characteristics:

- Rooted in established policies and requirements compliance.
- Most accurate when inputs from a variety of stakeholders are used.
- Uses previous specific application decisions to provide additional definition and guidance to related situations precedence.
- Is flexible and dynamic enough to respond to a changing environment.

Stakeholders can use MORA to assess the effectiveness of a technology solution's features throughout the life-cycle of the technology from initial research through technology development. Risk Assessors and Risk Managers can characterize how technology solutions will mitigate risks in relation to their effect on mission effectiveness. Using this formal process, system owners make decisions on how much risk they are willing to accept. In general, the MORA model shown in Figure 1 will provide insights into the essential elements that enable informed decision making.

Systems and technology are not static. Throughout the transition process, the parameters of risk change constantly. Thus, it is necessary to periodically revisit the understanding of the risks incurred while operating within the current and projected environments and to determine if a change in the protection approach (people, operations, technology) is warranted. The MORA process provides the necessary analysis to make informed decisions regarding the benefit of further investment in technology to reduce mission risks.

Finally, in the Decision-Making activity of MORA, the manager is going to decide:

- Whether to implement the proposed technology,
- Whether the proposed or implemented technology solution reduces the risks enough to justify continued research or development,
- How to monitor the risks to mission, and
- When (define circumstances) to re-initiate the risk assessment process

Managing a Mission Oriented Risk Analysis

MORA supports the program management process by providing analysis and justification for developmental and operational decisions. The MORA process involves the integration of complex research and transition activities being performed both independently and in concert with other potentially competing R&T activities. The application of project management principles enables senior executives to:

- Establish success metrics
- Enhance customer focus and alignment
- Quantify value versus cost
- Optimize allocation of resources
- Achieve strategic plans
- Improve time-to-market

In terms of network defense R&T, MORA program management will support:

- Determining the scope of the Risk Analysis
- Determining the impact a particular requirement will have on mission success
- Determining research feasibility
- Determining research and transition time constraints.
- Determining resource requirements
- Establishing/controlling budgets
- Assessing the value of alternative solutions
- Risk mitigation planning
- Formalized reporting

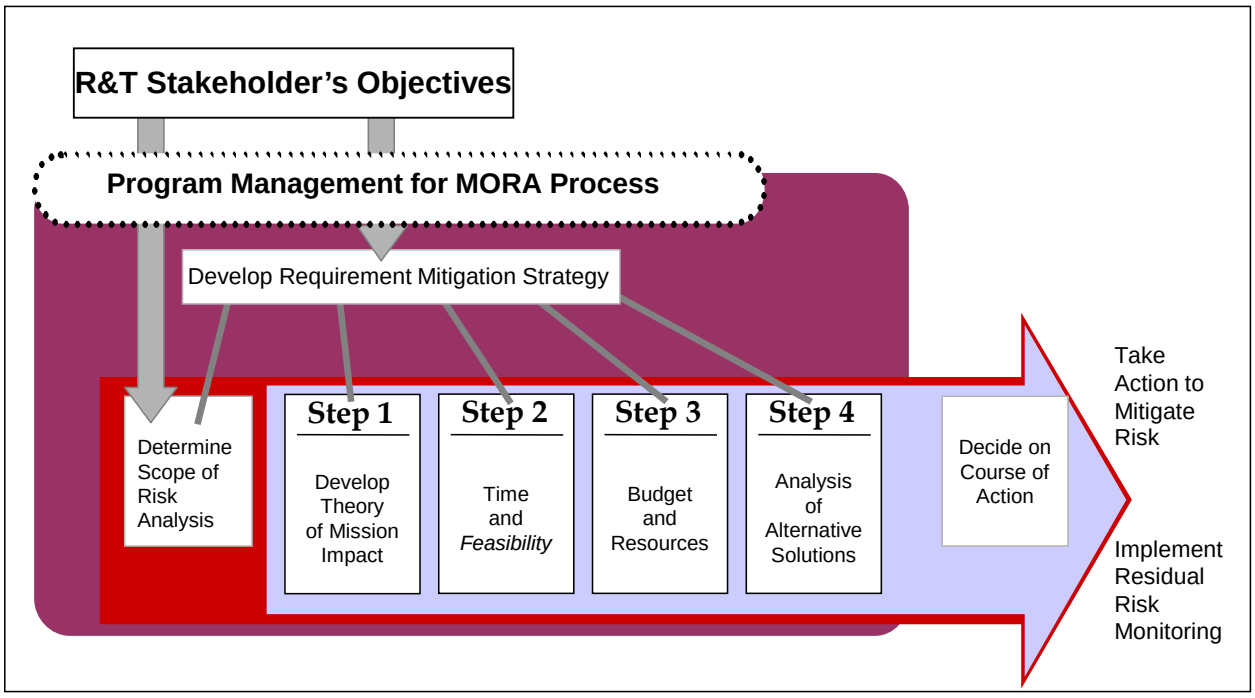

Figure 1 - Primary MORA Analytical Building Blocks

Mora Applicability R&T Technology Transition

Within the new product R&T transition process, MORA techniques are primarily applicable to prioritizing technology requirements and evaluating proposed solutions in terms of risk. Research decisions are based on risk minimization. Therefore, the impact of selections in the research community must also take into account multiple uncertainty factors related to budgeting and available resources. Figure 2 compares applicable MORA sections to the technology transition process.

Following requirement identification, a simple pre-screening process is used to refine the total requirement list to a more refined list for further mission-focused analysis. This prioritized list is further refined based on practical factors such as development time and the ability of existing technology to solve identified requirements. Research focus and sources evolve from the final requirements prioritization list. When proposals that address solutions or partial solutions to

requirements are received, these are compared against their overall system impact, the final cost of the solution, and an estimate of the proposal's ability to deliver an acceptable product. Guidelines for applying MORA to justify each of these risk management decisions are described in the following sections.

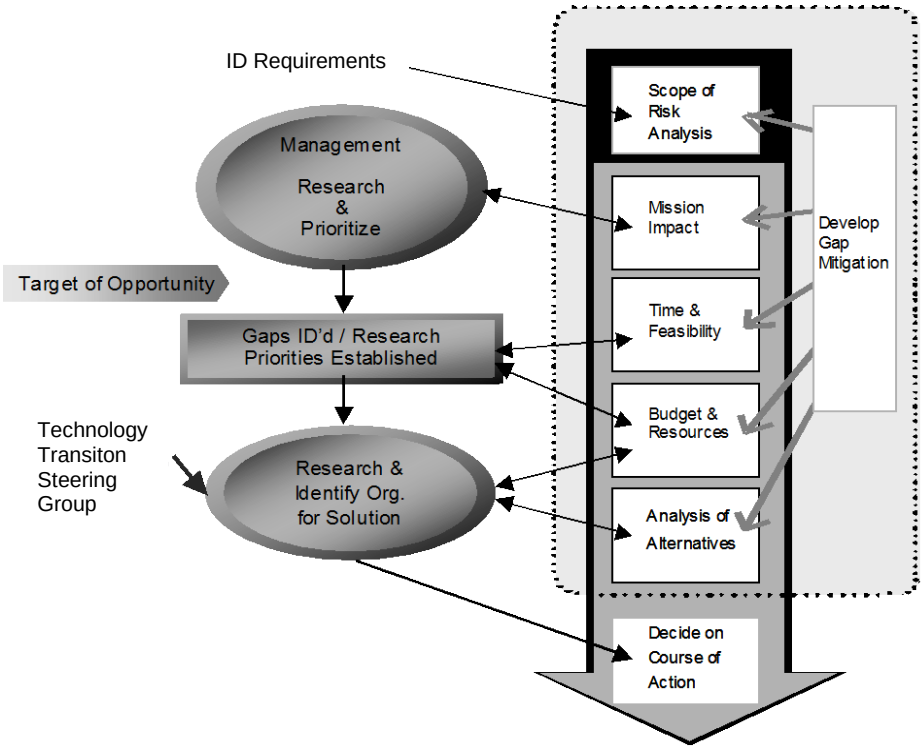

Figure 2 - MORA Steps in the Technology Transition Process Alignment

Determine the Scope of the Risk Analysis

The number, complexity and unique characteristics of technology requirements determine the scope of the risk analysis. The potential for an actual attack on a network, due to the lack of a defensive technology solution provides the basis for determining a mission impact if the attack is successful.

To ensure that the risks associated with interconnection of networks –shared risks – are appreciated, the Risk Analysis Environment Boundary is defined as incorporating the System Baseline Architecture, evolving system architecture, and relevant interconnected network architecture.

The general flow of specific steps supporting boundary and scope determination follows Figure 3.

Collecting and Defining Requirements

No single organization is responsible for all research initiatives. Nor is there any one laboratory, agency, or organization responsible for all ongoing cyber security research. Additionally, every organization has a few priority issues, but describing the specific problem and identifying the state-of-the art technology that might offer a technology solution has been both difficult and time consuming. For a comprehensive view into R&T activities, governments

rely on private sector companies and research institutions for intellectual and implementation expertise. Therefore, a collaborative public and private sector environment is necessary to identify, refine, and then solve research needs. Activities such as workshops and conferences that draw together top researchers from across the nation are sponsored by each of these organizations, or laboratories and agencies within these organizations, on a regular basis can create this environment.

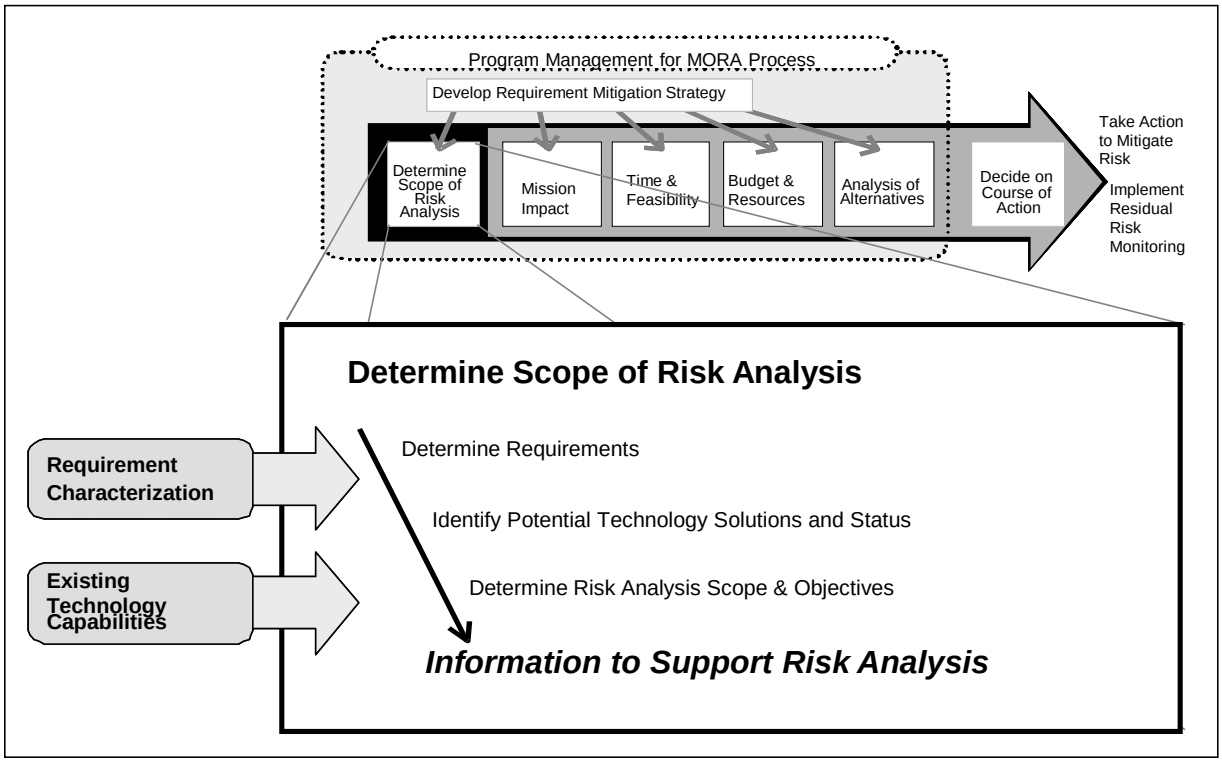

Figure 3 - Determine Scope of Risk Analysis

The following sources should be used to identify R&T requirements and their current solution status.

- Primary Sources
  - Government and Industry Stakeholders
- Secondary Sources
  - Community Workshops
    Hard Problems Lists
  - SMEs and Proposals
  - Other traditional research resources

Determine Risk Analysis Scope and Objectives

Performing a MORA on R&T requirements requires some bounding of the problem set. However, performing a comprehensive analysis on all or a large number of requirements would be a significant effort. Therefore, a more realistic approach to requirement prioritization is to reduce the overall number requiring further analysis.

It's best to perform the initial requirement reduction by collecting inputs from a broad mix of: operational users, representatives of traditional research laboratories, academia, industry, and

other interested stakeholders. The initial analysis would consist of requesting each representative to respond to a simple question: "Rank in order what you consider the top 5 research requirements and a sentence or two as to why." In the majority of cases, responders will have only some of the same requirements listed. Give a weighting to each responders prioritization of five for most important to one for least of the five requirements identified. In the case of equal rankings, add what the total would be and divide by the number included. The final weighted list summing all responses should provide a realistic basis for the initial requirement reduction activity.

Not all requirements can be solved with existing technologies. Additionally, some requirements are so broad that more focusing is necessary from a technology perspective before a particular solution approach can be identified. Based on web portal information, workshops, conferences, and technology forums, some bounding can take place by breaking down each identified large R&T requirement into focused subsets. In the case of solvable requirements, themes should emerge as to what technologies could potentially be applied to solve the problem components. Addressing larger network defense problems in terms of smaller components will help focus research activities to achieve steady progress towards solving difficult overarching issues. For each of the smaller problem subsets, business cases and selection criteria are developed based on mission objectives to further focus solicitation efforts in finding the correct entity to solve the problem.

Developing a Theory on Mission Impact

A mission is an organization's reason for existence. Selecting the highest priority requirement to solve based on a mission need requires answers to the following questions:

- Who needs it?
- What requirements do they want to solve first?
- How is their mission impacted without a solution?
- When do they want it?
- What resources are required and are they available?
- What current documentation exists and where is it?
- How useful is the technology solution to other organizations?

Developing a Theory on Mission Impact is depicted in Figure 4. Mission impact evaluates the inter-relationships of not having a solution for specific attacks and their potential effects on mission components if executed by an attacker. The mission impact, when supported by threats and vulnerability information, provides a measurable evaluation approach for determining the information system's ability to support an organization's mission when impacted by a cyber-based attack compromising its confidentially, integrity, or availability.

Characterize Mission and Organizational Requirements

How does an organization see itself? The mission of an organization should be described in terms of the organization's view of the world. Describe the organization's mission and the system's role in its success. Mission success is the dominate theme in this effort. Discuss system specific characteristics supporting the mission. If the Mission Impact Analysis is on a system that supports many missions, then this section states the mission of the system in terms of the organization's view of the world.

- State the mission and functions of the system and organization
- Determine mission-reliance on security aspects of information systems
- Describe in perspective of the level of activity supported (local system mission or system mission in strategic command structure)

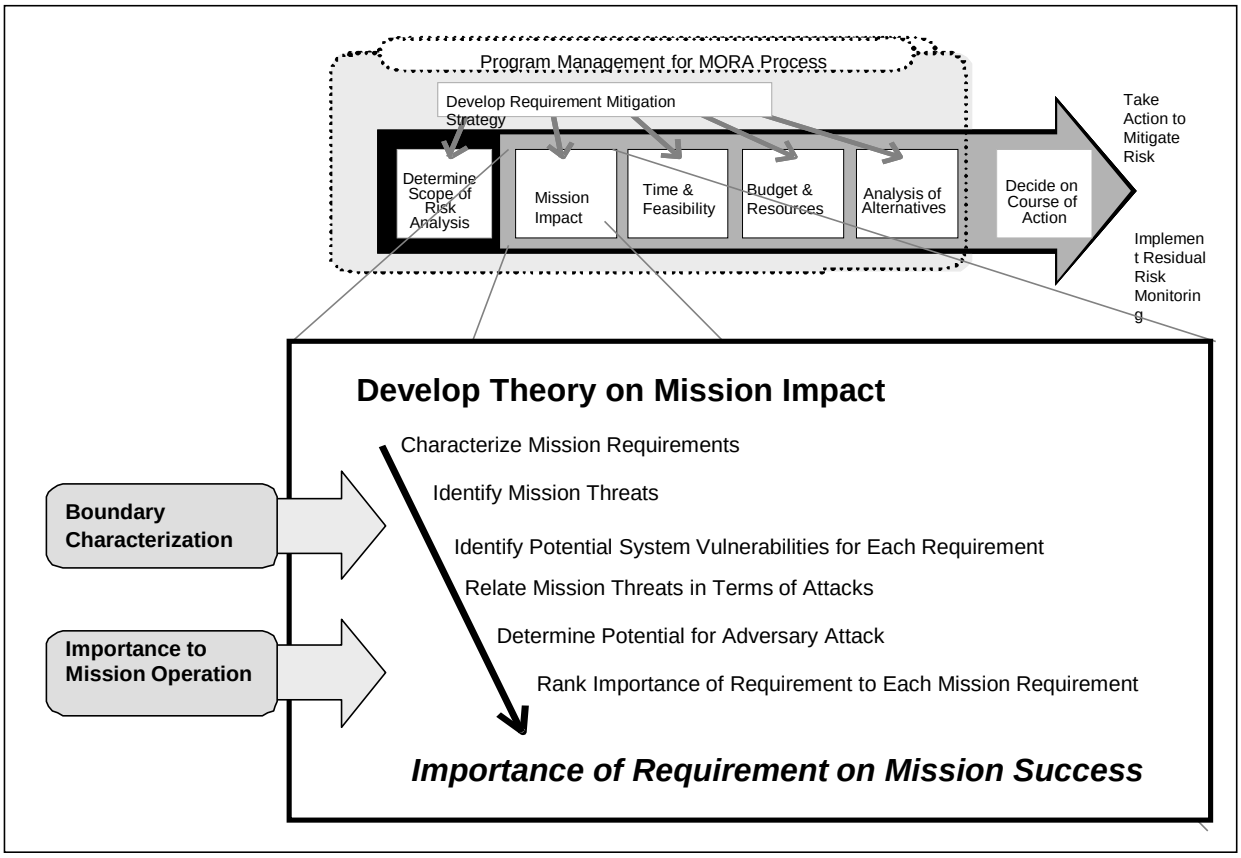

Figure 4. Develop Theory of Mission Impact

Characterization analyzes the mission operational requirements in terms of both timing and extent throughout the organization. The Theory on Mission Impact looks closely at the inter-relationships of specific attacks and their effects on mission components. Unfortunately, mission impact analysis must take place at the micro-level.

The extent of the architectural boundary to be protected must first be considered. This allows the mission impact to be tailored specifically to the unique needs of any size organization. In the case of global missions supporting computer network defense, requirement prioritizations and solutions must take into account maintaining capabilities to meet both deterrent and decisive national security objectives.

In reality, threats drive technology needs. Network defense solutions can take various forms from enclave boundary protection devices to large enterprise wide monitoring techniques. Therefore, the highest priority requirements should be considered in terms of how quickly a solution can respond to an identified threat. For unique needs, consider first those higher tier elements whose primary purpose is to thwart attacks/adverse events to allow the missions functional requirements to continue to be met despite the attacks. The term Tier is used in architecture descriptions to denote levels of decomposition.

Regarding functional requirements, these are often the applications that support mission objectives. In many cases, a system will have multiple applications in use. The best approach would be to consider each application in terms of its mission priority within the overall system and prioritized accordingly. However, this is an impractical solution. The practical approach is to pick the primary or most important application supporting the mission, and then use this application as the basis for subsequent impact analysis

Identifying Mission Threats

Information resides in hostile environments. These environments encompass threats, threat sources, adversaries, human errors, accidents, and natural disasters. Within these environments, information and data within information systems are prime targets of information operations. This activity deals with operations that attempt to gain information or degrade, destroy, or otherwise manipulate data or communications in order to achieve potentially harmful objectives. The intent will be to characterize the following relationships in terms of attacks in order to quantify the level of risk the system or its primary application is exposed to in the overall risk analysis effort:

- Relationship of Vulnerabilities to Attacks
- Relationship of Adversary/Threat Sources to Attacks
- Relationship of System Consequences to Successful Attacks
- Relationship of Mission Impact and Successful Attacks
- Relationship of Risk of Attack to Mission Impact

Scope of Attacks to Consider

An attack is a sequence of events that exploit a specific vulnerability or takes advantage of an inherent "feature" that resides on a system. The adversary (threat agent) takes an action against a vulnerability that causes an event (computer/network exploit) to take place that has a consequence that results in a harmful impact to the mission. An attack is the actual realization of the threat potential. Note that a warning that an event is taking place is not always available. Vulnerabilities are "weaknesses" or "features" in the system that can be exploited to cause harm to the system or the operations that the system supports.

There are immediate "system" consequences that can be the direct result of a successful attack:

- Unauthorized knowledge of system information (loss of confidentiality)
- Unauthorized changes to the system information or system design (loss of integrity)
- Loss of authorized use of system information or services (loss of availability or denial of service)

For each consequence there is a cost impact to the mission operation that the system is supporting. This cost can be much more than "financial costs". It may be measured in loss of lives, loss of mission success, loss of confidence in the system to support, and loss of capability. These are all measures of how a system attack can cause harm to the supported mission.

Relate Mission Threat in Terms of Potential Attacks

Risk is often considered as a function of Threat, Vulnerability, and Impact. Understanding the risk in terms of attacks implies:

- An understanding of the various potential attacks against the system, the system vulnerabilities being exploited by each potential attack, and the impediments to an adversary in mounting the attack. Knowledge of these facets yields an understanding of how successful this attack might be if it were attempted. [Likelihood of Success Given Attempt]
- An understanding of how and when adversaries might utilize each attack. This helps in understanding how likely this attack might be used against the system, particularly when the mission would be impacted the most. [Likelihood of Attempt]
- An understanding of how the system and ultimately the mission operations supported by the system will be harmed if there is a successful attack. This helps in understanding the harm if the attack is successful. [Mission Harm Given Successful Attack]
- An understanding of how the countermeasures represented by a technology solution will effect:
    - The Likelihood of Success Given Attempt (Defense)
    - The Likelihood of Attempt Given Consequence of Detection (Deterrence)
    - The Mission Harm Given Successful Attack (Resilience)

Determine Potential for Adversary Attack

Technology requirements identify limitations in current technology to mitigate identified vulnerabilities or potential threats. However, the existence of vulnerabilities does not necessarily imply they will be attacked by an adversary. For each organization there is a cost to the mission operations that the system is supporting. This cost can be much more than "financial costs". It may be measured in loss of lives, loss of mission success, loss of confidence in the system, and a loss of capability. These are all measures of how a system attack can cause harm to the supported mission. A realistic prediction for a MORA is simply to use the worst-case adversary's behavior based on:

- Relative Importance of Attacks
- Probability of Adversary Attempt
- Probability of Attack Success
- Adversary Willingness to Fail

Adversaries may be characterized by their willingness (probability of initiating) and ability (probability of completing) to engage in attacks that actually cause harm (degree of severity) to the organizational mission. Characterization is necessary to make the case based more on evidence then speculation as to what the adversary might do. It is impossible to predict an action based on capability alone. The analyst needs to build adversarial profiles based on adversarial:

- Interest
- Motivation
- History
- Skills Required (based on threats)
    - Scope
    - Sophistication of capabilities
    - Capability to develop a systematic attack process
    - Support organization
    - Intelligence gathering

Obtaining profile information is not the mission of threat analysis. Interest and stake is extremely important when considering sponsored adversaries. Most often it is hard to match the technology with specific adversary organizations and those they use to intrude on networks. While major and minor adversaries are easily identified, their internal relationships and motivations in times of pre-crisis, crisis, and conflict are more difficult to predict. For these conditions, it is easiest to determine the impact based on the assumption that the attack will always take place under worst-case conditions.

Rank the Technology Requirement to Each Mission

To determine the relative importance of mission impact based on the various threat, vulnerability, and attack conditions for each requirement area, some leveling method of comparison is needed. The following weighting is a suggestion and can be restructured based of unique mission needs. However, it should be understood that regardless of mission needs based on the threat to the primary application or some operational component, in the research arena other factors impact if a particular technology solution should be supported with available resources. Therefore, caution is used when weighting mission oriented needs against practical needs in solving a requirement. Avoid the trend to overweight this area.

There are different impacts to different types of actions based on the organization's mission and based on the ongoing activity (strategic, tactical, and operational) when a potential attack might take place. Before starting the weighting process, decompose the organization's mission.

Restate the organization's mission

- What are the mission phases?
- What functions must take place?
- In terms of specific systems and applications, what information and data is involved in performing these functions?
- How does the mission rely on this information and data?
- In relation to adversaries, is there a potential threat from a specific source?
- Are there potential vulnerabilities identified for a technology area? If not, is a potential vulnerability possible? If so, can the vulnerability result in a degradation loss in terms of:
    - Loss of Unauthorized knowledge of system information (loss of confidentiality)
    - Unauthorized changes to the system information or system design (loss of integrity)
    - Loss of authorized use of system information or services (loss of availability or denial of service)

These system or application degradation impacts include:

- Degradation of Functionality
- Degradation of Interoperability
- Degradation of Throughput
- Degradation of Ease of Use
- Degradation of Timeliness of Results
- Expenditure of Resources

Final Requirement Ranking

Results of the analysis describes mission impact on each of the system components in terms of a cyber-based attack resulting in the loss of a security service on applications associated with the system.

One means to collect data for ranking requirements equally is to create a questionnaire for representatives of all stakeholders to provide inputs. The questionnaire would ask stakeholders to select an answer based on the following questions. Once this activity is completed, weighted estimates can be made. For each adversary and identified vulnerability, determine first the impact to the system itself. Note that comparison levels are relative in that they do not represent scale, only impacts in terms of all other related impacts.

Rank Risk to Mission in terms of impact and likelihood of successful attack against known vulnerability.

Attack results in minor degradation with negligible impact.
- Strategic degradation – 2
- Tactical/Operational – 1

Attack results in some degradation with limited impact.
- Strategic degradation – 3
- Tactical degradation – 2
- Operational degradation – 1

Attack results in significant degradation that prevents large portions of mission.
- Strategic degradation – 5
- Tactical degradation – 3
- Operational degradation – 2

Attack results in major degradation that prevents mission accomplishment.
- Strategic degradation – 6
- Tactical degradation – 4
- Operational degradation – 3

Under some operational conditions, time considerations have a significant impact. Mitigation approaches can be automated, manual, or non-existent. When evaluating impact as a result of a delayed or a timely response to a crisis, the timing of an event could be considered in terms of how long the degradation impacts the mission's integrity or availability or how severe the confidentiality loss might be.

Time sensitivity
- One-time degradation quickly mitigated - 1
- Time-sensitive or one day degradation event - 2
- Continuous connection degradation or feed into a sensitive information source – 4

A requirement doesn't necessarily imply there is a specifically identified vulnerability to mitigate or that there are no current mitigation techniques in place, only that these techniques may be limited. Some requirements might be considered 'Grand Canyons' with many known or unknown vulnerabilities capable of impacting a mission, while others relate to overall improvement of current mitigation techniques, such as better situational awareness or training for analysts who detect attacks. Obviously, a direct known threat requires immediate attention, hence a higher weighting, but unknowns also require attention. Therefore, one approach is to

break a larger requirement into a more bounded solution approach and then treat it individually. The following weighting criteria are suggested:

Existing mitigation capability issues (Likelihood of Successful Attack and Mission Impact)
- Known vulnerability but no current mitigation capability - 6
- Limited operational mitigation capability - 3
- Time sensitive mitigation capability - 2
- Unknown vulnerability but no current mitigation capability - 1

Technology solution activity provides a partial solution to a known vulnerability
Technology solution activity provides measurable progress against a known vulnerability
Technology solution activity provides measurable progress against a potential but unknown vulnerability
Technology solution activity provides measurable overall progress against a known problem area

The final ranking in terms of mission impact for each technology solution is the result of a figure of merit based on a numeric weight summing all inputs. For the above suggested weighting comparisons, a range for mission impact of 16 units for each technology area is possible.

Analyze Time Constraints and Determine Feasibility

This section provides the basis for reshuffling requirement prioritization based on practical concerns. Simply knowing the existence of a requirement and how the mission might be impacted in the absence of a solution isn't sufficient to determine if a solution is feasible. Practical solutions are driven by technical opportunities and by researchers or users. Technical solutions must satisfy both agreed-upon needs of the customer and the capabilities of science to create solutions. Whether technology evolves per user requirements or through technology push, a complete understanding of the user's constraints will help avoid potential transition problems.

Historically at the outset of most projects, particularly in basic and applied research there is a considerable level of uncertainty as to the feasibility of such an undertaking. This is due to the fact that a project is usually a unique attempt to accomplish an endeavor that has never been done before and with resources that previously may not have been utilized in the same way. Therefore, a qualified judgmental approach to risk analysis regarding time and feasibility requires a broad understanding of both the technology involved and the capability of individuals or organizations to realistically provide a solution within a pre-determined time period.

Figure 5 below identifies the risk analysis steps necessary to make realistic time and feasibility comparisons between various technology solutions. This represents an approach for a more refined analysis of the stakeholder's highest ranked requirement needs, and not a process to be evaluated against all requirements.

Relate Mission Needs/Threats to Technology Solution Time

The initial mission impact ranking only provides a basis for reducing the total number of requirements to analyze. Once the impact due to the lack of a technology solution on mission success has been assessed, time and feasibility analysis will help focus the technology solution efforts on those requirements that can be practically supported. Immediacy is the "directness and intensity of interaction between two entities." In this case we define immediacy and the direct interaction between a high-level mission need and the practical feasibility of finding a solution

within an estimated time period. Not all requirements, regardless of their importance, can be solved with available resources and technology.

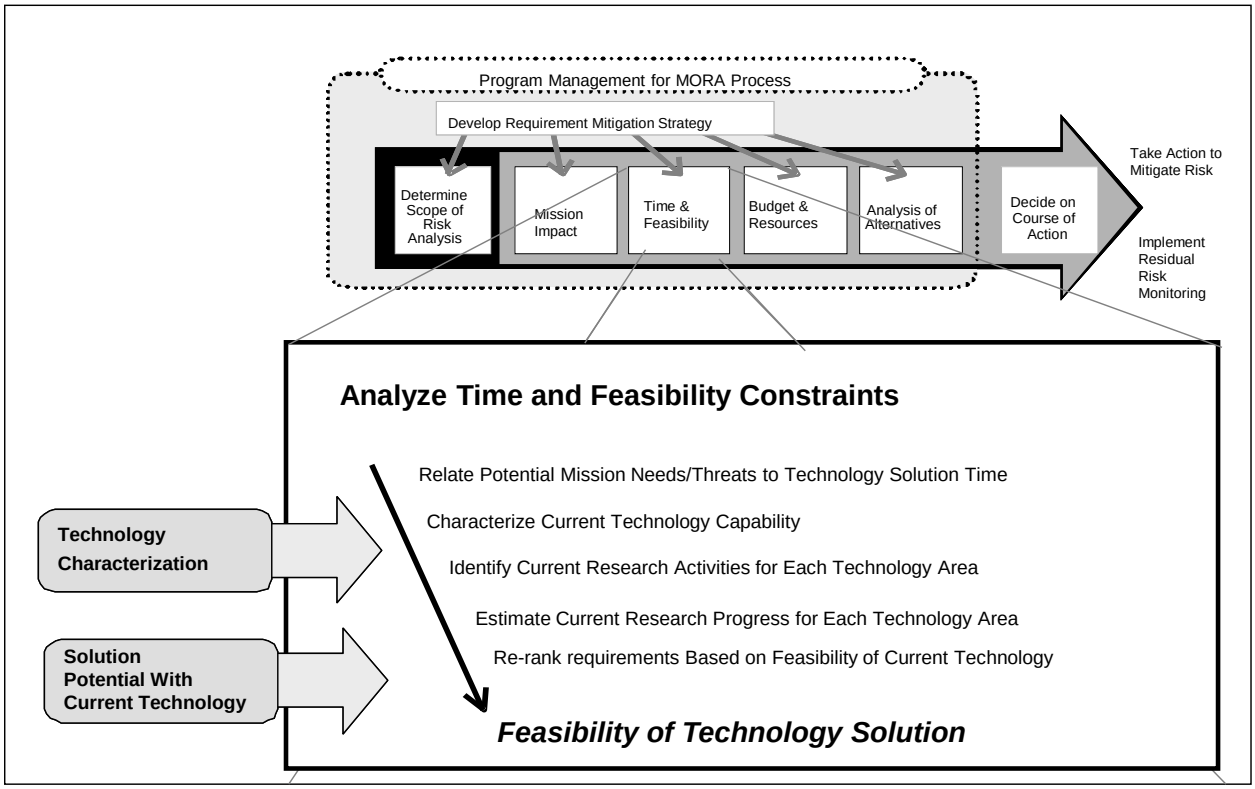

Figure 5 - Feasibility of Technology Solution

Characterize the Current Technology Capability

The rapid acquisition of network solutions is essential to mitigate the constantly changing threat/vulnerability environment. Further, the higher the technology readiness level for the technology achieved by the research community, the greater the probability of faster and more successful transition into an operational capability. In examining the capabilities of current technologies to solve CND requirements, it is essential to determine the maturity of these technologies. An estimate of maturity can be made by developing answers to the following questions:

- What is the requirement the research task is trying to resolve?
- How is it done today?
- What are the limitations of current practice?
- What technologies can be applied?
- What is new in the proposed approach / technology?
- Why do we think it will be successful?
- What evidence suggests the approach will work?

Selecting maturing technologies will be most successful in solving requirements. This MORA process forces the evaluation of each requirement based on maturity and practical considerations for research selection. It is important to understand that at this point we will be

addressing potential alternative solutions and determining swing weightings based on these alternatives for each of the remaining defined research requirements. Table 1 below depicts the analytical approach.

Table 1. Weighted Comparisons

Requirement #1 Swing Weight Comparisons (Not all Criteria Shown)									
	Time to Solve			Feasibility				Score	Rank
	1 yr	2 yr	4+yr						
Alternative 1									
Alternative 2									
Alternative 3									
Alternative 4									
Alternative X									

Identify Current Research Activities for Each Requirement

An effective means of assessing the feasibility and current state of a particular technology is through establishing a broad based consensus among stakeholders. The A workshop and interviews with leading researchers should be performed at least quarterly. Additionally, technology forecasts produced annually by various government and educational organizations should be reviewed as they become available. A questionnaire to facilitate the assessment of the state of the technology and applicability toward meeting the requirement should be completed by representatives from each stakeholder group, educational institutions, national research labs, and industry. The consolidated, weighted criteria based on the following suggested weighting, will result in a refined priority list.

Perceived maturity of technologies proposed for technology solution.

Mature – 2, Evolving - 1, Unknown - 0

Based on historical perspective, how long will it take for the underlying technology to evolve or a technology solution (partial or full) to exist?

One year – 5, two years – 3, More then 4 years - 1

Potential for a full solution or partial solution of a requirement based on current state of technology

Likely - 4, Partial (% x 2), Unlikely - 1, Unknown - 0

Difficulty/Risk of successful resolution

Low - 6, Medium -4, High - 2

Although requirements are unique, are there opportunities to combine like pieces of each requirement? If there were overlap in technologies then maybe one effort could solve different parts of other requirements.

High potential for combination – 4, Medium potential – 3, Unknown potential - 1

Do any of these have commercial or broader government potential?

High potential for combination – 6, Medium potential – 3, Unknown potential - 1

Estimate Current Progress for Each Technology Solution

The progress of a solution development against CND requirements will be judged differently if the proposed solution is a research activity or product integration. If a new product is suggested its capabilities must be matched to validated requirements. Technology can be driven by technical opportunities and by researchers or users. Whether technology evolves per user requirements or through technology push, understanding the user's constraints will help avoid potential transition problems.

When no current or partial technology solution is available prior to the development of the proposed product, the availability of a new solution is considered the highest priority. If a partial solution is available, but a new technology solution represents a leap ahead of previous approaches, then application of the following weighting criteria should be more applicable. Before performing the analysis, first determine what related research activities are ongoing and where they are located, and then estimate the progress of each research activity.

Available organizations that have performed significant research in this technology
More than four - 3, two to four – 2, single source or unknown - 1
Do you know of any similar product/research activity going on now (who/where?
Likely - 4, Partial 3, Unlikely - 1, Unknown – 0
Strength of proposed organization based on previous research activities
Established company – 3, Start-up –2, No other Products - 0
Commitment of organization to successful solution
Strong Management Team – 3, Single Manager/Researcher – 1, No visibility – 0
Strength of research staff. (Note that this criteria will be considered in more detail when performing resource estimates)
Strong Research Team – 3, Single Established Researcher – 2, First Time Research Project - 0
Has a proof of concept been performed
Proof-of-Concept but not Final Deliverable – 2, Good Idea Only - 1

If a product is proposed, it is suggested to use the following weighting criteria:

Potential competing organizations with a similar product
Single source or unknown – 3, One competitor - 2, Multiple Competitors – 1
Do you know of any organizations using the product (who/where)
Government - 4, Commercial 3, Unknown – 0
Strength of proposed organization to maintain logistical support based on previous similar product support
Established company – 3, Start-up –2, No other Products - 0
Commitment of organization to successful solution
Strong Management Team – 3, Small/Single Manager – 1, No visibility – 0
Capability of organization to upgrade with technology
Strong Engineering Team – 3, Small engineering team – 2
Has the product met government acceptance criteria
Government documentation available – 2, Commercial documentation only - 1

Budget and Resources Impact

At this stage of the risk analysis, each technology solution has been ranked based on mission impact and internal swing weighting based on feasibility is determined. Some additional fine-tuning is necessary before making a final determination of worth and a budget decision, particularly if new research is to be funded from among various proposed alternatives. This section deals with analyzing risks for various competing budget decisions. It is important to understand that at this point comparative costs are available.

In the business world, benefits are measured in terms of market choices. If a solution is considered too expensive, then it won't be solved regardless of the resources available. Benefits in the research and technology world should be based on expectations of results and evaluated based on projected benefits. However, people move to other projects, commercial organizations fail, operational needs require funding changes, and competing technologies or concurrent research activities often provide a cheaper, faster, or more comprehensive solution.

Early planning and aggressive execution ensure risk assessments support critical technical, schedule, and cost risks. In this manner, mitigation for both current risks and potential future risks can be planned. Planning is difficult since reality dictates that budgets are never exact and predicting research success is not an exact science.

Developing a Theory on Budget and Resource Impact is depicted in Figure 6. Traditional risk analysis relies primarily on cost, schedule and performance impacts. Underlying these factors are risks associated with who is performing the research and how long the research will take to complete. Therefore, when dealing with selecting the highest priority research requirement to fund based on limited people and budgetary resources, additional discriminators are necessary. This section provides guidelines for analyzing resource risks. The intent will be to characterize the following relationships in terms of capabilities in order to quantify the level of risk the stakeholder is exposed to in the overall risk analysis effort:

- Relationship of technology approach to individual researcher interest
- Relationship of technology approach to organizational interest
- Relationship of technology approach to organizational strength
- Relationship of technology approach to competing approaches

Characterize Human & Organizational Resource Research Risks

Although products are seldom designed to address everything needed to completely solve a CND requirement, research ideas are traditionally aimed at solving the problem they address. While the proposed research points towards a successful outcome, it does not assure its success. Therefore, organizations that fund a research activity based on a critical mission need without first analyzing the resources available take a significant risk in achieving overall success for their investment.

In research, budgeting people is as important as budgeting costs. People resources to support research activities fall into either researcher or organizational support. A CND requirement exists because a solution is difficult, often driven by technical unknowns. Solutions can require applying the most advanced researchers whose knowledge in a particular field will ensure the stakeholder has minimized uncertainties to the highest extent possible.

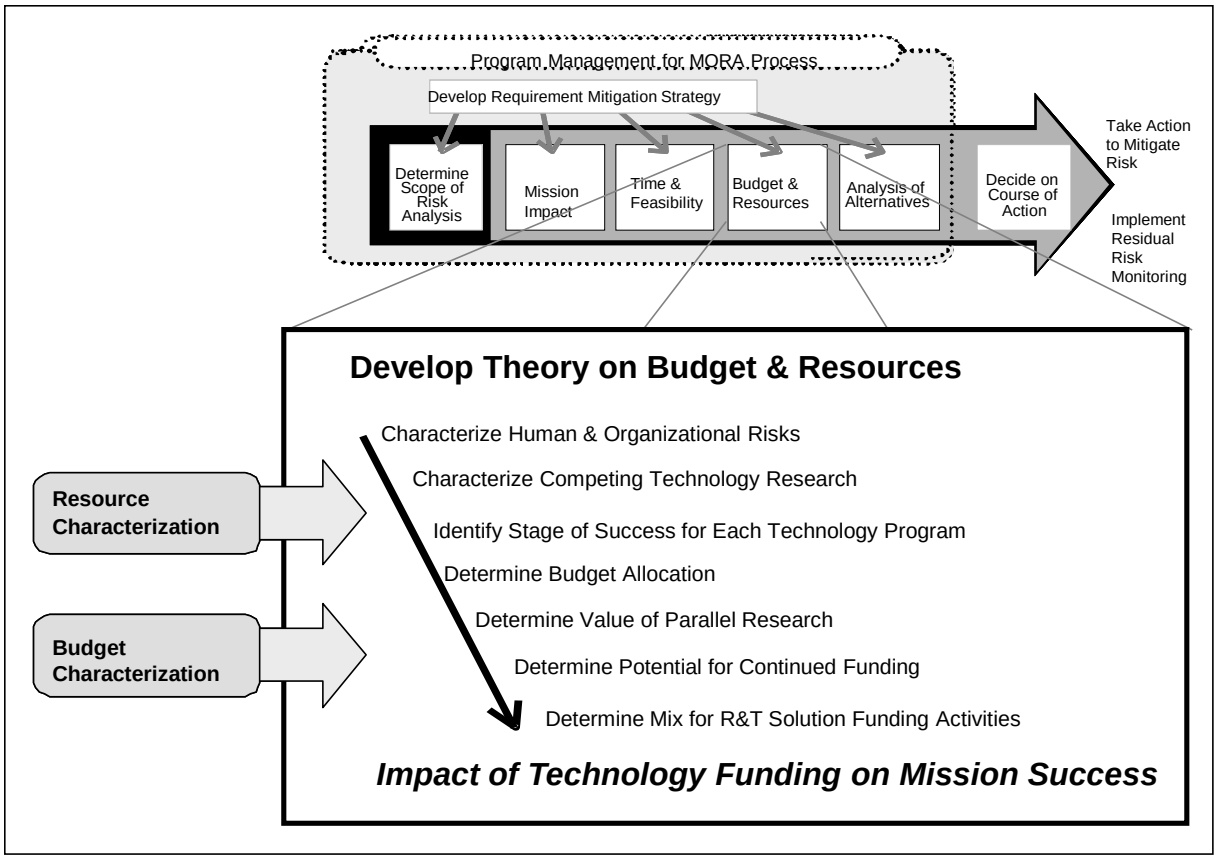

Figure 6. Impact of Technology Funding on Mission Success

Scope of Human and Organizational Related Research Risks to Consider

If a decision regarding various research activities to budget is being considered, answers to the following questions can be used to determine prioritizations:

Is the research team capable of solving the requirement?

Strength of Key Researcher Resume

Advanced degree in related field – 2, No unique educational factor - 0

Experience in directly related field – 3, Similar experience – 2

Does the organization have technical resources they can draw from to ensure technology risks are minimized?

Alternative researcher as lead on prior similar successful research programs – 3, Alternative researcher supported prior similar successful research programs - 2

What metrics should be considered in determining success or failure during phases of the overall research or development process?

Proposed measurable metrics are realistic – 3, Metrics have been developed - 2

Characterize Competing Technology Research

Risk associated with competing technology solutions is difficult to predict. In general, capital costs should not be a decisive factor in technology selection. However, migration costs for users in terms of training next generation skills will impact the time and risk of implementing a final technology solution.

Does the proposed technology solution offer a significant improvement over a competing technology?

Users will be able to quickly adapt to the new technology – 3, Lead time for adaptation necessary – 2, Potential for significant training – 1, Difficult adaptation - 0

No significant impact on the legacy environment – 2, Some impact expected – 2, Significant impact expected - 0

Estimate flexibility when upgrading is necessary: Significant flexibility – 3, Moderate flexibility – 2, Inflexible - 0

Identify Stage of Success for Each Technology Solution Program

Estimate the value of pursuing parallel solution activities.

A strong potential exists for this approach to reach a successful solution sooner then any other approaches – 3

Estimate if a potential competing commercial solution will evolve before investment costs are recovered: No commercial solution or solution within 3 years – 3, Commercial solution within 2 years – 1, Commercial solution within 1 year - 0

Budget Allocation

The total cost to develop and transition a product is not the sole determinant for deciding on which research effort to budget. Actual costs can be estimated in terms of lack of funding for immediate operational needs and enhancement or loss of organizational capabilities, particularly as they relate to future competitive costs. Although no weighting criteria are suggested, the following questions provide guidelines for considering actual allocation issues.

- What budgetary resources are required and are they available?
- Have all costs been considered such as development, acquisition, documentation, integration/installation/impact on existing infrastructure, certification/accreditation, and life-cycle?
- How might future budget restrictions impact the technology transition prior to completion?
- What is the risk to research organizations if continued funding is not available?
- What is the value of maintaining equivalent capabilities at different organizations?

Potential for Continued Funding

Historically, enterprises that build applications based on untested architectures routinely exceed their budget for development. Similarly, research activities often exceed early budget estimates, plus are often cut prior to transition when operational funding gains higher priority. For this reason, accurate funding estimates based on measurable metrics and bridge funding

during new budgeting periods involve risk. The following questions are suggested to address these issues for planning:

- Is sufficient funding available to completely cover research and development costs for transition?
- If there is a funding cut, will the sponsor be able to recover the technology solution proposed within six months without serious impact?
- Have development milestones or breaks in work been considered for places that would support the least impact on recovery?

Determine Mix for Research Funding Activities

The final research solutions to fund are based on those representing the best value, with the least immediate risk of failure, and the highest need based on mission objectives. This approach satisfies the short-term managed risk criteria for successful program management. However, the approach does not take into account the longer-term objective of critical CND requirements.

In a perfect world, all technology requirements could be broken down into focused subsets, and after analysis themes would emerge as to what technologies could potentially be applied to solve the problem components. Addressing R&T problems in terms of smaller components will help focus research activities to achieve steady progress towards solving difficult overarching issues. The problem is that some requirements are so large that a piecemeal approach to a solution won't work. However, if partial solutions are not attempted, then final complete solutions might not eventually emerge.

An approach to solving these "longer-term" problems is to selectively fund a mix of activities, some of which are not specifically directed at a formal solution during the life of the task. These research activities are directed more towards proof-of-concept studies or better definitions of the problem. After immediate research and development needs are addressed, it is recommended to select a small number of research proposals that address some subset problem area of those requirements considered "Grand Canyons."

Analysis of Alternatives

This section details the formal trade-off process for requirement prioritization and proposal or solution selection. The actual decision about the best requirements to select is not part of the formal risk analysis process. It is, however, part of the risk management process and the ultimate focus of the analysis; to provide the most useful and meaningful data and analytical insights to support critical risk decisions. Utilizing the R&T MORA process for each research initiative, the decision maker can be presented with:

- Alternative courses of actions
- Their pros and their cons
- "Expert opinion" recommendations on the course of action
- Comparative cost analysis results

Of course, once decisions on which technology solutions to proceed with have been made, the risk management cycle is not complete. By modifying the Time and Feasibility and the Budget and Resources sections of MORA, projects can be re-analyzed at discrete points such that the continuing risks can be evaluated.

Summary of Mission Critical Parameter Trade-Off

The mission critical parameter trade-off information puts the entire MORA process into perspective. It better informs the decision maker, allowing the testing of various changes in models assumptions (sensitivity analysis) and providing support to recommended alternatives. Ultimately, it comes down to the decision maker's understanding of the problems and issues, their confidence in the data and insights presented to them, their own intuitive weighting of the various and complex mission critical parameters, and their belief about future circumstances that influence their decisions. The analysis process provides the best insight to support the decision maker's decisions.

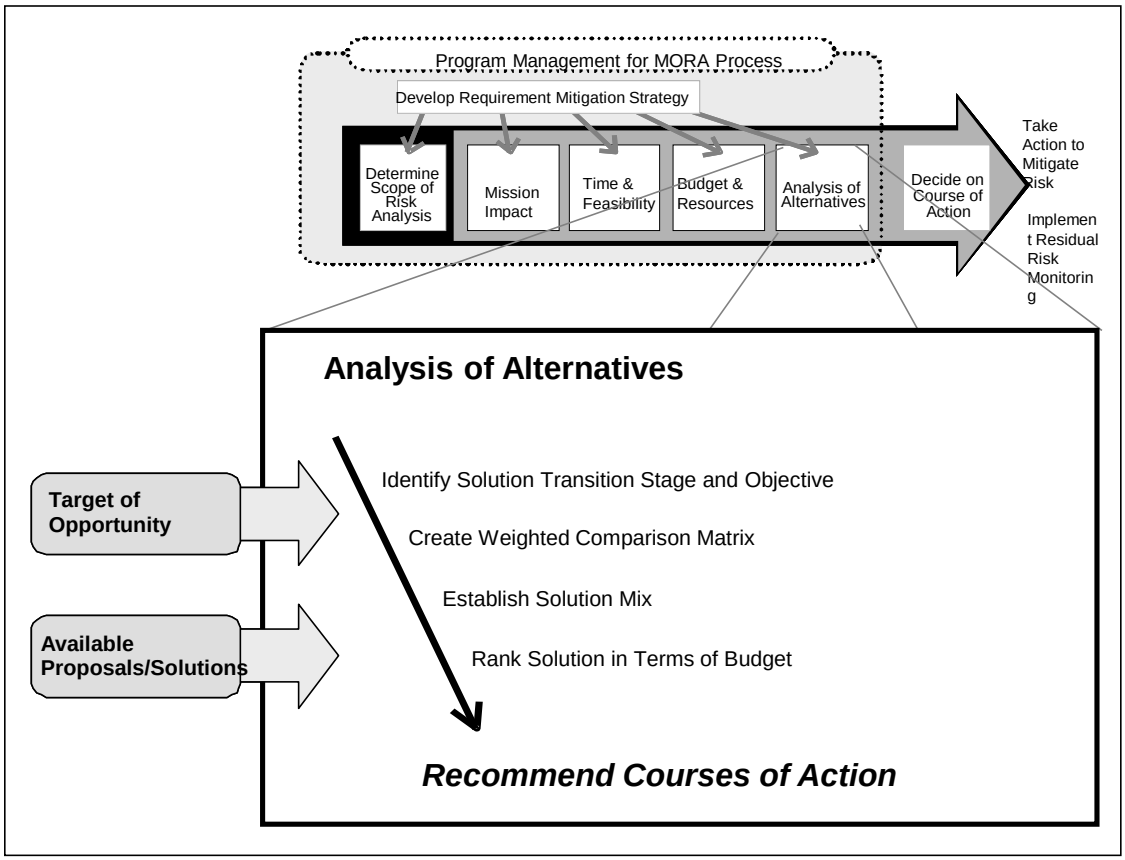

Figure 7. Analysis of Alternatives

As previously described, an initial requirement reduction process based on subject matter expert opinions should be performed prior to the formal mission impact analysis. This is not mandatory, but is a realistic way to reduce the total amount of analysis that will be necessary. For a more thorough initial requirement reduction, the analyst should use a small sampling of questions such as those in the matrix below, Table 2, to reduce the overall number of requirements to be analyzed.

Table 2. Initial Reduction of CND Research and Technology Solutions Based on SME Inputs

Rank	Rqmt. Desc.	Potential for a Solution	Similar product or research available	Risk in a successful solution	Opportunity to combine	Commercial potential	Cost estimate	Best SME guess of priority

After the initial reduction, create a prioritization matrix, Table 3, based on cumulative scores from each of the factors described in the mission impact section.

Table 3. Mission Impact Ranking

Initial Rank	Rqmt. Desc.	Risk to mission	Time sensitivity	Existing mitigation capability	Any other relevant factor	Total weight

The final requirement ranking should take into account the state of current technology as well as the difficulty in solving a particular requirement. It is likely that some requirements are high on the list of mission priorities, but for practical reasons may not be solvable with current techniques. Therefore, after reducing the remaining list of requirements to the most important in terms of mission impact, analyze each requirement in terms of feasibility and reshuffle the list based on final weightings, Table 4.

Table 4. Feasibility Ranking

Final Rank	Rqmt.. Desc.	Mission impact weight	Current technology weight	Existing product or research solution	Any other relevant factor	Total weight

Cost Benefit Comparison

Ranking and prioritization are essential to focus research actions, but in order to reach a final conclusion as to the desirability of a project, all aspects of the project, positive and negative, must be expressed in terms of a common unit; i.e., there must be a "bottom line." The most convenient common unit is money. This means that all benefits and costs of a project should be measured in terms of their equivalent money value. A program may provide benefits which are not directly expressed in terms of dollars but there is some amount of money the recipients of the benefits would consider just as good as the project's benefits. Therefore, an accurate prediction of all projected costs is necessary prior to the final cost benefit analysis.

Budgeting and resources relate to who has proposed a solution, if the solution is a product solving the entire requirement or a subset of the requirement, or if the solution is research resulting in better understanding or enhancing technology that might eventually result in a technology solution. Using the budget and resource weighting provides a comparative means of determining the financial soundness of a particular technology solution against all others. However, the final cost benefit comparison should relate back to mission impact.

Recommend Course of Action

Placing a value on worth is the most difficult metric to determine. From the Mission Impact and above Analysis of Alternatives studies, a set of characteristics can be captured in a table similar to Table 5 below and the changes to mission impact as a result of attacks can be re-entered into the impact analyses to determine the change in “benefit” due to the implementation of a successful countermeasure or technology solution. To determine the change in net benefit, the additional fixed and continuing financial and non-financial costs need to be incorporated into the cost benefit calculation.

Table 5. Ranking Course of Action Against Cost Benefit

Course Of Action	***Change In Adversary Risk for All Attacks and Adversaries***	***Change In Success Given Attempt for All Attacks and Adversaries***	***Change In Impact Given Success for All Attacks and Adversaries***	***Additional Non-Financial Costs***	***Additional Financial Costs***	***Net Change In Benefit Due to Course of Action***
Status Quo (Baseline = Existing)	None	None	None	None	None	None
Technology Solution 1	Increases Likelihood of Detection (Reduces consequences)	None	None	Decreases Interoperability	Moderate Acquisition Costs Low Maintenance Costs	Moderate negative Net Benefit (Net Utility)

Technology Solution 2	Increases Likelihood of Detection and Attribution (Reduces both consequences and likelihood of attempt	Greatly Reduces Access Required for Many Attacks	None	Decreases Interoperability Decreases Ease of Use	High Acquisition Costs Low* Maintenance Costs	Moderate positive Net Benefit (Net Utility)

*Note that low, medium and high are relevant terms and should be weighted based on individual perspectives.

Development Program Risk Analysis

The following section describes risk analysis techniques that help program managers deal with risk management decisions after a particular development program has been awarded. Many traditional risk management approaches are used by different organizations and they are acceptable. This section identifies one risk management technique based on cost, schedule and performance risks.

Requirement selection, funding, and partnering decisions using the MORA approach supported decision-making by helping to answer the following questions:

Investment/Technology Strategy

- What are the critical research requirements and priorities?
- What level of investment is required?
- What is the market potential for investment opportunities?
- How should the performance of the technology development be evaluated?

Partnering Strategy

- What is the value proposition to our research / investment partners
- What is the right mix of participants (VC, labs, academia, tech firms …)
- What is the payout structure (fee, grants, options / equity)
- What commitments do we expect?
- What level of influence / control do we require?

Operation Model

- What are the key activities that need to be performed?
- What resources/skills are required to administer the funds?
- What are the extended enterprise strategy, organizational architecture, and governance plan?
- What is the implementation roadmap?

Once the research or development process is initiated, various risk management approaches exist to minimize design, test, and production risks. During the development process, the risk factors are used to drive prioritization of systems engineering needs. Each risk factor is individually analyzed in terms of its specific potential for impacting the overall program in terms of cost, schedule, final performance or solution based on total requirement. Selecting the appropriate figure of merit that will indicate a percent of impact is left to the reader. As in the

MORA process, the intent is to apply weighting criteria such that the various risks can be evaluated on an equal basis.

The following approach is suggested to manage these process-oriented risks:

Cost Risks

Cost Impact Rating			
Rating	**Risk Elements Impacted**	**Unique Risk Element**	**Impact of risk is a xx% cost overrun**
	Management - Program Management/Infrastructure	a. b. …	
	Design/Development		
	Resources		
	Support Documentation		
	Budget		

Schedule Risks

Schedule Impact Rating			
Rating	**Risk Elements Impacted**	**Unique Risk Element**	**Impact of risk is a xx% cost overrun**
	Management - Program Management/Infrastructure	a. b. …	
	Design/Development		
	Resources		
	Support Documentation		
	1.1.1.1 Budget		

Performance Risks

Performance Impact Rating			
Rating	**Risk Elements Impacted**	**Unique Risk Element**	**Impact of risk is a xx% cost overrun**
	Management - Program Management/Infrastructure	a. b. …	
	Design/Development		
	Resources		
	Support Documentation		