

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

DISSERTATION

QUANTIFYING RISK FOR DECENTRALIZED OFFENSIVE CYBER OPERATIONS

by

Michael S. Klipstein

June 2017

Dissertation Supervisor Kent Wall

Approved for public release. Distribution is unlimited.

Reissued 7 Sep 2017 with corrections to committee titles.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2017	**3. REPORT TYPE AND DATES COVERED** Dissertation	
4. TITLE AND SUBTITLE QUANTIFYING RISK FOR DECENTRALIZED OFFENSIVE CYBER OPERATIONS			**5. FUNDING NUMBERS**
6. AUTHOR(S) Michael S. Klipstein			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number NPS.2016.0031-IR-EP7-A.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

As computer networks have become ubiquitous, the amount of information stored within government computer networks has grown exponentially. With the possibility of further decentralization of authorities to conduct offensive cyber operations, organizations below the national level are unable to adequately assess risks and the associated consequences of these offensive operations due to the lack of exposure, experience, and education of staff personnel. Compounding this problem are the heuristics and biases used in decision making when the requisite expertise is absent. This lack of understanding of risks and potentially faulty decision making presents a gap in command and control structures. This research explores the question: *How effective is a simulation framework incorporating both subject matter expertise and assessments of uncertainty at overcoming the inexperience of decision makers in assessing risk and subsequent decision making within new operations?* This research effort expands multi-criteria decision-making theory by accounting and incorporating both the expertise and uncertainty of the experts into the framework. This proposed framework was tested at national-level cyber organizations and CCMD exercises. The results were then compared to see if the framework could mitigate inexperience. The results are that organizations unfamiliar with cyber operations are able to assess risks at a proficiency level equivalent to an experienced organization.

14. SUBJECT TERMS risk; cyber risk; cyber operations; offensive cyber operations; decentralization			**15. NUMBER OF PAGES** 307
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

QUANTIFYING RISK FOR DECENTRALIZED OFFENSIVE CYBER OPERATIONS

Michael S. Klipstein
Major, United States Army
B.A., Columbia College of Missouri, 2007
M.S., University of Maryland, College Park, 2011

Submitted in partial fulfillment of the
requirements for the degree of

DOCTOR OF PHILOSOPHY IN INFORMATION SCIENCES

from the

NAVAL POSTGRADUATE SCHOOL
June 2017

Approved by:

Kent Wall
Professor Emeritus of
Systems Engineering
Dissertation Supervisor

Dan C. Boger
Chair of Information Sciences
Dissertation Committee Chair

Alex Bordetsky
Professor of Information
Sciences

Raymond Buettner
Associated Professor of Information
Sciences

Douglas MacKinnon
Professor of Information
Sciences

Approved by: Dan C. Boger, Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

As computer networks have become ubiquitous, the amount of information stored within government computer networks has grown exponentially. With the possibility of further decentralization of authorities to conduct offensive cyber operations, organizations below the national level are unable to adequately assess risks and the associated consequences of these offensive operations due to the lack of exposure, experience, and education of staff personnel. Compounding this problem are the heuristics and biases used in decision making when the requisite expertise is absent. This lack of understanding of risks and potentially faulty decision making presents a gap in command and control structures. This research explores the question: How effective is a simulation framework incorporating both subject matter expertise and assessments of uncertainty at overcoming the inexperience of decision makers in assessing risk and subsequent decision making within new operations? This research effort expands multi-criteria decision-making theory by accounting and incorporating both the expertise and uncertainty of the experts into the framework. This proposed framework was tested at national-level cyber organizations and CCMD exercises. The results were then compared to see if the framework could mitigate inexperience. The results are that organizations unfamiliar with cyber operations are able to assess risks at a proficiency level equivalent to an experienced organization.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. CURRENT SITUATION....1
B. MULTIDISCIPLINARY RESEARCH....1
C. HYPOTHESIS, RESEARCH QUESTION, AND POTENTIAL CONTRIBUTIONS....2

II. COMMAND AND CONTROL: C2 RISKS....5
A. INTERDEPENDENCE OF COMMAND AND CONTROL ELEMENTS....5
B. RISK CONCERNS OF COMMAND AND CONTROL....6
C. RISK ASSESSMENT....8
D. PROBLEMS WITH QUALITATIVE RISK ASSESSMENT MODELS....9
E. PROMISES OF QUANTITATIVE ASSESSMENT METHODS....10

III. CYBER OPERATIONS AND RISKS....13
A. A GROWING THREAT....14
B. TYPES OF CYBER OPERATIONS....15
1. Offensive Cyber Operations....15
2. Intelligence Gathering Operations....17
C. RISKS IN CYBER OPERATIONS....18
D. CAPABILITY DEVELOPMENT RISKS....19
1. Risk of Loss of Adversary Network Access....19
2. Risk of Capability Loss....24
E. OPERATIONAL RISKS....27
1. Risk to Operations....27
2. Risks of Compromise....29
3. Risk of Attribution....31
4. Risk of Retaliation....33

IV. COGNITIVE ASPECTS OF DECISION MAKING....35
A. COGNITIVE DECISION MAKING PROCESS....36
B. HEURISTICS....37
1. Representativeness....37
2. Availability....38
3. Anchoring and Adjustment....39
4. Affect....41

C. BIAS 42
1. Confirmation Bias 42
2. Attention Bias 43
3. Belief Bias 43
4. Clustering Illusion 43
D. GROUP DYNAMICS 44
E. OVERCONFIDENCE VERSUS OVERESTIMATION OF RISK 45

V. DECISION MAKING WITH MULTIPLE OBJECTIVES 49
A. THE MODELING OF DECISION MAKER PREFERENCE UNDER CERTAINTY 49
B. CONSTRUCTING THE ADDITIVE MODEL OF DECISION MAKER PREFERENCES UNDER CERTAINTY 51
1. Constructing Decision Maker Individual Value Functions 51
2. Modeling Decision Maker Tradeoff Weights 53
C. CONSTRUCTING AN ADDITIVE MODEL FOR COST-EFFECTIVENESS 55

VI. RISK MODELING 57
A. A BRIEF HISTORY OF RISK 57
B. CONTEMPORARY DEFINITIONS OF RISK 58
C. A QUANTITATIVE DEFINITION OF RISK 59
D. LIMITATIONS OF THE EXPECTED UTILITY THEORY APPROACH TO RISK 60
1. Substitution Axiom 60
2. Loss Aversion 61
3. The Ambiguity Effect 62
4. Framing Effects 63
E. THE APPLICATION OF THE QUANTITATIVE DEFINITION OF RISK TO CYBER OPERATIONS 63
1. Answering the First Question 63
2. Answering the Second Question 66
3. Answering the Third Question 66
4. Answering the Fourth Question 66
F. A PRACTICAL IMPLEMENTATION IN CYBER OPERATIONS 69

VII. METHODS 73
A. DESIGN 73
B. RESEARCH QUESTION AND HYPOTHESIS 73

C. PARTICIPANTS AND SETTINGS 74
1. Subject Matter Experts 74
2. Scenarios 75
3. Combatant Command Cyber Planners 77
D. INSTRUMENTATION 78
1. Risk Attitude Assessment 79
2. Objective Hierarchy Construction 79
3. Effectiveness 80
4. SME Elicitation 83
5. Modeling Effectiveness 85
6. Cost 88
7. Modeling Costs 90
8. Graphic Output 91
E. PROCEDURES 92
F. EXPERIMENTAL PROCESS 94
G. EXPERIMENTAL DATA OUTPUTS 95

VIII. DATA ANALYSIS 99
A. RISK ATTITUDES AND PROFILES 100
B. SCENARIO 1A 103
1. Scenario 1A with All Participants 103
2. Scenario 1A with Experienced Personnel Removed 107
3. Scenario 1A with Inexperienced Personnel Removed 108
4. Scenario 1A with USCYBERCOM Personnel Only 110
5. Scenario 1A Conclusions 111
C. SCENARIO 1B 112
1. Scenario 1B with All Participants 112
2. Scenario 1B with Experienced Personnel Removed 115
3. Scenario 1B with Inexperienced Personnel Removed 117
4. Scenario 1B with USCYBERCOM Personnel Only 118
5. Scenario 1B Conclusions 119
D. SCENARIO 2 120
1. Scenario 2 with All Participants 121
2. Scenario 2 with Experienced Personnel Removed 124
3. Scenario 2 with Inexperienced Personnel Removed 125
4. Scenario 2 with USCYBERCOM Personnel Only 127
5. Scenario 2 Conclusions 128
E. SCENARIO 3 129
1. Scenario 3 with All Participants 129
2. Scenario 3 with Experienced Personnel Removed 133

3. Scenario 3 with Inexperienced Personnel Removed 134
4. Scenario 3 with USCYBERCOM Personnel Only 136
5. Scenario 3 Conclusions 137
F. SCENARIO 4 138
1. Scenario 4 with All Participants 138
2. Scenario 4 with Experienced Personnel Removed 141
3. Scenario 4 with Inexperienced Personnel Removed 142
4. Scenario 4 with USCYBERCOM Personnel Only 144
5. Scenario 4 Conclusions 145
G. SCENARIO 5 145
1. Scenario 5 with All Participants 146
2. Scenario 5 with Experienced Personnel Removed 149
3. Scenario 5 with Inexperienced Personnel Removed 151
4. Scenario 5 with USCYBERCOM Personnel Only 152
5. Scenario 5 Conclusions 154

IX. ANALYSIS OF RESULTS 157
A. TRENDS 157
1. Inexperienced Personnel Overcome a Lack of Experience 157
2. Value for Experienced Personnel 158
3. Use of Region 1 for Decision Making 159
B. INTEGRATION WITH THE EXISTING LITERATURE 160
C. GENERALIZABILITY 161
D. LIMITATIONS 161
E. FURTHER RESEARCH 162
1. Information Ranking, Viewing, and Incorporating 162
2. Piecewise Linear Model 163
3. Potential Use of Other Models for Representing SME Assessments 165
4. Overconfidence in SME Values 165
5. Descriptive Models of Decision Maker Choice Behavior 166
6. Framework Automation 166
F. CONCLUSIONS 167

APPENDIX A. NSA PREPUBLICATION EVALUATION 169

APPENDIX B. SME DEMOGRAPHICS 171

APPENDIX C. SCENARIO DISTRIBUTION MATRIX 173

APPENDIX D. SME ELICITATION SCORES 175

APPENDIX E. SAMPLE DOSPERT QUESTIONNAIRE 181

APPENDIX F. SME ELICITATION PACKET 185

APPENDIX G. PARTICIPANT DEMOGRAPHICS 231

APPENDIX H. PARTICIPANT SCENARIOS AND GRAPHICS 233

APPENDIX I. IRB APPROVAL 259

SUPPLEMENTAL 261

LIST OF REFERENCES 263

INITIAL DISTRIBUTION LIST 277

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Combined and Layered Aspects of this Research....2
Figure 2. Example Graphical Depiction of Mid-Value Spitting....52
Figure 3. Example Graphing Output of Decision Maker Values for Hierarchy Goals....53
Figure 4. Illustration of Tradeoff Weight Determination....55
Figure 5. Example Sigmoid Curve of a Prospect Fuction. Source: Kahneman & Tversky (1979)....62
Figure 6. Top Level of Objective Hierarchy Illuminating the Decision Maker's Concerns....64
Figure 7. Example of SME Distribution of Costs....69
Figure 8. Dials for Adjusting for Decision Maker Weight....71
Figure 9. Example Graphical Outputs as Evidence in a Staff Recommendation....72
Figure 10. Maximizing Damage Hierarchy....81
Figure 11. Maximizing Intelligence Hierarchy....82
Figure 12. Minimizing Detection Hierarchy....83
Figure 13. Minimizing Attribution Given Detection Hierarchy....85
Figure 14. Minimizing Compromise Given Detection Hierarchy....86
Figure 15. Example of an Elicitation with Less Uncertainty....86
Figure 16. Example of an Elicitation with More Uncertainty....87
Figure 17. Example Table of SME Elicitations for a Given Scenario....87
Figure 18. Minimizing Cost Hierarchy....89
Figure 19. Example Distribution of Costs for a Given Alternative....91
Figure 20. Sample Simulation Output....93
Figure 21. Mapping of Written CoA to Graphical CoA....94
Figure 22. Example of Amount of Sum of Rank Order Changes in Monte Carlo Simulation Analysis....96
Figure 23. Example of Cross Tabulation of Participant-Provided Data....96
Figure 24. Example Monte Carlo Sampling Simulation Output Distribution....97
Figure 25. ANOVA Results of Risk Seeking Tendencies for Four Groups of Participants....101

Figure 26. ANOVA Results of Risk Seeking Tendencies for Two Groups of Participants....102
Figure 27. Scenario 1 with All Participants....104
Figure 28. Scenario 1A Choices and Change for All Participants and Nothing Held Constant....105
Figure 29. Scenario 1A with Experienced Personnel Held Constant....106
Figure 30. Scenario 1A with Inexperienced Personnel Held Constant....107
Figure 31. Scenario 1A with Experienced Personnel Removed....108
Figure 32. Scenario 1A Choices and Change with Experienced Personnel Removed....108
Figure 33. Scenario 1A with Inexperienced Personnel Removed....109
Figure 34. Scenario 1A Choices and Change with Inexperienced Personnel Removed....110
Figure 35. Scenario 1A with USCYBERCOM Personnel Only....111
Figure 36. Scenario 1A Choices and Change with USCYBERCOM Personnel Only....111
Figure 37. Scenario 1B with All Participants....113
Figure 38. Scenario 1B Choices and Change for All Participants and Nothing Held Constant....113
Figure 39. Scenario 1B with Experienced Personnel Held Constant....114
Figure 40. Scenario 1B with Inexperienced Personnel Held Constant....115
Figure 41. Scenario 1B with Experienced Personnel Removed....116
Figure 42. Scenario 1B Choices and Change with Experienced Personnel Removed....116
Figure 43. Scenario 1B with Inexperienced Personnel Removed....117
Figure 44. Scenario 1B Choices and Change with Inexperienced Personnel Removed....118
Figure 45. Scenario 1B with USCYBERCOM Personnel Only....119
Figure 46. Scenario 1B Choices and Change with USCYBERCOM Personnel Only....119
Figure 47. Scenario 2 with All Participants....121
Figure 48. Scenario 2 Choices and Change for All Participants and Nothing Held Constant....122
Figure 49. Scenario 2 with Experienced Personnel Held Constant....123
Figure 50. Scenario 2 with Inexperienced Personnel Held Constant....124

Figure 51. Scenario 2 with Experienced Personnel Removed 125
Figure 52. Scenario 2 Choices and Change with Experienced Personnel Removed 125
Figure 53. Scenario 2 with Inexperienced Personnel Removed.....126
Figure 54. Scenario 2 Choices and Change with Inexperienced Personnel Removed 127
Figure 55. Scenario 2 with USCYBERCOM Personnel Only 128
Figure 56. Scenario 2 Choices and Change with USCYBERCOM Personnel Only.....128
Figure 57. Scenario 3 with All Participants 130
Figure 58. Scenario 3 Choices and Change for All Participants and Nothing Held Constant.....131
Figure 59. Scenario 3 with Experienced Personnel Held Constant.....132
Figure 60. Scenario 3 with Inexperienced Personnel Held Constant 133
Figure 61. Scenario 3 with Experienced Personnel Removed 134
Figure 62. Scenario 3 Choices and Change with Experienced Personnel Removed 134
Figure 63. Scenario 3 with Inexperienced Personnel Removed.....135
Figure 64. Scenario 3 Choices and Change with Inexperienced Personnel Removed 136
Figure 65. Scenario 3 with USCYBERCOM Personnel Only 137
Figure 66. Scenario 3 Choices and Change with USCYBERCOM Personnel Only.....137
Figure 67. Scenario 4 with All Participants 139
Figure 68. Scenario 4 Choices and Change for All Participants and Nothing Held Constant.....139
Figure 69. Scenario 4 with Experienced Personnel Held Constant.....140
Figure 70. Scenario 4 with Inexperienced Personnel Held Constant 141
Figure 71. Scenario 4 with Experienced Personnel Removed 142
Figure 72. Scenario 4 Choices and Change with Experienced Personnel Removed 142
Figure 73. Scenario 4 with Inexperienced Personnel Removed.....143
Figure 74. Scenario 4 Choices and Change with Inexperienced Personnel Removed 143
Figure 75. Scenario 4 with USCYBERCOM Personnel Only 144

Figure 76. Scenario 4 Choices and Change with USCYBERCOM Personnel Only....145
Figure 77. Scenario 5 with All Participants....147
Figure 78. Scenario 5 Choices and Change for All Participants and Nothing Held Constant....147
Figure 79. Scenario 5 with Experienced Personnel Held Constant....148
Figure 80. Scenario 5 with Inexperienced Personnel Held Constant....149
Figure 81. Scenario 5 with Experienced Personnel Removed....150
Figure 82. Scenario 5 Choices and Change with Experienced Personnel Removed....151
Figure 83. Scenario 5 with Inexperienced Personnel Removed....152
Figure 84. Scenario 5 Choices and Change with Inexperienced Personnel Removed....152
Figure 85. Scenario 5 with USCYBERCOM Personnel Only....153
Figure 86. Scenario 5 Choices and Change with USCYBERCOM Personnel Only....154
Figure 87. Consolidated Account of Analysis by p-value....155
Figure 88. Example Piecewise Linear Elicitation of Decision Maker Values for a Maximization Objective....164
Figure 89. Example Piecewise Linear Elicitation of Decision Maker Values for a Minimization Objective....165

LIST OF ACRONYMS AND ABBREVIATIONS

ARM	Advanced RISC Machine
CNA	Computer Network Attack
CCMD	Combatant Command
CD	Compact Disk
CNE	Computer Network Exploitation
CNMF	Cyber National Mission Force
COA	Course of Action
DCO	Defensive Cyber Operations
DODIN Ops	Department of Defense Information Network Operations
DOSPERT	Doman-Specific Risk-Taking
DVD	Digital Video Disk
FCAPS	Fault, Configuration, Accounting, Performance, Security
FOSD	First Order Stochastic Dominance
HW	Hardware
IMEI	International Mobile Equipment Identity
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISR	Intelligence, Surveillance, and Reconnaissance
LAN	Local Area Network
NIST	National Institute of Standards and Technology
NPS	Naval Postgraduate School
OCO	Offensive Cyber Operations
OPT	Operational Planning Team
OSI	Open Systems Interconnection Group
PLA	People's Liberation Army
PSP	Personal Security Products
SCADA	Supervisory Control and Data Acquisition
SIGINT	Signals Intelligence
SME	Subject Matter Expert
SOP	Standard Operating Procedures

SR	Surveillance and Reconnaissance
SW	Software
TSOC	Theater Special Operations Command
TTP	Tactics, Techniques, and Procedures
USAFRICOM	United States Africa Command
USB	Universal Serial Bus
USCENTCOM	United States Central Command
USCYBERCOM	United States Cyber Command
USEUCOM	United States European Command
USNORTHCOM	United States Northern Command
USPACOM	United States Pacific Command
USSOCOM	United States Special Operations Command
USSOUTHCOM	United States Southern Command

EXECUTIVE SUMMARY

A. MOTIVATION

This dissertation provides a proof-of-concept for a new framework for assessing risks in decision making in new or novel situations by using a multi-disciplinary approach. This framework provides a tailor-made expression of risk based on the decision maker's preferences and desires. The research setting for this experiment is the staff of combatant commands who must analyze risks to arrive at recommendations of courses of action (COA) regarding offensive cyber operations. In this research, offensive cyber operations are defined as both intelligence operations, such as computer network exploitation, as well as computer network attacks. This multidisciplinary approach is shown in Figure ES-1.

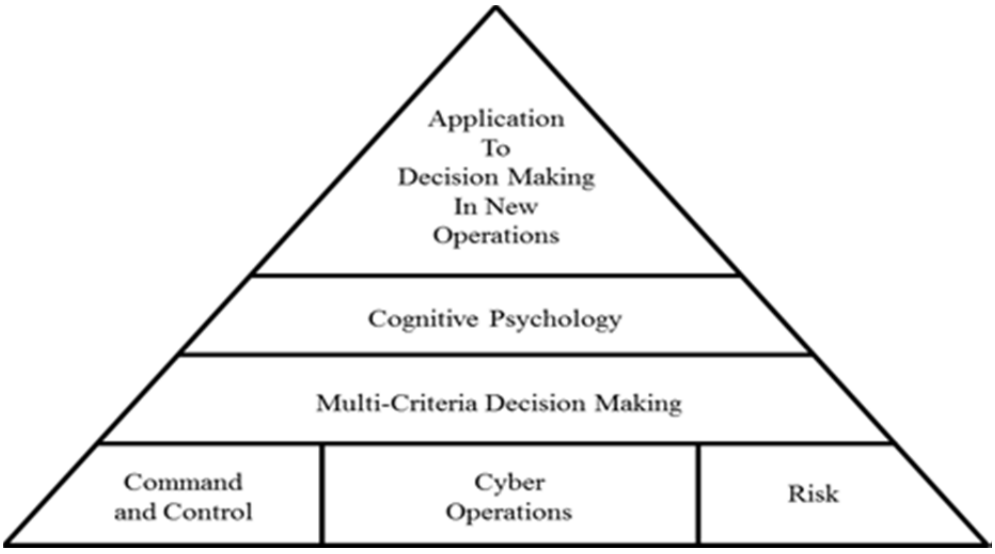


Figure ES-1. Multi-disciplinary Research Approach

This dissertation argues that military organizations below the national level of operations lack the requisite experience, education, and expertise to adequately assess risks, including examining and recommending courses of action for decision making. This argument becomes stronger the closer the organization is to the tactical level.

Decision makers, particularly inexperienced ones, rely upon flawed methods for arriving at a decision. Group dynamics favor a strong personality even if the person is incorrect. Heuristics are mental "rules of thumb" used to fill in missing information or to make a comparison to a known quantity for simple analysis. "Bias" is the way a person interprets information based on experience, education, prejudices, and personal opinions. "Affect" refers to the emotional state of a person as this has been shown to effect decision making. The efficacy of these cognitive processes decrease in reliability as environmental complexity rises. Commanders and staffs lacking the education, experience, and expertise in cyberspace operations will quickly fall prey to the complexity of these operations when making decisions.

This proof-of-concept framework uses expert knowledge and simulation to overcome the limits placed on decision makers by psychological impediments that arise from inappropriate heuristics, bias, group dynamics, and the overconfidence by the decision maker or overestimation of the risks due to a lack of knowledge or experience. The framework uses an objectives hierarchy, developed with the decision maker, to capture and quantify the effectiveness (value) the decision maker associates with each course of action. The framework also constructs a cost model to quantify the resources required for implementation by each decision alternative. This particular iteration of the proof-of-concept uses a non-monetized cost model; however, a monetized cost model is possible. Subject matter experts (SME) define and appraise levels of cost and effectiveness for each decision alternative. These evaluations consider both the SMEs' estimates and the uncertainty the SMEs recognize in their estimates. In the simulation, this information is combined to become the variable cost-effectiveness for each decision alternative. The results of the simulations are presented graphically in a manner that makes clear the relative risks of each decision alternative. This allows the decision maker to evaluate the relative risks of each in terms of its likelihood to be less effective than what is minimally required, and/or more costly than what is maximally acceptable. This graphical output eliminates the ambiguity and uncertainty involved with the current methods of risk analysis—namely high/moderate/low risk, which have no common defining metrics.

B. OBJECTIVE HIERARCHY CONSTRUCTION

Decision makers, in general, have more than one concern in making a decision. They want to choose an alternative COA that produces the best possible outcome for each concern. Additionally, the decision maker also has preferences for the resource costs of an alternative. However, these issues of concern are not always straightforward and require considerable thought. The result is an objectives hierarchy that defines the issues of concern in terms of a set of objectives. These objectives take the infinitive form of a verb such as "to maximize" or "to minimize." Examples from cyber operations might be "to maximize intelligence gathered" or "to minimize the probability of detection."

This research aims to create a simulation framework that will incorporate SMEs' expertise along with the commander's goals, objectives, and constraints regarding the minimum effectiveness and the maximum cost for a course of action. Effectiveness is defined by the following five objectives:

1. To Maximize Damage
2. To Maximize Intelligence Gained
3. To Minimize Detection
4. To Minimize Attribution Given Detection
5. To Minimize Compromise Given Detection

Minimizing Costs is defined by the following four objectives:

1. To Minimize Personnel Costs
2. To Minimize Equipment Costs
3. To Minimize Infrastructure Costs
4. To Minimize Time Costs

For the purposes of this research, non-monetized costs are used, specifically time to create or modify a capability for use. Additionally, only the first level of the objective

hierarchy (Damage, Intelligence, Detection, Attribution, and Compromise) was used in this research due to time constraints. However, future researchers could incorporate and model the lower hierarchical levels. See Figure ES-2.

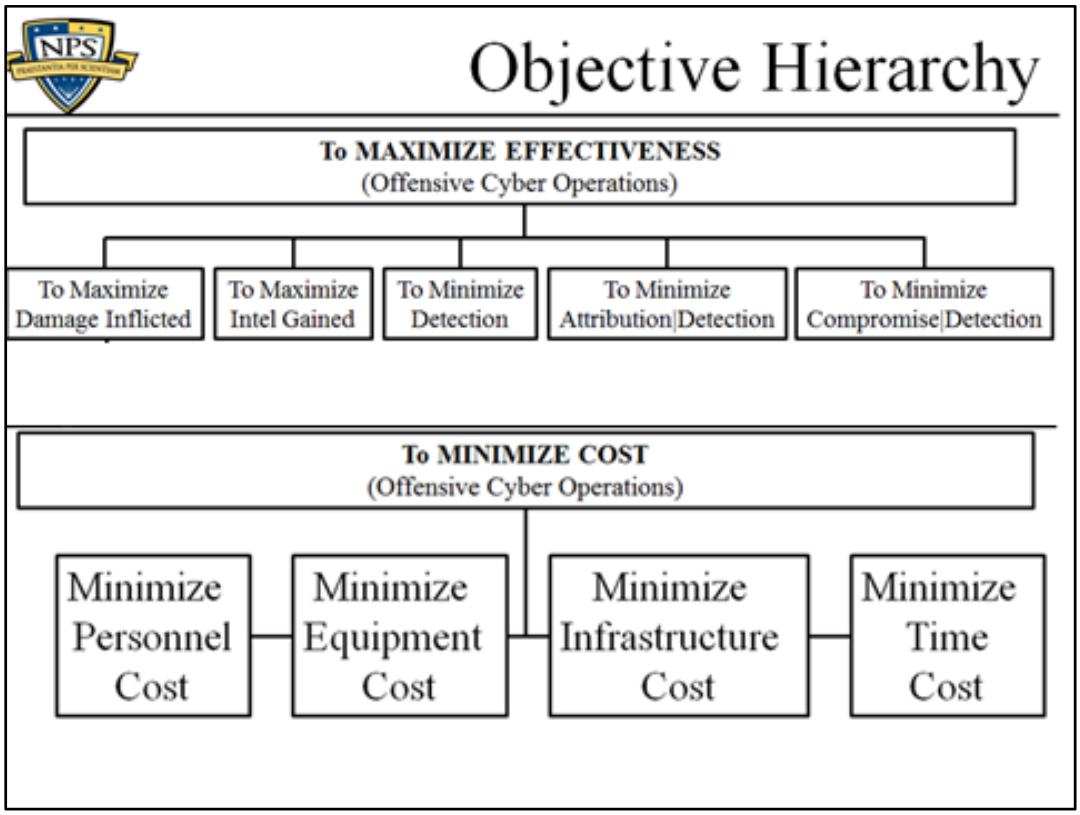


Figure ES-2. Top Levels of Effectiveness and Cost Hierarchies

C. MODELING DECISION MAKER CONCERNS

The decision maker expresses preferences regarding the set of outcomes of a given alternative. For example, this individual may wish to maximize certain outcomes, to the extent possible, through the choice of COA. At the same time, this decision maker may desire to minimize the remaining set of outcomes. The commander's preferences are elicited through a process of iterative questions. See Figure ES-3 for an example of decision maker value modeling. These preferences are represented by a function often called the "overall value function." See Figure ES-4 for an example of decision maker preferences for an operation.

What should be noted is that although the objectives are "to maximize" and "to minimize," the invoked objectives are not necessarily completely maximized or minimized. The dials in Figure ES-4 demonstrate this. In this scenario, the decision maker places equal weight or value on inflicting damage and avoiding attribution. The graph and their associated weights represent the ratio of value between the objectives in the mind of the decision maker. Maximizing or minimizing an objective is defined in the goals of the decision maker, not the conceivable extreme solutions. The process of the decision maker assigning relative weights to objectives, in a ratio to one another, forces the decision maker to acknowledge and make tradeoffs between the objectives to reflect reality. Furthermore, even if the decision maker assigns all value to one objective, implicit constraints exist within the problem that do not allow unconstrained optimization. Thus, the decision maker is forced to contemplate the most feasible solution set.

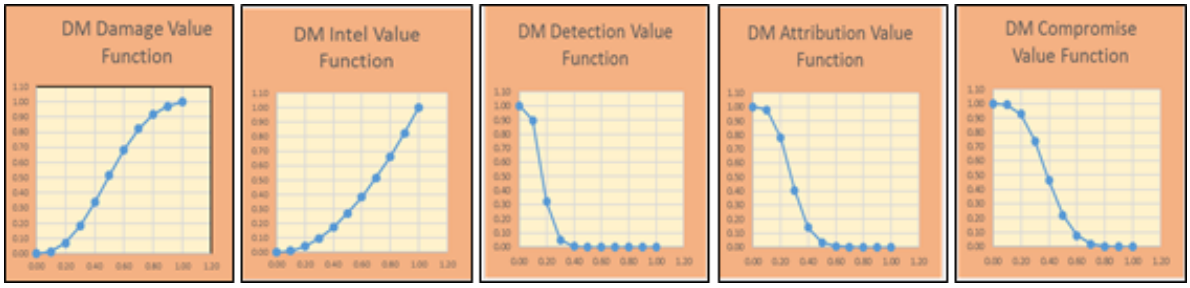


Figure ES-3. Example Graphing Output of Decision Maker Values for Hierarchy Goals

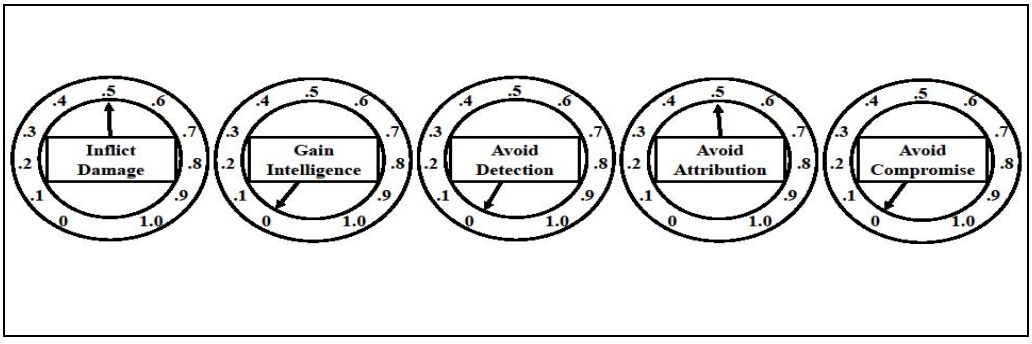


Figure ES-4. Depiction of Dials for Adjusting for Decision Maker Weight for a Given Operation

D. SIMULATION OUTPUTS

Graphical simulation outputs are illustrated in the Sample COA Evaluation portrayed; they are divided into four regions, starting with Region 1 in the upper left corner and then progressing in a clockwise manner. Please refer to Figure ES-5. Region 1 is the desired region. In this area, the evaluated COA meets or exceeds the minimum effectiveness and does not exceed the maximum cost. Moving to the top right is Region 2. In this region, the COA meets the minimum effectiveness but it has broken the cost constraint. Continuing clockwise is Region 3. In this area, the minimum effectiveness has not been met and the maximum cost has been breached. This area is the worst for a course of action. Finally, is Region 4. In this area, the minimum effectiveness has not been met but the maximum cost has not been exceeded. The sample in Figure ES-5 is a simulation of a single course of action with 100,000 simulation iterations. Participants in the research were given graphics with 3,000 iterations to facilitate their seeing individual simulation iterations more easily. This lower number also allowed participants to better judge the density of iteration outcomes. As demonstrated, Region 2 had the highest probability of occurrence and therefore, to meet the required minimum effectiveness, the decision maker would have to increase the maximum cost available for this COA.

As in all military organizations, the commander is the final decision authority. However, this simulation framework is intended to augment and assist organizational staff in evaluating COAs and recommending for decisions. This framework aims to bring greater understanding of the operational risks involved with cyber operations to organizations with nascent process maturity.

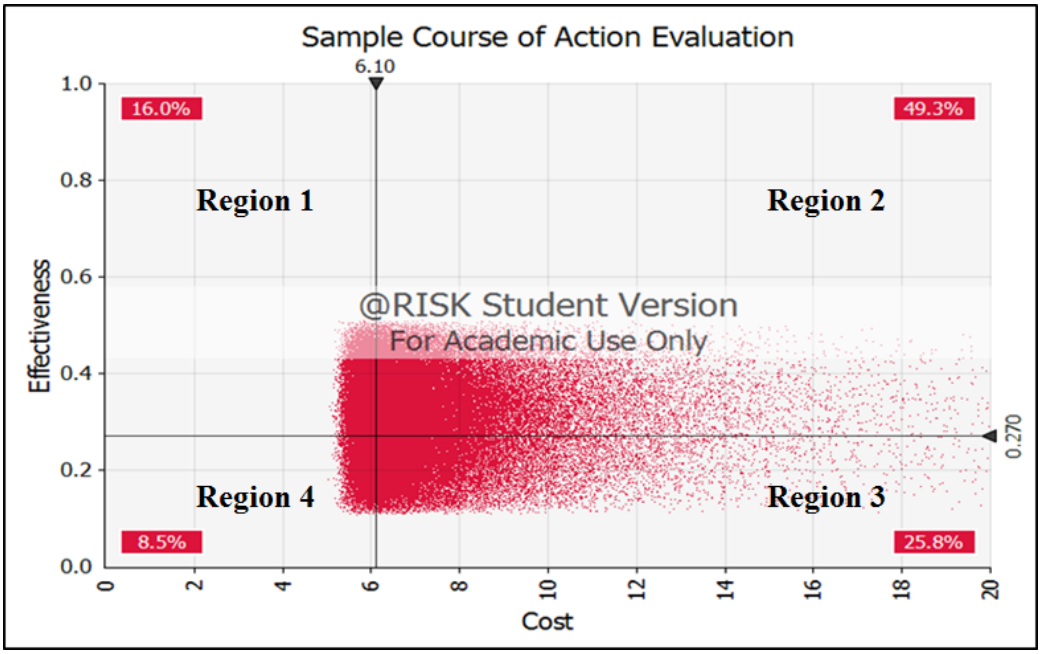


Figure ES-5. Sample COA Evaluation

E. CONCLUSION

Current operational risk assessment doctrine is insufficient for a staff to comprehend an operation's probability of success. Joint Publication 3–0 describes the role of the commander in operational art: "The commander is the central figure in operational art, not only due to education and experience, but also because the commander's judgment and decisions are required to guide the staff throughout joint operation planning and execution" (Department of Defense, 2011, p. II-4). However, if a commander and the staff lack the experience, education, and expertise for these decisions, grievous errors with potentially strategic ramifications will soon follow. Military organizations below the national level need a more comprehensive manner for assessing risks in offensive cyber operations.

Reference

Department of Defense. (2011). *Joint operations* (JP 3–0). Washington, DC: Author.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, I would like to acknowledge and thank my wonderful wife and son for being willing to accept the late nights, missed vacations, and all the times I went to work when others did not. Without your support and understanding, this would not be possible.

I would next like to thank Dr. Kent Wall. Your enthusiasm, knowledge, and patience are what fueled my success. Words cannot express how much I appreciate your mentoring in this journey. I appreciate what you have taught me, both professionally and personally. None of this would have been possible without your guidance and support. As a professor emeritus, you spent probably too much time at work because of me.

I would also like to thank the members of my committee. Dr. Doug Borer, thank you for suggesting the topic over a white boarding exercise. Dr. Alex Bordetsky, thank you for your interest and enthusiasm in this research. Dr. Doug MacKinnon, thank you for your encouragement, the habits you instilled in me, and also for giving the mathematics a second look. Dr. Ray Buettner, thank you for seeing the value of this research. You allowed me to gather all the data from the real targets of this research instead of using proxy participants. Your understanding made this research more valuable and powerful. Dr. Dan Boger, thank you for mentoring me for the last three years. You truly drew the short straw that day. Thank you for the impromptu meetings, the ability to don the department chair hat one minute and the mentor hat the next. Your guidance and support has been invaluable.

To the subject matter experts and participants who participated in this research—the value of your willingness to participate when leading hectic work and personal lives cannot be overstated. Thank you. This research was for you, in the end, but would not have been possible without you. Again, thank you.

Last, but not least, I would like to sincerely thank COL(ret) Greg Conti, Ph.D. and LTC David Chang, Ph.D. Without you two, I would not have had this opportunity.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. CURRENT SITUATION

As the military considers decentralizing offensive cyber capabilities below the national level, the organizations that receive and employ this capability are insufficient for making accurate assessments on the risks involved in these operations. These organizations lack the experience and proficiency within their staffs and command teams. Proficiency in the art of command stems from years of schooling, self-development, and experience via both training and operations (Department of the Army, 2012). Experienced cyber professionals currently reside at small, centralized locations where they work toward national level objectives. The numbers of these subject matter experts (SME) are too small currently to spread to the different Combatant Commands (CCMD) and accomplish national level missions. A CCMD is an organization assigned a region of the world or a specific function for military operations. If decentralization occurs, inexperienced cyber decision makers would likely fall victim to cognitive pitfalls for assessing risk.

B. MULTIDISCIPLINARY RESEARCH

This research combines multiple fields as seen in Figure 1. Command and Control, Cyber Operations, and Risk are the foundation. Command and Control requires new processes of risk assessment for conducting cyber operations. Cyber operations is a new warfighting domain containing unique characteristics that exist in no other domain. Risk increases when new operations are conducted by inexperienced organizations, especially when using existing command and control processes.

Multi-criteria decision-making unites these three fields with quantitative formulations to arrive at adequate risk assessments using solicited subject matter expertise. Moving up the pyramid, cognitive psychology is added to better understand decision making. The culmination of this research is a decision support framework that aids understanding of risk for decision makers in new or novel operations. In these

operations, the decision makers lack sufficient education, experience, and expertise to assess the risks.

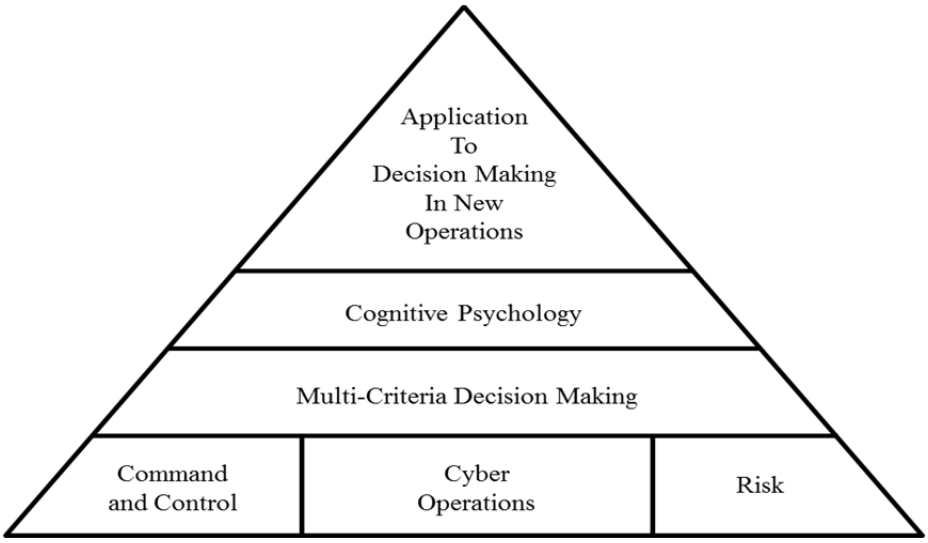


Figure 1. Combined and Layered Aspects of this Research

C. HYPOTHESIS, RESEARCH QUESTION, AND POTENTIAL CONTRIBUTIONS

This research effort attempts to answer the following question: How effective is a simulation framework incorporating both subject matter expertise and assessments of uncertainty at countering the inexperience of decision makers in risk assessments and subsequent decisions within new operations? This dissertation hypothesizes that a framework built on SME knowledge that incorporates the uncertainty that a SME acknowledges will allow decision makers to make more informed assessments and consequently, better decisions. Better decisions in this context is defined as inexperienced personnel arriving at the equivalent decisions as experienced personnel. This effort investigates whether the SMEs' knowledge and their acknowledgement of a lack of knowledge can negate the effects of inexperience, heuristics, and bias in decision maker preferences. This dissertation proposes creating a framework that uses multi-objective optimization to account for the multiple factors considered when assessing risk for

offensive cyber operations and thus expands multiple objective optimization theory (Keeney & Raiffa, 1976).

Until this effort, multi-criteria decision making has not been undertaken for applications in cyber operations. This research potentially adds five contributions to the existing body of knowledge:

- It incorporates SME mental models of risk and their uncertainty. Previous research did not account for the SME's mental models for arriving at an assessment of risk.
- It goes beyond the SME knowledge base to account for uncertainty in the SME's assessment of a scenario.
- It eliminates the shortcomings of the Risk Matrix approach, which is only a qualitative approximation of uncertainty.
- It uses the sigmoid function to model whether higher or lower is "better" in regards to the preferences of the decision maker, depending on if the decision maker wishes to maximize or minimize an objective. Previous research has focused on the use of linear, exponential, logarithmic, and power functions.
- This work is the first use of multi-criteria decision making in cyber operations.

The proposed framework would assess risks based on terms of "Cost" and "Effectiveness." These variables account for the decision maker's restraints when evaluating proposed courses of action or alternatives and are comprised of an aggregation of variables. Cost decomposes into the price of personnel, equipment, and time, to name a few. Effectiveness considers matters such as risks to other operations, loss of access to the adversary network if discovered, and the ramifications of retaliation if discovered.

Chapter II will discuss command and control in military operations and in particular, the difficulties of command and control in cyber operations if decentralized. Chapter III presents the different types of cyber operations; the two types of offensive operations are discussed in depth along with the risks involved with these operations. Chapter IV continues the literature review by discussing the cognitive aspects of decision making and focuses on how heuristics, biases, group dynamics, the decision maker's mood, and estimates of risk assessment using qualitative measures—combined with a

lack of experience—all contribute to making ineffective decisions. Chapter V discusses decision making under conditions of certainty. Chapter VI expands this discussion with decision making under conditions of uncertainty. Chapter VII discusses the methods used for the experiment undertaken for this research. Chapter VIII analyzes the results of the experiment for this research. Chapter IX discusses the results, generalizability, limitations, and future work for this research effort.

II. COMMAND AND CONTROL: C2 RISKS

Cyber operations require command and control activities, just as a tank assault or an aircraft raid would. According to Van Creveld (1985), command and control involves three elements: organization, procedures, and technology. Organization pertains to how the organization is structured for its mission, including the number and type of personnel in given positions and the equipment and resources allocated for mission accomplishment. Procedures encompass the routines that allow an organization to accomplish its mission in an efficient manner. In military units, procedures manifest as rules; regulations; field manuals; Tactics, Techniques, and Procedures (TTPs); and Standard Operating Procedures (SOPs). Technology in this case is not limited to information technology systems. It also incorporates all systems that allow the decision maker to send, receive, and analyze information for later decisions. Technology may also be comprised of both people and machines working together as a system, such as a drone operator piloting an unmanned aircraft. The drone may be outfitted with weapons or sensors for gathering intelligence. However, both the drone and the operator must work as one system.

A. INTERDEPENDENCE OF COMMAND AND CONTROL ELEMENTS

Interdependence exists between these three elements of organization, procedures, and technology. A change or growth in one, causing an imbalance between the three, often will facilitate a change or growth in the other two elements until a new stasis is attained. In his book *Command in War*, van Creveld (1985) uses the helicopter as an example, discussing how technology advanced past the capacity of the organization and its procedures. With the introduction of the helicopter into military operations, personnel were able to move deeply into and more quickly around the battlefield. Subsequently, reporting procedures needed to evolve so that situational awareness of personnel locations could be maintained in such a fluid environment. Additionally, the technology that supports reporting needed to be upgraded to account for the increased distances forward combat units were from their headquarters. A comprehensive understanding of

the operating environment is based on an understanding of the current situation viewed through these lenses. Knowledge gleaned from this analysis of the operating environment assists decision makers in evaluating courses of action.

In the helicopter example, commanders achieved a new balance between the three elements by implementing new radios. In this example, the advancement of technology initially led to reporting procedures providing out of date information. Additionally, radio communications equipment were reevaluated in order to provide longer ranges, last longer on battery power, and be lighter to carry. The balance that subsequently was achieved between the three elements allowed commanders to better understand the positions of their personnel across a rapidly changing battlefield.

B. RISK CONCERNS OF COMMAND AND CONTROL

Risk fits into each of these lenses of organization, procedures, and technology and must be considered not only in traditional operations, but in cyber operations as well. Risk from an organizational perspective manifests in the structure of the organization. If an organization lacks sufficient personnel or if these personnel lack domain-specific knowledge or skill sets, the organization is at risk for not meeting its objectives. Risk from a procedural perspective means that the organization does not have sufficient doctrinal or administrative information to successfully undertake a mission. This means that personnel may lack the appropriate authority or materiel to accomplish missions. Risk from a technology perspective means that information is coming in too quickly to analyze or that the information required to continue planning or conducting operations is insufficient. In both the helicopter example, once the information becomes available it is out of date.

The command and control systems for cyber operations must grow more robust to mitigate some of the risks inherent in a new environment. These operations do not move across a traditional map in a near-linear fashion as do tanks, aircraft, and naval vessels. Additionally, information coming back into headquarters for analysis and subsequent decisions relies solely on what machines send and therefore needs interpretation. This process is counter to that of traditional operations in which a human analyzes an

adversary's order of battle. The human can recognize the traditional formations, evolving strategies, and their place within the larger adversarial operation. Since cyber operations cannot be observed in a traditional sense, with other participants on the battlefield witnessing the events unfold from multiple perspectives and vantage points, the risks increase.

Current military doctrine describes the requirements for commanders and their representative staffs to be proficient in the art of command. However, this proficiency stems from years of schooling, self-development, and operational and training experiences (Department of Defense, 2011b; Department of the Army, 2012). This education and experience in cyber operations is what commanders and staffs below the national level lack. Therefore, the ability to make accurate assessments of risk for decision-making is absent, thus raising the risks in these operations. Recent studies have identified the decentralization of command and control in cyber operations as both ill-defined and problematic (FitzGerald & Wright, 2014; Leed, 2013). In traditional military operations, commanders operate within a relatively close distance to soldiers executing the operation. This proximity allows the commanders to better develop situational awareness of the unfolding operation, to oversee progress toward objectives, and to direct the changes in maneuver that may be needed to account for unforeseen events. FitzGerald (2014) and Leed (2013) both identified a lack of coherent command and control mechanisms between combatant command organizations, responsible for the operations, and the actual computer network operators, located at Ft Meade, MD. In a decentralized cyber operations scenario, the CCMD commander feasibly could be located half a world away from the operators executing the mission. This geographic and temporal separation adds to the delay of information to and from the commander. FitzGerald (2014) and Leed (2013) concluded that organizations below the national level are ill-prepared to understand the risks and ramifications of operating in the Cyber domain. The procedures used to assess risks in operations are discussed next and cyber operations and their unique risks are discussed in the following chapter.

C. RISK ASSESSMENT

The systems for risk analysis such as ones used in the Department of Defense require extensive experience and knowledge of the risks and consequences involved. In fact, the Department of Defense (2011c, pp. II–4, c) explains this requirement in the Joint Operations manual: "Commanders draw on operational art to mitigate the challenges of complexity and uncertainty, leveraging their knowledge, experience, judgment, and intuition to generate a clearer understanding of the conditions needed to focus effort and achieve success." Commanders and their staffs are incapable of assessing the risks involved in offensive cyber operations based on this statement. Cyber operations exhibit the potential to be considered mixed gambles, where both gains and losses may occur simultaneously. This is in contrast with single-domain gambles where only gains or losses may occur (de Langhe & Puntoni, 2015).

No existing doctrine for commanding and controlling military operations, much less cyber operations, include the application of multi-criteria decision making for weighing and trading off between risks and rewards. The Department of Defense uses fourteen different systems to analyze and assess risk (Army War College, personal communication, February 2016). Of these, six are immediately disqualified for use in cyber operations. These methodologies pertain to food inspection and preparation, chemical storage and disposal, and workplace safety and accident reporting. The proponent agencies for these are: the Food and Drug Administration, the Environmental Protection Agency, and the Occupational Safety and Health Administration. Although these agencies have to assess risks that may in fact bring harm to people, these risk assessment methodologies have no component for incorporating risks to operations as needed by the military.

Of the remaining eight methodologies, one is a Department of Defense directive that augments an OSHA risk assessment from the previous paragraph. The Army has two methodologies, one for operations and one for health assessments. The latter is non-applicable to cyber operations. The Navy offers two methodologies also, one for operations, the other pertains to HAZMAT storage and disposal. For obvious reasons, this HAZMAT methodology is not applicable to cyber operations. The Air Force offers

one risk assessment methodology for operations that has the potential for applicability to cyber operations. Joint doctrine offers a single risk assessment methodology for operations that has the potential for use in cyber operations. Lastly, the National Institute of Standards and Technology offers a risk assessment methodology that is used widely in the DOD and in the commercial sector. This methodology for assessing risk pertains to information assurance in information technology networks. Unfortunately, for the purposes of this research, this methodology is inadequate as it focuses on the information and technology from a defensive perspective. This leaves us with potentially four potential systems for assessing risk from the Army, Navy, Air Force, and Joint doctrine.

D. PROBLEMS WITH QUALITATIVE RISK ASSESSMENT MODELS

These risk analysis methodologies are qualitative and ambiguous at best. These systems uses terms such as "high," "moderate," or "low" risks to describe the severity of the risk (Broder & Tucker, 2012; Department of the Army, 2013). These terms have no clearly defined meaning or context. Often, the definitions of these terms includes qualitative descriptions such as "unlikely to occur," "severe impact," and "highly likely" that offer no discrete boundaries to divide and define the areas.

The National Security Council has approved a color-coded schema for assessing the severity of cyber incidents later implemented in the National Cyber Incident Response Plan (Department of Homeland Security, 2016; U.S. Government, 2015). This system uses terms such as "unlikely to impact" for the lowest severity and "poses an imminent threat" for the most severe consequence. Qualitative systems for risk assessment, such as this schema and also used by the Department of Defense, are inherently flawed: the qualitative nature of these scales suffers from a lack of standardization and meaning, range compression, and the presumption of regular intervals between scale increments.

Qualitative scales lack standardization and meaning. This is incongruent with the relied upon expertise for counsel that resides with the experts. Two people with different experience levels and backgrounds would surely have different interpretations for what is "severe" or "high impact" (Bennett, 2000). This is because non- numeric descriptions

lead to different interpretations of data. In the previously discussed study by Budescu, Broomell, and Por (2009) participants applied their own subjective meaning to the nominal scales, even though a quantified definition existed. However, these subjective meanings were based on the heuristics of each person. Another example of these heuristics at play is the decision maker mentally assigning values, numbers, or probabilities when none exist (Ellsberg, 1961). These heuristics take into account the bias, past experiences, and cognitive understanding of each person. Heuristics are discussed in-depth later in Chapter 4. Therefore, it is certainly impossible for a group of disparate people from different backgrounds and experiences to arrive at the same definition of what constitutes for each level of risk.

Two other flaws of these systems are range compression and the presumption of regular intervals. If numbers are assigned to risk assessments using as an example, a 1–5 or a 1–10 scale, a small incremental movement can have a large impact on the alternatives or consequences. As the scale range decreases, the magnitude of impact conversely increases, that is, if the numbers and the corresponding meanings have regular intervals. With the presumption of regular intervals between levels, a 1–2-3-4-5 scale implies that a 4 is twice as good/ bad as a 2; this is not necessarily true (Hubbard, 2009; Savage, 2012). Since different backgrounds and experiences create different heuristics used to assess the severity of a situation, the current risk assessment systems are inadequate. These inadequate risk assessment systems coupled with the cognitive pitfalls discussed previously create potential failure when used in new operations where the decision maker and support staff lack the experience and education in understanding the risks and consequences involved.

E. PROMISES OF QUANTITATIVE ASSESSMENT METHODS

Quantitative methods for assessing risks and rewards offer benefits over the current qualitative practices. First, quantitative methods are less subjective. In using mathematical models for analyzing risk, the data can be interpreted in limited ways. When the question of “How risky is this?” is posed, the answer is not based on the

respondent's experiences, biases, or mental models that are used where experience is lacking.

Next, quantitative methods reduce the inconsistencies of multiple differing opinions given to the decision maker. In this scenario, differing opinions of the risks confront the decision maker. With quantitative methods, a verifiable and repeatable process can be used to overcome differing opinions or personnel being absent (Keeney & Greogory, 2005; Keeney, 1992, 1996; Keeney & Raiffa, 1976). No one opinion is used at the sake of all others. Lastly, by using multiple experts, a greater understanding of the "truth" can be ascertained and considered for decision. Quantitative methods also allow for multiple viewpoints and opinions to be modeled together, allowing for the breadth of experience to be brought to bear on the situation at hand.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CYBER OPERATIONS AND RISKS

Cyber operations consist of operations to achieve objectives in the global information environment. The DOD defines this environment as consisting of "interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (Department of Defense, 2011a, 2013). This definition accounts for individual desktop and laptop computers, webservers, and the infrastructure that makes the Internet and world wide web come alive and that provides millions of users with information and entertainment every day.

What most people, including researchers, do not consider though is that this definition touches many more aspects of life. The smartphone in a pocket is more a computer with telephonic capabilities than it is a phone with computational power. Home devices such as thermostats, vacuums, and televisions are connecting to the Internet as part of the Internet of Things. As more and more devices connect to the Internet and woven into the fabric of our lives, the vulnerability posed increases. Our nation has become more dependent on the Internet as critical infrastructure for daily existence. Financial markets along with banks and credit unions that underwrite the markets rely on the Internet. Public utilities regulate their services and maintenance through the Internet. Even the phone calls made from traditional land lines within homes and businesses rely on the Internet.

Cyber operations are conducted across the range of military operations at "condensed time ranges and with great precision and lethality" (Schneider, 2016). Although these operations alone can achieve some military objectives they are often integrated into the planning and coordination of traditional kinetic operations. Commanders use cyber operations to retain freedom of maneuver in cyberspace, accomplish command objectives, deny freedom of maneuver to the adversary in cyberspace, and enable other operational activities (Department of Defense, 2013, p. I.3.a). Often these operations obtain and develop intelligence regarding a nation-state, an organization, or a specific individual for potentially kinetic or non-kinetic targeting.

Three categories of cyber operations exist: defensive cyber operations (DCO), offensive cyber operations (OCO), and DOD Information network operations (DODIN Ops) (Department of Defense, 2013; Department of the Navy, 2014).

DCO are proactive measures to protect and defend the DOD or other friendly cyberspace (Department of Defense, 2013). These operations occur only within DOD networks unless coordinated through both the DHS and the DOD. DODIN Ops are the operations to build and maintain the network infrastructure for the DOD and occur exclusively within the DOD. This body of research does not include DCO or DODIN operations.

Only two types of offensive operations are considered in this research effort; they are OCO, formally known as a computer network attack (CNA), and intelligence, surveillance, and reconnaissance (ISR); surveillance and reconnaissance (SR); and computer network exploitation (CNE). The last three describe the same actions being conducted under different organizations and will be discussed later in depth. Although ISR/ SR/ CNE are considered intelligence operations as opposed to offensive operations, for the purposes of this research, ISR/ SR/ CNE will be defined as offensive. The rationale for this is the adversary perspective. The three aforementioned operations all appear the same as the beginning phases of an attack being conducted in an adversary network. The attacker has broken into the victim's network, conducted a reconnaissance, and potentially removed any information of value. However, with a computer network attack, the activity continues along the continuum for damage to occur. From an adversary perspective, these intelligence operations may appear to be the early stages of an upcoming attack.

A. A GROWING THREAT

As part of the 2011 Strategy for Operating in Cyberspace, the DOD required that all division and corps-level organizations begin incorporating cyber operations into their large-scale exercises (Department of Defense, 2011a). Each year, this requirement has been reaffirmed and its importance continues to grow. In 2008, cyber ranked 12th and 13th in the Director of National Intelligence's assessment of the threats to the United States

(ODNI, 2008). In 2013, Cyber ranked as the highest priority in the threat assessment, displacing terrorism for the first time since 2001 (Bremmer, 2015). Also, in 2013, GEN Alexander, then Commander of U.S. Cyber Command and the National Security Agency, testified before Congress that the need for offensive and defensive cyber teams was paramount to the nation's security (McGregor, 2013).

Additionally, in 2015, the National Defense University for China's 3 Peoples' Liberation Army (3 PLA) released updated doctrine concerning the "Network Military Struggle." In this document, the position of the 3PLA became: "victory in war first starts from victory in cyberspace; whoever seizes the initiative in cyberspace will win the initiative in war." This document clearly identifies that dominance within cyberspace is requisite for Chinese national interests in conflict. This document also illuminates the Chinese stance on using a first-strike capability against its adversaries with characterizations of "gain the initiative through striking first and seize the decisive opportunity" " (Kania, 2015).

B. TYPES OF CYBER OPERATIONS

As the multiple Geographic Combatant Commands (CCMD) begin to include cyber operations into their portfolios, two types of operations will become available to the commands. The first is offensive cyber operations; the other is ISR/ SR/ CNE. Offensive cyber operations are analogous to the deployment of tanks and aircraft. They project power to meet a desired end state. Computer network exploitation is subtler. It is the collection of intelligence to meet the requirements of the command. These exploitation operations supplement other intelligence operations such as Human Intelligence, Imagery Intelligence, Geospatial Intelligence, Open-Source Intelligence, and Measurement and Signature Intelligence. Both OCO and CNE will be discussed further in this section.

1. Offensive Cyber Operations

Offensive cyber operations, formerly known as computer network attack operations, are designed to project power through cyberspace. These operations focus on

either the information resident in the device or the physical device itself. There are four effects that may be achieved in OCO: disrupt, destroy, degrade, and manipulate (Department of Defense, 2013, pp. II–5).

Disruption operations temporarily prevent an adversary from accessing information or a resource for a specified period of time (Department of Defense, 2013, pp. II–5). Disruption operations vary between 0% and 100% of a capability. The greater the percentage of the disruption, the more profound the effect. As an example, a 50% disruption may manifest as the ethernet card intermittently working for a set period. This would outright diminish the user's ability to access information or frustrate the user due to the computer lag.

The next effect is destruction. Destruction permanently and completely denies access to information or a resource (Department of Defense, 2013, p. II–5). A destruction effect may manifest as overwriting files, encrypting of data, and deleting the key to decipher. Destruction operations were observed in the 2012 attack on Saudi Aramco. Saudi Aramco is a petroleum and natural gas company based in Saudi Arabia. This company is thought to possess the largest stockpile of crude oil in the world (Financial Times, 2010; Saudi Aramco Oil Company, 2015). In this example, attackers entered the business network and unleashed a virus that deleted data on 30,000 workstations (Reuters, 2012; Sheppard, Crannel, & Moulton, 2013).

Another manifestation of the destroy effect is physical destruction. Two publicly known cyber attacks have caused physical destruction. The first was the Stuxnet attack of 2011 (Falliere, O Murchu, & Chien, 2011). This attack increased and decreased the speed of centrifuges spinning at an Iranian nuclear material enrichment laboratory. This attack manipulated the centrifuges outside of safe operating parameters. Although not confirmed, it is estimated that between 900 to 1000 centrifuges required replacement (Warrick, 2011). The second instance of physical damage occurred in Germany in 2014 (Zetter, 2015). This attack manipulated and disrupted control systems at an unnamed German steel mill. Zetter states that the damage to the control systems resulted in the plant operators being unable to shut down a blast furnace in the prescribed manner, resulting in "massive damage."

The third effect for OCO is degradation. Degradation effects are based on a percentage of degradation of the computer's processing capability (Department of Defense, 2013, pp. II–5). Closely resembling disruption, degradation focuses on the percentage of capacity or access diminished, rather than the time duration. Degrade effects may manifest as slowing the hard drive to a fraction of its normal speed. This effect would slow the user's access to information residing on the internal hard drive, slow access to programs, and potentially prevent access to network resources due to surpassing the allocated time to authenticate.

Manipulation effects are the only effects that solely focus on the information residing on the target machine. Manipulation effects may manifest as changing the information, issuing false orders from a leader's account, preventing orders from being issued, or changing the routing table within a router so that information cannot make it to the intended destination. Both OCO and CNE have inherent risks that can impact the organization conducting the operations, as well as partner agencies and foreign states. These will be discussed in Sections C, D, and E.

2. Intelligence Gathering Operations

Intelligence, Surveillance, and Reconnaissance, Surveillance and Reconnaissance or Computer Network Exploitation operations are a subset of OCO with the purpose of intelligence gathering (Department of Defense, 2013). ISR and SR operations are intelligence operations conducted by conventional forces. Although ISR has long been the standard name for these activities, the new doctrine is now moving to SR to avoid overstepping legal authorities due to the use of the word "Intelligence." This issue stems from legal arguments on who may conduct intelligence operations. CNE operations are the same, however due to the complexities of legal authorities, these operations are conducted by organizations tasked to conduct Signals Intelligence (SIGINT) on behalf of the nation. One such example of this is the National Security Agency.

These intelligence operations primarily target the physical aspect of a computer network such as hardware and physical mediums connecting the hardware. These mediums are discussed in a later section. The purpose of ISR/ SR/ CNE operations is to

gather intelligence in a manner that is unnoticed by the adversary until such covert action is no longer feasible. A target is no longer feasible when the operation is discovered, the machine is replaced, or the person who is the actual target moves to another machine. ISR/ SR/ CNE may support other future operations such as OCO or DCO.

OCO is supported by confirming that the operating system, other software, and conditions are correct before launching an attack. DCO is supported by observing an adversary infiltrate a friendly network in real-time, confirming the existence of evidence for a past attack by an adversary. Additionally, ISR/ SR/ CNE may discover new versions of an adversary's malware capabilities so that mitigation strategies may be developed and employed prior to these capabilities' use (Department of Defense, 2013, pp. II–5). As previously stated, ISR/ SR/ CNE are defined in this research as an offensive operation as the computer network must be penetrated without permission or knowledge and that these intelligence operations appear the same as the early stages of an attack within the adversary's network, with the only difference being the intent.

C. RISKS IN CYBER OPERATIONS

Cyber operations have inherent risks, even for experienced organizations. In 2008, intelligence analysts believed that an Al-Qaeda website was partly responsible for the rising escalation of violence in Iraq and subsequent U.S. casualties. The DOD ordered the Joint Task Force—Global Network Operations, the military arm legally capable of attacking networks on behalf of the U.S. government, to attack the site. This operation commenced with little confirmation of the intelligence. This was due to the rapid planning cycle brought about by the escalation of violence in Iraq. When the operation commenced, it was successful in its intent—more so than had been expected. The website in question was, in fact, a joint CIA and Saudi Intelligence Service website used to lure and monitor terrorist activities and movements. The operation destroyed data on webservers in Saudi Arabia, Germany, and Texas. This fratricide could have been prevented by a deliberate reconnaissance effort on the part of the Joint Task Force—Global Network Operations. This reconnaissance would have caused the CIA to question the operation at a minimum (Jarmon, 2014).

D. CAPABILITY DEVELOPMENT RISKS

All the intelligence gathering capabilities are for naught if the operations are unable to be conducted or if the operations jeopardize other operations. I have identified two main risks in cyber operations, which consist of sub-elements. Capability Development Risks include the risk of losing access to an adversary network and the risk of capability loss. Operational Risks include the risk to operations, the risk of compromise, and the risk of retaliation. This analysis assumes that the organization conducting these operations have all the requisite legal authorities. In the event of not having the appropriate authorities, this research assumes that operational planning would cease and the operation would not commence.

1. Risk of Loss of Adversary Network Access

Multiple points require consideration when discussing the potential loss of access to an adversary's computer network. Where is the target physically located? A target such as North Korea receives its Internet connections and access from China, another potential adversary of the United States. Conversely, is a non-state adversary's machine located within an ally of the United States? In this case, operational leaders would need to coordinate with the allied nation and gain permission to conduct operations on the adversarial computer. It is more probable that the allied nation would perform the operation in lieu of the United States.

Beyond physical location, the next consideration is the target's location within the network. Not every node has the same access and privileges within the network. Domain controllers authenticate users and privileged access to resources within the network. Routers that move information between networks can be used to discover the adjacent networks that converge at the target router. Switches store device information for all the nodes connected to that switch. Servers store data, resources, and potentially the profiles of users. The purpose of the operation determines the device that is targeted.

When an organization prepares to conduct an operation on an adversary network, it must determine what, if any, other friendly actors are already conducting operations within that network. The organization with primacy has the responsibility to deconflict

multiple actors occupying the same network or machine. Primacy is the condition that whoever was the first to conduct and sustain operations within the network or machine has the authority to regulate other activities. The organization that occupies first has to grant permission for any other organization wishing to conduct operations within that network. If permission is not granted, the second organization cannot conduct the operation. However, if the permission is granted, both organizations are at risk of being detected. If one organization is detected, the other will likely be detected if immediate actions are not taken to remove capabilities and traces of actions. Therefore, the more actors operating within a network, the greater the risks involved for detection by the adversary. This risk be discussed more later in the chapter.

Next, the adversary network's infrastructure and architecture must be considered. Research is required if the adversary is using proprietary or uncommon operating systems. Personnel with in-depth understanding of these technologies facilitate the operations so that operating systems do not crash, traces of operations are removed, and the intended effects occur. For example, Siemens is one of the preeminent developers and builders of supervisory control and data acquisition (SCADA) systems along with the operating systems that control them. Before any operations occur in these SCADA systems, the friendly operators must be intimately familiar with the intricacies and dependencies of the system. Additionally, some countries continue to run what is considered to be "outdated" systems. These systems are left in place unless they fail due to the costs of modernization and the dependencies associated with custom software and periphery devices. These outdated systems, which include those designed and retired in the 1970s, are no longer taught in schools, so further research is needed to understand their intricacies.

Once the network architecture and the target device are understood, an access point is needed into the network. In a secure network, the target network may have only a single point that is accessible by friendly actors. In 2011, Iran announced that it would create its own Internet using information the government deemed appropriate from the greater Internet (Rhoads & Fassihi, 2011). Information not deemed appropriate would not be imported into Iran's national Internet. This effort aims to create a censored Internet to

exist in parallel with the global Internet and to gradually shift all of Iran onto the national Internet. Currently, this effort is past the scheduled completion date. The Iranian population will be isolated from the rest of the world if this is accomplished. If the national Internet is finished, both Iran and its adversaries would seek to identify all network vulnerabilities that would allow unauthorized access. The fewer access points that are available, the higher the risk for loss of network access.

Once inside of the adversary network and the target device, operators need appropriate privileges to access and execute processes. This condition is also true if the operator wishes to traverse the network and enter other network segments or devices, which often requires privilege escalation. Privilege escalation occurs when a friendly operator enters the network and uses either stolen credentials or defeats software security mechanisms, to attain privileges of an administrator. This act allows the operator to access to all data, processes, and logs on the device and the ability to move across the network and enter other devices. Risks increase when an adversary has only a few administrators who carefully monitor administrator-level access into devices.

The final risk is the medium used to access the adversary network. Five main types of mediums exist for the purposes of this discussion: close access, wired local area network (LAN), wireless, cellular, and satellite access. Close access is defined as being close enough to physically touch the device. Close access includes the use of media such as compact disks (CD), digital video disks (DVD), universal serial bus (USB), and typing commands. The purpose of this is to manually insert software or hardware on the target device. Close access operations may occur if the device is completely separated from Internet access, which is a high risk operation in and of itself. Close access operations will not be discussed or considered in this research.

Wired LANs are what most people are familiar with in networks. Wired LANs are known as the cable or fiber that connects into the computer on one side and to a switch or other access point on the other. Wired LANs are used for their reliability and simplicity since there are no wireless signals that may be interfered with. Wired LANs allow for remote administration and maintenance so long as the end device itself is turned on. Since wireless signals will have interference or degradation, wired LANs offer higher

speeds and more reliability for data moving from one location to another. For cyber operations, wired LANs allow for the mapping of networks and movement from one location to another with ease as an operator moves from one device to another using a predefined route from the roadmap-like nature of the management devices. Examples of such management devices are a switch, which map all devices that connected to it and a router, which map all networks connected to it.

Contrast this with a wireless network. The radios within each device emanate signals and therefore, data in all directions in a wireless network. When a device creates a connection with another device and passes data, the transaction is visible to every other device monitoring that radio frequency. Additionally, wireless signals are limited by distance, the construction materials in walls, floors, and ceilings, along with other electrical emanations. This means a friendly cyber operator would need to be relatively close to the adversary device to detect the wireless signals and conduct operations. Close access operations are more in line with the example described above. The other possibility is that an adversary device connected to a LAN is also connected to other devices through a wireless connection such as Wi-Fi or Bluetooth. If access to the adversary network is accomplished through the LAN and then a wireless connection is needed for movement to another device, all other devices in the room potentially will see this occur. This use of wireless connections becomes a problem if the network administrator is recording or conducting live analysis of wireless transmissions. Additionally, all devices in the immediate area potentially would require investigation before finding the correct destination, compounding the difficulty of a wireless environment. Increasing the problem of wireless environments is security. Multiple security devices are marketed for little monetary or training costs. These devices passively detect and record wireless signals and can analyze the signals at a later time or in real-time by with other devices, thus raising the risk level.

Cellular networks are often overlooked. The typical smartphone in a person's pocket has more computational power than the computers that were used to launch a man to the moon (Puiu, 2015). Cyber operations should consider smartphones as a computer with a telephonic capability as opposed to the general consensus of a phone with some

computational ability. On the surface, a cell phone offers some of the same problems that a wireless device, as previously discussed, has. The Wi-Fi and Bluetooth transmission are limited in range and visible to everyone. However, cell phones all have an IMEI number. The International Mobile Equipment Identity (IMEI) number is a globally unique 15-digit number assigned to every cellphone. Because telephone networks are computerized to dynamically allow greater optimization of circuits, these phone are accessible from a LAN using the telephone access provider's network. Additionally, technologies exist to masquerade as a cellular base station. These technologies allow for targeting of individual phones or allowing every phone to connect. This creates a connection between the fraudulent base station and the cell phone that may be used to monitor and pass data to the real base station, geo-locate an individual, or to activate other functions on the phone, such as the Bluetooth or Wi-Fi.

Once the phone has been identified and accessed, it then can become a launch point for other effects. Often a phone may connect to a computer through a USB port or a wireless connection to move data. Another option is that the phone automatically connects to the same wireless network that a targeted computer resides on. This connection between the phone and computer or wireless network allows for movement of a friendly cyber operation's capability to a targeted node or to enter the targeted network. Additionally, the phone's internal capabilities, such as the camera or microphone, may be leveraged to provide essential information (Risen, 2015). Cellular networks however come with additional risks. Telecom providers routinely monitor their networks for anomalous activity and quickly investigate. These providers are usually owned by the adversary nation or a third-party nation. Secure or sensitive facilities often will not allow cell phones inside due to the increased security threat. Additionally, each combination of cell phone hardware and operating system has its own dependencies and structure, as is seen in the Android operating system. This limitation will be discussed more in the loss of capability section.

The last connection medium discussed is satellites. Satellites offer their own unique aspects. A satellite may illuminate a large portion of the planet. Low Earth orbit satellites offer smaller footprints of illumination but, these may still be over 3,000 km

(Redding, 1999). On the opposite end of this spectrum is the geosynchronous satellite, requiring only three of these to cover the Earth. Satellites offer unique issues though. Although a radio wave travels at the speed of light through the atmosphere and space, the half-second delay incurred from a signal traveling from an antenna on Earth, to the satellite, and back to another antenna on Earth is enough to cause detrimental effects in cyber operations where milliseconds are the unit of measurement. A delay that is even a half-second long may be enough to miss an opportunity to hijack an adversary's online session. Additionally, as with cellular telecom providers, the adversary or a third party nation often owns the satellites and routinely monitors the traversing traffic.

2. Risk of Capability Loss

Cyber capabilities are the software programs, sometimes also referred to as tools, which are used to break into machines and achieve effects. A simple capability may be a key logger to record every keystroke an adversary makes in the hope of attaining administrator credentials. On the opposite end of the spectrum is a complicated tool such as Stuxnet that was briefly discussed earlier. Stuxnet is considered complicated as it could propagate in two different ways, check to see if it already infected a machine, and vary its effects on the centrifuges to avoid detection (Falliere et al., 2011). What made Stuxnet even more complicated is that it employed four zero-day vulnerabilities (Bieleny, 2012; Rid, 2012; Warrick, 2011). A zero-day is a flaw within the computer code that no one, not even the manufacturer, is aware of. It is known as a zero-day because there are zero days available to mitigate this vulnerability.

When considering a capability for use against an adversarial target, multiple aspects must be considered to choose the right capability and maximize the chances of success. These are the hardware, the software to include the operating system, personal security protection (PSP), signatures, and redundancy. The hardware architecture is the first consideration. A capability designed for a 64-bit processor as a lot of modern computers are will not work on a 32-bit processor. However, the opposite will work. Additionally, Intel processors that are used in many computers today have a different architecture than an Advanced RISC (reduced instruction set computing) Machine

(ARM) architecture that is popular for smartphones and other smaller devices due to low power requirements. Each different architecture requires specific knowledge to attain the same end state.

The next consideration is the software including the operating system on the target device. Software comes in 32 bit or 64 bit versions to accommodate the hardware architecture. These versions also exist for the operating system on the device. What makes targeting the operating system more complicated is the fact that it has multiple combinations possible. For example, Microsoft XP supported 106 written languages natively and additional languages were available for download. What makes this important is that each language change makes a modification to the operating system. A classic example is the difference between the keyboard layout supporting English in the United States versus English written in Britain. Although they are nearly the same spoken language, the keyboard map has changed and thus, the input and outputs of the computer change at a minimum. This is important when attempting to enter a stolen credential for privilege escalation or working on a system whose language is read right to left as is Hebrew, Arabic, and Persian Farsi to name a few.

Taking this a step further, consider the additional security and features that are provided by the manufacturer. A commonly known manifestation of this is the Microsoft Service Packs. These service packs provide needed security and maintenance updates along with new features for the user. These updates also change the operating system and often will close security vulnerabilities. Continuing with Microsoft XP as the example, there are four basic levels this operating system: XP, XP with Service Pack 1, XP with Service Pack 2, and XP with Service Pack 3. Each of those four levels has a 32 bit and 64 bit possibilities, giving a total of eight possibilities. Each of those eight possibilities natively support 106 languages raising the number of potential combinations to 359,128. Luckily, some languages are more predominant than others. Although Microsoft ceased supporting the XP operating system in April 2014, many systems with this operating system persisted two years later. In fact, the London Metropolitan Police continues to pay Microsoft for well over 27,000 systems running XP (Parrish, 2016).

Personal Security Protections are the software applications that most people call their anti-virus. This includes both the native applications in the operating system and the third party vendor software such as MacAfee and Symantec. These security applications monitor all processes within a device. Suspicious processes are halted, quarantined, and a notification sent to the user and potentially the PSP manufacturer for further examination. In some cases, such as the Chinese Qihoo 360 software, suspicious actions are sent to an Internet-based engine for analysis, comparison, and cataloging by the company. What makes Internet-based engines such as Qihoo 360 more dangerous is that these analytical engines potentially use reputation engines also. A reputation engine compares a sample to every other subscriber's submissions. If the sample has been seen numerous times, the reputation is considered "good." If this instance is the first time the reputation engine has seen the sample from any subscriber, the sample's reputation is considered suspect and devious, requiring more inspection or quarantine. Capabilities developed for cyber operations need to undergo testing to see what PSPs can and cannot detect the capability. The risk profile increases as adversaries adopt PSPs that either detect cyber capabilities more often or adopt Internet-based analytical engines. This is especially dangerous as it is nearly impossible to model Internet-based PSPs or reputation engines in a laboratory.

Signatures in software refer to the hash value of remnants of software code that remains on a device after the capability installs. Some capabilities leave no signatures behind for forensic examination. They either delete the installation file completely or are installed from a file remotely. In this later case, the file would exist at the friendly location of the operation or at a third-party location to prevent possible attribution. The goal is to reduce or eliminate as many software signatures as possible. However, the complete elimination of signatures on all capabilities is impossible. Therefore, similar capabilities with similar functions must have different signatures if they cannot be eliminated. This prevents a PSP from finding multiple tools easily after the company updates the signature library.

Redundancy refers to the number of capabilities available to perform the same or a similar function. To tie together previous examples, a friendly cyber operation keylogger is discovered on a computer through a forensic investigation. This is a new

keylogger and the signature does not exist in the PSP library. The PSP company evaluates the keylogger and creates a virus definition that is globally distributed to all subscribers. For the U.S. to continue gathering the intelligence garnered from adversaries typing, a new keylogger is needed. This new keylogger must have a different software signature than its predecessor, be missed by PSPs, accommodate the operating system and other software on the target, and be compatible with the hardware of the targeted device.

Now, expand those requirements out to encompass all the software capability functions such as, keyloggers, back doors into systems for later use, implants for listening and doing automated tasks, and network mapping and enumeration tools for discovering what machines are on the network by type and by software. Obviously, the risk increases if capabilities are needed quickly or are used in high risk operations. In the high risk operations scenario, the likelihood of being discovered is increased due to the adversary's sophistication. Therefore, a separate capability set is needed to reduce the chance of a capability discovered in a high-risk operation that otherwise would lead to a global discovery of the capability.

E. OPERATIONAL RISKS

Although the risks previously mentioned may cause significant repercussions, a greater risk is the potential to other operations being conducted. Risks in this area may extend beyond the local network and become global. Additionally, a detection or compromise of an actor may lead to other friendly actors and operations being discovered.

1. Risk to Operations

When planning cyber operations, the risk to the organization and potentially other friendly organizations needs consideration. A discovery of a capability by an adversary could waterfall into discoveries of other organizations conducting their own cyber operations within the network or subsequently, other locations around the globe. This is seen in the Kaspersky Equation Group report (Kaspersky Labs, 2015). In this report, the

discovery of one compromised system led to the discovery of multiple systems around the globe infected with the same capability. Additionally, the report discusses how the prior mentioned discovery also led to the discovery of other capabilities being used in multiple networks. Careful records of capability employment locations are needed in the event of a discovery. This allows friendly organizations to understand the potential impacts of a compromise and to prioritize remediation efforts. Two categories of risks exist in this scenario: risks to our organization and the risks to other friendly organizations.

The situation is bad enough if a lone organization is discovered on an adversary network. Capabilities or TTPs discovered by an adversary investigation could compromise other operations conducted by the discovered friendly organization. Compounding this problem is the potential for another friendly organization discovered during the investigation mentioned previously. In this event, both organizations potentially will lose multiple operations, capabilities, and accesses. As the number of times the same capability is used within a network increases, so does the risk. The proverbial needle in a haystack becomes more prominent.

Additionally, the risk increases as the number of actors increases within a network. Although this is deconflicted by whoever has primacy, this is not a guarantee of success. As discussed earlier, primacy belongs to the organization that first sustains operations within a target network. This organization has the ability to approve additional friendly actors and what operations these new organizations may conduct. If an organization is planning an operation within an adversary network, and it is discovered that primacy belongs to another organization, the operation cannot commence until permission is given. The potential also exists that permission will not be given and therefore, another alternative must be considered.

One of the greatest risks to operations is the discovery of an operation within a network that has a single access point. High-risk operations may have only one access point into the network to reduce the anomalous activity for an administrator to find. Another possibility is that the network access requires human introduction of the capability into the network, as with Stuxnet (Falliere et al., 2011). In these examples, the

loss of the single access point would eliminate all operations within the adversary network. Thus, the risks elevate when a single access point exists for a network.

2. Risks of Compromise

When an organization plans and conducts cyber operations the risk of compromise always exists. PSPs may update signature definitions and catch a capability. An administrator may notice and investigate anomalous behavior. The operator may commit a mistake that draws attention to the operation. Consider this example. In the course of our organization conducting cyber operations our capability is discovered. When this occurs, an immediate triage is needed to answer important questions. How was the capability discovered? What other capabilities are collocated on the same machine? Has the discovered capability been used in other locations within the same network? If other capabilities were collocated with the discovered capability, do these yet undiscovered capabilities reside elsewhere in the target network? Does the discovered capability reside in other networks of this adversary? Does the discovered capability reside within other adversary networks? Where else do the undiscovered collocated capabilities reside? This example demonstrates the potential impacts across the organization and to other friendly organizations. To put this into perspective we will examine another set of questions.

Has the capability been employed multiple times in the same network? If the answer to this question is "yes," then the risk of the capability being discovered increases. Additionally, the intelligence value provided by these capability instantiations should be considered either gone or suspect. If other employments are not found, the information brought back is considered suspect as the adversary may feed false information into the system in an attempt to either identify the attacker or to fool intelligence systems.

Does the capability reside within multiple networks of the targeted adversary? As an example, a capability is discovered in a Chinese Interior Ministry network. In this scenario, time may exist to remove capabilities from other government networks to stymie the loss of intelligence.

Does the compromised capability reside in multiple networks of multiple adversaries? Using the Chinese Interior Ministry example above, the capability has been employed also in the Philippines. Although the discovery in China is of concern, unless the Chinese government publicly announces the discovery or turns it over to a PSP company, the risk of discovery in the Philippines is minimal. This is not true if the other target is an ally of China in this example.

Does the compromised capability reside in multiple networks of allied adversaries? This scenario raises the risks as the assumption of allies sharing information is required. Building on the Chinese example above, the capability also resides in North Korean networks. North Korea is an ally of China and relies on China for Internet access and much of the North Korean communications infrastructure. China would be wise to share this information with North Korea to prevent contamination between the two countries. Additionally, the assumption is that adversary allies will share information to reduce the effectiveness of friendly intelligence operations.

Has a zero day been used? This previously discussed capability will draw attention if discovered. Zero-days are a sign of the highest sophistication of cyber actor, the nation-state organization. If a zero-day is found, a forensic investigation will occur to discover how the vulnerability was accessed and how it was delivered. Software development and PSP companies would request that the zero-day be given to them for remediation and updates to PSP definitions. The use of a zero-day raises the risk profile considerably due to the resources needed to create and weaponize this vulnerability (Bieleny, 2012; Rid, 2012; Warrick, 2011).

Did the compromised capability require a satellite transmission? As discussed previously, communication satellites are often owned by the adversary or a third-party entity. This owner likely monitors the traffic coming through the satellite and may be able to correlate geographically where the transmission came from.

Has the adversary discovered a cyber capability in the last year? In the event of the discovery of a cyber capability, the assumption is that the adversary will exhibit heightened awareness. Administrators will routinely examine networks and traffic within

the networks for suspicious activity, particularly of information leaving the network. If an adversary is known to have discovered a friendly capability, regardless of the friendly organization, a higher risk assessment is warranted.

What other friendly actors are collocated with the placement of the discovered capability? As previously discussed using the Kaspersky Equation report (Kaspersky Labs, 2015) the additional presence of another actor operating within the same adversarial space raises risks. However, following the Chinese Interior Ministry example, if another friendly actor is collocated within adversarial space the distance that the other friendly actor is from the discovery is important. The farther the collocation is from the discovery, the better. This allows for notification of the other friendly actor and the potential retrieval of their capabilities to prevent compromise.

Does the adversary have the ability to attribute the intrusion of their networks? This question raises concerns with potentially serious ramifications. Just as Stuxnet was immediately blamed on the United States due to its sophistication and the target being Iranian nuclear centrifuges, another cyber operation may be attributed to the U.S., rightly or wrongly (Bieleny, 2012; Rid, 2012; Warrick, 2011). Technical sophistication is required to trace the transmission through the Internet to the source. This requires resources, training, and potentially access to other networks.

3. Risk of Attribution

Inherently more dangerous than compromise is the risk of attribution. With detection, the adversary understands that something occurred. Compromise elevates the risks to the situation from the waterfall effect of your or other organizations' capabilities being discovered in one or more networks, as demonstrated in the Equation Group Report (Kaspersky Labs, 2015). However, attribution brings a new level of risk. With attribution, not only can the adversary say "something bad has happened" but they can say "you did it."

This condition brings a litany of issues. Some of which are political embarrassment and fallout, discovery of the infrastructure used for these computer operations, and retaliation. Political embarrassment and fallout are beyond the scope of

this research. Retaliation will be discussed later. Discovery of the infrastructure used for operations is the operational risk decision makers need to consider in their risk assessments.

The infrastructure used for these operations is meant to provide anonymity to friendly forces. Covert in nature, it uses protocols and hidden nodes within the Internet, some of which have been coopted or "captured" for these operations, the friendly operators hide within the abundant traffic "noise "of the Internet. From this noise, operations are obfuscated and are able to minimize the ability of the adversary to trace the operation back to its origin. Additionally, the adversary may actually allow the operation to occur because the operation is potentially hosted from a trusted source that has been coopted by friendly forces as part of a multi-step campaign.

If attribution to this infrastructure is made, the adversary then has the ability to do multiple things. First, the adversary has the ability to covertly observe friendly operations and gain both intelligence about our operations and also insight into how we conduct them. The ramifications for this include coopting the networks that we already conduct operations in so that they can get either a copy of the intelligence we attain or use our access to gather their own information. Additionally, the adversary may patch or change the access used by friendly forces in the target network so that only the adversary can have access. This would appear as if the network owner changed the configuration. The adversary may conduct an attack within this third party network to eliminate U.S. access and to potentially being attribution to the US. This action would prevent the U.S. from accessing the network, bring blame to the US, and keep the adversary out of the conversation.

More significantly however, is the potential of the adversary bringing attribution to the friendly infrastructure and then conducting intelligence and later, attack operations within friendly sanctuary. Not only could friendly intelligence be compromised or manipulated, the intelligence already collected then would be doubted. This situation worsens if the adversary conducts an attack within this infrastructure. Not only is the covert nature of the infrastructure violated, but the intelligence garnered from the use of

the infrastructure is in doubt, and no more operations can ensue until a redundant infrastructure is readied and confirmed to be unattributed.

Literature discusses the FCAPS methodology for managing networks developed by the Open Systems Interconnection (OSI) Group within the International Organization for Standardization (ISO) in the 1980s (ISO, 1989). FCAPS is an acronym for fault, configuration, accounting, performance, security. FCAPS is suitable for day-to-day operations of a network infrastructure. However, it fails to meet the needs risk assessment in this application. The security portion of the framework has a loose application at best with the last purpose listed in the ISO: "c) the reporting of security-related events" (ISO, 1989, pg. 3). With the risks involved in these operations, the more prudent action for attribution is to move to a redundant infrastructure that is considered unattributed and therefore, safe for operations.

4. Risk of Retaliation

If an adversary rightly or wrongly accuses the U.S. of breaking into their networks for intelligence gathering or conducting a computer network attack, the risk of the adversary retaliating is present. The U.S. has already labeled much of the computer infrastructure used to maintain utilities, banking, and travel as critical to the operations of the United States (The White House, 2013). An analysis of the adversary and their capabilities is required.

Does the adversary have the resources or the access to the resources to track operations back to the U.S.? This aspect raises the risk of attribution and in some cases, potential retaliation. If the adversary is a sophisticated cyber actor such a Russia, China, or Iran, or has an allied relationship with a sophisticated actor, the risk elevates (Duggan, 2015). If the adversary is not a sophisticated cyber actor such as Libya, Afghanistan, or non-state actors, or does not have access to an allied sophisticated actor, the risks do not rise.

Does the adversary have the capability to retaliate against critical U.S. infrastructure? In this scenario, an assumption is made that a sophisticated actor would risk the ramifications of retaliation against the U.S. on behalf of an ally. In 2013, the

White House issued Presidential Policy Directive 21 declaring 16 sectors of national infrastructure as "critical." This presidential directive assigned responsibilities for protecting these sectors among the federal agencies. Additionally, Presidential Policy Directive 21 delineated energy and communications as "uniquely critical due to the enabling functions they provide across all critical infrastructure sectors" (The White House, 2013). However, in 2010, the Russians hacked into the NASDAQ (Micahel Riley, 2014)**.** In 2012, the Iranians were blamed for the denial of service attacks on the financial sector (SIboni & Kronenfeld, 2014). Recently, China was suspected in the OPM breach where millions of records were stolen (Sanger, 2015).

Has the adversary demonstrated the ability to access critical infrastructure? Sophisticated cyber actors have already been found within U.S. critical infrastructure. Some of the adversarial operations have been for espionage or theft of intellectual property (Gilbert, 2014; Rid, 2012; Sheppard et al., 2013; U.S.-China Economic and Security Review Commission, 2008). Other intrusions look to manipulate the financial industry (Gertz, 2014; Michael Riley, 2014; Yadron & Gorman, 2013). Others have been for intelligence gathering (Mandiant, 2013).

With the potential decentralization of authority to conduct offensive cyber operations below the national level, lower level commanders would enter a realm where they are inexperienced and lack experienced or educated staffs to assess situations and risks. Furthermore, more nation-state and non-state actors are beginning to enter cyber operations (P. Duggan, 2015; Flemming & Stohl, 2000). These lower level commanders and their respective staffs need to understand the hurdles ahead of them to make timely and appropriate decisions (Eisenhardt, 1989; Fox & Tversky, 1995). Cognitive aspects that work in day-to-day life are inadequate for making risk assessments and decisions in new and unfamiliar operations. Additionally, the current risk assessment methodologies are qualitative, ambiguous in nature, and therefore inadequate for informing decision makers.

IV. COGNITIVE ASPECTS OF DECISION MAKING

Command and control of cyber operations relies on the ability to make decisions in a timely and accurate manner. As discussed previously, cyber operations do not occur across a linear map like traditional operations; the reach and ramifications of actions are much greater. Classical decision theory is often applied to command and control scenarios, but this theory is inadequate for decisions made under risk, in uncertainty, or with ambiguous information. According to classical decision theory, the objective is to maximize gains or the expected value by applying information in a specific way that advances these goals. Decision theory also assumes that the decision maker is accurately and consistently weighing, aggregating, and prioritizing information (Gutnik, Hakimzada, Yoskowitz, & Patel, 2006)

In the course of everyday life, people use different cognitive mechanisms to make sense of information, fill in gaps, and interpret data for decisions. They make deductive assumptions about situations to make sense of what they see, as in seeking to determine the cause of a car wreck. People also make assumptions to fill in gaps of information to continue planning or executing operations. Every military plan includes assumptions about what the adversary will do. People also interpret information, as happens every day in courts across the country, as different interpretations are argued. When, however, the decision maker is ill-equipped to arrive at appropriate decisions, and these cognitive mechanisms are applied, decisions may be faulty or inadequate.

The problem addressed in this work is when decision makers lacking experience, education, and expertise in cyber operations use these cognitive mechanisms to arrive at operational decisions. This dissertation provides a framework to potentially mitigate the effects of these cognitive mechanisms, offering individuals more objective solutions or recommendations. Consequently, this chapter will consider and discuss multiple aspects of decision making. The first will be a review of the cognitive process of decision making. Next, the chapter will examine heuristics, affect, and biases to include their effects on the decision maker. The third focus will be how decision makers are

susceptible to overestimating or underestimating the risks involved in their decisions. Finally, group dynamics and their effects on decisions will be discussed.

A. COGNITIVE DECISION MAKING PROCESS

Cognitive psychology recognizes decision making as one of the 37 fundamental cognitive processes of the brain (Wang, Liu, & Ruhe, 2004; Wang & Ruhe, 2007). Decision making is defined as the "process that chooses a preferred option or a course of action from a set of alternatives on the basis of given criteria or strategies" (Wilson & Keil, 1999; Yingxu Wang, Wang, Patel, & Patel, 2006). Wang et al. (2006) describe how two processes exist in the mind for controlling the 37 cognitive processes. The two processes are the Subconscious Process and the Conscious Process. The Subconscious process is in charge of the aspects of sensation, memory, perception, and action. These processes could manifest as vision, short-term memory, self-consciousness, and a sense of spatiality. The Conscious Process is responsible for meta- cognitive and higher cognitive processes. These could manifest as attention and decision making. (Yingxu Wang et al., 2006) and (Wang & Ruhe, 2007) further describe how decision making could follow one of three paradigms: normative, descriptive, or prescriptive. Normative decision making assumes that the decision maker is rational with well-defined preferences that obey rational behavior. Descriptive decision making is based on empirical data and experimentation of choice behavior. Prescriptive decision making focuses on the methods and processes used to improve decision making with the goal of making the decision maker's process more in line with normative decision making.

Regardless of the paradigm, decision making strategies and the associated criteria used for arriving at a decision fall into four categories: intuitive, empirical, rational, and heuristic (Wang & Ruhe, 2007). Intuitive criteria are based on the easier or familiar choice available based on perceived propensity or expectation; in short, common sense. Empirical criteria are based on exhaustive trials and results along with existing accepted knowledge and consultation. Rational criteria are trade-offs between costs, time, money, reliability, functionality, or any other criteria that has to be optimized against other competing requirements. Heuristic criteria are based on personal judgement and beliefs,

"rules of thumb" or personal bias (Kane & Webster, 2013; Wang et al., 2004). It is the area of heuristics and bias that this research attempts to mitigate or overcome.

B. HEURISTICS

Heuristics are the simple mental models or shortcuts that are used to explain complex ideas or unfamiliar situations (Colwell, 2005). However, heuristics are used to make "educated guesses" when information is lacking (Davis, Kulick, & Egner, 2005; Dowd, Petrocelli, & Wood, 2014; Grifffin, Neuwirth, Giese, & Dunwoody, 2002; Kahneman, 2003; Kane & Webster, 2013). Tversky and Kahneman (1974) describe three heuristic categories. They are representativeness, availability, and anchoring and adjustment. This work expanded with the inclusion of affect as a category (Finucane, Alhakami, Slovic, & Johnson, 2000). Each of these heuristics will be discussed in depth.

1. Representativeness

Representativeness is the use of mental categories for organizing and correlating information (Davis et al., 2005). A piece of information has high representativeness if it is very similar to a prototype of a category. Additionally, representativeness is used to compare new information to the category or between pieces of information. This may manifest as how people judge cause and effect on the basis of similarity of events. This tendency may lead to incorrect assumptions that relationships exist between pieces of information when actually they do not. Consider this example given by Tversky and Kahneman:

> consider an individual who has been described by a former neighbor as follows: "Steve is very shy and withdrawn, invariably helpful, but with little interest in people, or in the world of reality. A meek and tidy soul, he has a need for order and structure, and a passion for detail." How do people assess the probability that Steve is engaged in a particular occupation from a list of possibilities (for example, farmer, salesman, airline pilot, librarian, or physician)? How do people order these occupations from most to least likely? In the representativeness heuristic, the probability that Steve is a librarian, for example, is assessed by the degree to which he is representative of, or similar to, the stereotype of a librarian. Indeed, research with problems of this type has shown that people order the occupations by probability and by similarity in exactly the same way. (p.185)

In some situations, people will assign their own values to situations, overriding information that is given. When information is incomplete or time is not available for an exhaustive information search, heuristics are applied as assumptions to mitigate the missing data (Brookins & Ryvkin, 2014; Gilovich, 1991). These assumptions are prone to biases and often framed using extreme scenarios in the decision maker's mind. Framing is the manner in which the problem and solution choices are presented interacting with the norms, habits, and expectations of the decision maker, thus leading to the representativeness of the data. The purpose of framing is to simplify the analysis and evaluation of the potential solutions for the decision maker.

2. Availability

Availability refers to the ease in which a concept or information can be brought to mind (Davis et al., 2005; Gilovich, 1991; Kane & Webster, 2013). This may manifest as a person estimating how frequent or likely an event will occur. When an infrequent event or information however is brought to mind, the estimation of its likelihood can be overstated. For example, Tversky and Kahneman (1974) describe how people may overestimate the likelihood of dying of a heart attack in middle age due to the occurrence among acquaintances.

Budescu, Broomell, & Por (2009) demonstrated that even if the full information is available, people would still assign their own heuristics to the situation. In this 2009 study, Budescu, Broomell, and Por used predictions from the Intergovernmental Panel on Climate Control and asked 223 volunteers, divided into control and treatment, also known as translation in this study, groups what the phrases Very Unlikely, Unlikely, Likely, and Very Likely meant. These phrases were given numerical values. For example, Very Likely had a greater than 90% chance of occurring, while Very Unlikely had less than a 10% chance of occurring. In this study, the translation group was given the phrases but not the numerical scales and asked to apply these phrases when analyzing data. The control group was allowed to see the numerical scales at any time when they were asked to apply the phrases. What the researchers demonstrated was that even though the Control Group had access to the Panel's scales, the participants still assigned their own values.

This observation supports the notion that an individual's heuristics override and assign subjective values to information external of the decision maker's cognitive processes.

Additionally, people using availability heuristics are likely to retrieve extreme events at the time of decision to simplify the situation at hand and to limit the number of outcomes considered. In this context, extreme events are defined as one that is relatively rare in occurrence (Ludvig, Madan, & Spetch, 2013). These events are easily comprehendible, however unlikely to occur. This phenomenon manifested itself more prominently when risky choices led to extreme outcomes. This aspect of decision making puts the decision maker at a distinct disadvantage. Not only are out-of-context mental frames of reference used in weighing alternatives, but the decision maker will tend to choose a riskier option which results in a more extreme outcome.

This detriment is compounded when the decision maker has incomplete data. In this scenario, the decision maker must rely upon heuristics to fill in the holes with assumptions that allow the decision making process to continue. Aggravating this situation further is the aspect of time. In a time-constrained environment with incomplete information, heuristics applied as assumptions cannot be confirmed or denied and may become part of the decision making process as if they are fact (De Dreu, Nijstad, & van Knippenberg, 2008; Driskell & Salas, 1991; Kleespies, 2014). In military operations, particularly cyber operations where situational awareness of the contested space often cannot be illuminated from multiple sources, the incomplete data coupled with a time constrained situation is common. This puts decision makers in a dilemma for command and control of operations. Not only is time short, but information is missing. Heuristics and biases, compounded with a lack of experience, may lead the decision maker to choose a course of action that is not only sub-optimal, potentially detrimental.

3. Anchoring and Adjustment

Anchoring and adjustment refers to a situation in which people estimate a number. This number used as a starting point, particularly in negotiations, is referred to as the anchor. The anchor then shifts up or down to reach an answer that is plausible or acceptable. This shifting is the adjustment (Davis et al., 2005). However, anchoring and

adjustment lead to the tendency for people to stay close to the anchor point, even if it is unreasonable. This effect is more pronounced when subjects must make decisions quickly (Yudkowsky, 2008). Additionally, this effect is more profound when estimates are presented as a confidence interval. One often repeated finding asserts that when participants are 98% certain that a number is within a particular range, they are incorrect about 40% of the time (Lichtenstein, Fischhoff, & Phillips, 1977; Tversky & Kahneman, 1974).

Tversky and Kahneman (1974) state,

> People make estimates by starting from an initial value that is adjusted to yield the final answer. The initial value, or starting point, may be suggested by the formulation of the problem, or it may be the result of a partial computation. In either case, adjustments are typically insufficient. That is, different starting points yield different estimates, which are biased toward the initial values. (p. 1128)

The ramifications of this type of heuristic being incorrect are many. In their meta-analysis, Orr and Guthrie (2006) demonstrate realistic dangers of anchoring. Anchoring is a common and well-known practice in negotiations where a value, often numerical, is offered as an example or an initial offer. From this value, negotiations can commence. Individuals are likely to use this tactic to increase the potential of attaining their goals in the negotiations. This number may be introduced either innocently or maliciously.

As an example, suppose you are interested in purchasing a house. The asking price conveys meaningful information about the house and neighborhood. However, an overreliance on this asking price may result in overpaying for the house. The second potential pitfall from anchoring in this scenario is if you, as the potential home buyer, overly rely on irrelevant or uninformative information in the decision process. For example, an article in the newspaper recounting the median price of houses in San Francisco would be irrelevant if you are purchasing a house in Atlanta where the cost of living and property is much lower. However, this information may be used as a reference point when considering a counteroffer to the asking price for a house in Atlanta. Anchoring using extraneous information has the ability to shape thinking in decision makers and cause cognitive fallacies as this information has the potential to mislead in multiple ways.

4. Affect

Affect refers to emotions or feelings that sway the judgement of the decision maker. Examples of the emotions or feelings that may sway a decision maker are fear, anger, surprise, or dread and have a personal value of "goodness" or "badness" (Clore, Gerald L & Huntsinger, Jeffery R, 2007). Affect is not to be confused with the mood of the individual as mood is considered longer in duration (Finucane et al., 2000; Kane & Webster, 2013).

A decision maker's affect can be manipulated using the decision maker's heuristics as a vehicle when framing the problem (Finucane et al., 2000). In that study, 200 participants were given surveys about the risks and benefits they perceived about nuclear power, food preservatives, and natural gas. The participants were then divided into four groups: high risk, low risk, high benefit, and low benefit. Next, they were then given innocuous vignettes about these technologies. The low benefit for nuclear power vignette centered around the statement "Nuclear power today produces only a small percentage of our nation's electricity." The participants were then given the same surveys as in the beginning. In this study, of the 657 total surveys given, manipulation occurred in 50% of the cases.

Prior research has identified the linkage between affect, the decision maker's perception and assessment of risk, and decision-making. Arceneau (2012) and (Girodo, 2007) describes the power of fear in decision making, even when a valid counter argument is available and provided. Kahneman & Tversky (1979) demonstrated that affect can cause the decision maker to be risk averse if already gained resources or potentially gained resources potentially will be lost. Additionally, Kahneman and Tversky demonstrated that negative affect leads to more risky choices in decision-making. This finding was reinforced by research by Buelow & Suhr (2013), Bruyneel, Dewitte, Franses, & Dekimpe (2009), Figner, Mackinlay, Wilkening, & Weber, (2009) Weber & Chapman (2005), and Kahneman & Lovallo (1993). Conversely, happiness may desensitize a decision maker to a genuine or likely loss (Figner et al., 2009; Isen & Geva, 1987; Kahneman & Tversky, 1979; Nygren, Isen, Taylor, & Dulin, 1996).

C. BIAS

Biases are tendencies to conceptualize new information in known or comfortable ways that potentially lead to erroneous judgements and decisions that produce systematic deviations from a standard of rationality or good judgment (Kane & Webster, 2013). Biases derive from past experiences, interpretations of the world, social pressures, emotional responses to stimuli, the limitations of the individual's mental processing capacity, or a mismatch between the decision maker beliefs and the environment (Davis et al., 2005; Kahneman & Tversky, 1984; Kahneman, 2003, 2013; Tversky & Kahneman, 1974, 1981). Biases are implemented in everyday choices; such as what store to shop at, what brand of clothes to purchase, where the best neighborhood to live in is, and what car to drive, to name a few. Most importantly, biases participate in the use of heuristics to create understanding or perceptions reality for the decision maker. Although no definitive list exists within psychology of all the biases that decision makers will encounter, I will highlight the bias effects of a small core that face every decision maker. These are confirmation bias, attention bias, belief bias, and the clustering illusion. (Tversky & Kahneman, 1974; Milkman, Chugh, & Bazerman, 2009; Heilbronner, Hayden, & Platt, 2010; Dowd et al., 2014). These biases are predominant within the decision making literature and plague both laymen and scientists within decision making research (Kane & Webster, 2013). This discussion will be followed with an overview of the role that group dynamics plays for distorting decision making and how risk is either overestimated or underestimated.

1. Confirmation Bias

Confirmation bias is when an individual looks for or favors information over other information because it confirms existing beliefs or a desired endstate (Davis et al., 2005). During election campaigns, constituents often seek information that favors their preferred candidate and seeking information that casts the other candidates in an unfavorable light (J. Duggan & Martinelli, 2010; Kane & Webster, 2013). The ramifications of this bias in decision making are highly significant. Salient information will be discounted or ignored, leading to inaccurate analysis of events and poor decision making.

2. Attention Bias

Attention bias is a fixation on a stimulus that leads an individual to regard other stimuli or information as less significant or even ignore them altogether. Although the decision maker may consider this action to focus on the most salient information, prior research has shown differently. Past research efforts have demonstrated that obese children will fixate on information or cues regarding food to the point of the detriment of other cognitive tasks (Kane & Webster, 2013; Koch, Matthias, & Pollatos, 2014). This fixation, not a holistic evaluation by decision makers, may lead to disastrous consequences due to the demotion of relevant information.

3. Belief Bias

Belief bias describes the dynamic in which the logical strength of an argument is judged based on the believability of the conclusion (Kane & Webster, 2013; D. Schneider, 2007). This is seen in situations where the outcome is revolutionary or unprecedented. Consider the example that a good experience will be more enjoyable when it follows a bad experience. This potentially stands to reason as the good experience will seem "better" after the occurrence of a bad experience that takes the observer below the baseline of enjoyment. However, research in jelly bean tasting demonstrates that this is a fallacy. In fact, the same results held when bad experiences followed a good experience (Novrmsky & Ratner, 2003). Thus, decision makers asked to accept a recommendation that departs from normal procedure or attempts something novel are likely to deny the request or accept with great skepticism.

4. Clustering Illusion

The clustering illusion is a state in which the decision maker perceives patterns in data that do not actually exist (Kane & Webster, 2013; Oskarsson, Boven, McClelland, & Hastie, 2009). Consider the example examples of "hot hands" in gambling or disease clusters in neighborhoods. These patterns may seem obvious on the surface, but no data supports the patterns that the analyst or decision maker perceives. To put this into perspective, consider a fair coin flipped 10,000 times. During these 10,000 trails, streaks of either "heads" or "tails" will occur. People will begin to doubt the fairness of the coin

and attribute the streak as a pattern, even though the Law of Large Numbers accounts for these streaks (Oskarsson et al., 2009).

D. GROUP DYNAMICS

In an organization such as the military, where a staff does analysis for the decision maker, group dynamics typically come into play. Often, assertive and sometimes aggressive personalities are sought for key positions to maximize the probability of mission success. These personalities are sought for bold and audacious planning instead of predictable and repetitive planning. One of these instrumental positions is the Operations Officer. This individual is responsible for all planning and coordination that occurs within an organization's garrison and wartime operations. The Operations Officer also has the responsibility to ensure that any proposed operation meets the commander's articulated vision for the endstate and therefore not voiced by subordinates.

Subordinates, or even peers, may actually disagree and at times with choices made, even though this would be considered undesired by the decision maker. Disagreeing individuals may begin to question the knowledge, abilities, and understanding of the problem at hand. This cognitive doubt then becomes a silent agreement by the disagreeing individuals with the decision made (Asch, 1955, 1956; Gilovich, 1991). Adding to this disagreement is the condition in which personal agendas come into play (Garvin & Roberto, 2001). If key personnel are attempting to advance their reputation for mission accomplishment and continued success in the face of overwhelming circumstances, this agenda will often override outside inputs warning of higher risks and unattainable goals (De Dreu et al., 2008). When a disagreeing opinion is offered for overall plans and courses of action, the person with the agenda will often ignore the divergent points of view or even consider that person divisive (Asch, 1956).

High stress or even crisis situations have other unintended consequences within groups. Research has shown that under such stress, group members will defer to the leadership and even withhold important information (Foushee, 1982). Additionally, when stress is applied to groups, decision making authority is often withheld at higher levels of the group hierarchy (Driskell & Salas, 1991). In this study, aircraft flight recorders

recovered from crashes were examined, and it was found that flight crews withheld information from the pilot that they were deferring to prior to the plane crashing. Research also demonstrates that people deferring to the opinions, ideas, and actions of the group leader occurs more in stressful situations (Driskell & Salas, 1991; Helmreich, 1979). This results in a failure to obtain and integrate all relevant information and a tendency to focus on attaining the missing information (Burtscher & Meyer, 2014).

E. OVERCONFIDENCE VERSUS OVERESTIMATION OF RISK

If people find themselves in unknown circumstances, the likelihood of being either overconfident or overestimating the risks is possible (Davis et al., 2005). In this context, an overconfident person is one who assesses the situation with a lower risk than what is accurate. Conversely, a person who overestimates risk is one who assigns a higher risk value than is necessary. Decision makers often overweigh low probabilities of success and thus underweigh higher risks. This phenomenon can be seen when people buy lottery tickets but not insurance when they live in a likely disaster area (Heilbronner et al., 2010; Kahneman & Tversky, 1984). A significant contributing factor is how the problem is framed to the decision maker. Decision makers tend to trend as risk averse for gains and risk seeking for losses (Ludvig et al., 2013; Tversky & Kahneman, 1974). Additionally, Heilbronner states that decision makers "are more risk seeking when they will be forced to learn the outcome of the unchosen option than when they will not" (Heilbronner et al., 2010).

Kahneman and Lovallo (1993) describe how individuals manifest overconfidence in themselves when assessing the risk associated with multiple choices. In their study, participants assessed that they were correct approximately 99% of the time when in reality the success rate hovered around 80%. Part of this discrepancy stemmed from optimism. Cooper, Woo, and Dunkelberg (1988) describe how entrepreneurs often assess their chances of success as higher than that of peers within the same field, citing that participants did not base predictions of themselves on predictors of success, such as college education and experience within that field. When self-assessing, the entrepreneurs considered the situation holistically and did not factor individual aspects such as a lack of

education or experience. Within the sample of entrepreneurs, over 80% of the individuals surveyed assessed themselves as having a 70% or higher chance of success. Conversely, the sample rated their peers' success at only 59%. In reality, the five-year success rate was closer to the historic 33%.

Kahneman and Tversky (1981) detail how framing choices considered as potential solutions can radically alter the decision maker's risk attitude.

> consider a person who has spent an afternoon at the race track, has already lost $140, and is considering a $10 bet on a 15: 1 long shot in the last race. This decision can be framed in two ways, which correspond to two natural reference points. If the status quo is the reference point, the out- comes of the bet are framed as a gain of $140 and a loss of $10. On the other hand, it may be more natural to view the present state as a loss of $140, for the betting day, and accordingly frame the last bet as a chance to return to the reference point or to increase the loss to $150. (p. 456)

This work, along with others, clearly demonstrates how a decision maker is more risk averse when the outcome is framed as a gain. In this research, the decision maker has made the mental leap that the potential gain is already possessed. The perceived value of a potential gain decreases with the rise in risk (Davis et al., 2005; Gutnik et al., 2006; Heilbronner et al., 2010; Kahneman & Tversky, 1984; Lerner & Keltner, 2001; Loomes & Sugden, 1982; Ludvig et al., 2013; Pachur, Hertwig, & Wolkewitz, 2014; Pratto, Glasford, & Hegarty, 2006; Prelec & Loewenstein, 1991).

However, if the problem is framed as a loss, the decision maker becomes risk seeking. In previous research, it has been demonstrated when given options for risk and reward, people will accept ten times the risk for potentially ten times the reward (Kahneman & Tversky, 1979; Markowitz, 1952; Weber & Chapman, 2005). Using the horse racing scenario listed above, when the outcome is framed as a loss, the decision maker will cognitively frame the scenario as a deficit and will attempt to break even or turn the loss into a gain. To do this, the decision maker must increase the risks they are willing to accept in order to obtain greater reward (Gutnik et al., 2006).

In striking contrast though is the "peanut effect" (Weber & Chapman, 2005). This effect states that decision makers are more risk seeking when small gains are at stake

versus larger gains. This condition where smaller gains induce larger risk tolerance can be graphically stated using a utility function. Kahneman and Tversky (Kahneman & Tversky, 1979; Tversky & Kahneman, 1992) describe how the utility function is concave for gains and convex for losses with the origin of the graph being the point of indifference. By framing the potential gains in smaller terms than what the decision maker considers a large gain, the risks tolerated increase dramatically on the utility function. Larger gains expressed on the utility function begin to plateau and require greater increases of risk to bring reward as compared to the amount of risk taken for an equal amount of reward when expressed as a small gain.

When weighing risk, the potential for regret often factors into decision making. The potential that an increased value or utility would be obtained if a different decision was chosen is often considered as part of the decision making process (Humphrey, 2004). Consider the person who plays the lottery each week, habitually picking the same numbers. This person may have used the same numbers for years and in the process losing money each week. However, this person will continue to be risk seeking each week. In the event that those numbers routinely played each week are chosen as the winning numbers, the regret of not purchasing a lottery ticket would be enormous. Hence, this person will continue to lose money each week and experience greater value knowing that these numbers are played in the event they are drawn. Conversely, a person who is overly sensitive to regret may, in fact, become risk averse.

All of the previously mentioned aspects of the cognitive decision making process are generally used without any mathematical rigor in day-to-day decision making. Making simple single objective decisions typically does not require mathematical rigor in everyday life. However, if the decision maker must concern themselves with multiple objectives that may cause trading off between objectives for attaining the maximum perceived value, then mathematical methods and rigor are needed. The next chapter will discuss decision making with multiple objectives under conditions of certainty. This discussion will be followed with the sixth chapter, which examines decision making with multiple objectives under conditions of uncertainty.

THIS PAGE INTENTIONALLY LEFT BLANK

V. DECISION MAKING WITH MULTIPLE OBJECTIVES

Commanders of cyber forces are concerned with maximizing the effectiveness of operations while minimizing their resource costs. Operational commanders prefer a minimum risk alternative that maximizes effectiveness while simultaneously minimizing costs. This is a problem of classic multi-criteria decision making as described by Keeney and Raiffa (1976). This dissertation addresses the issue of risk in this classic problem by taking a two-staged approach. First, the solution of the deterministic multi-criteria decision problem is obtained. Second, this author embeds this deterministic solution in a framework of uncertainty as viewed by subject matter experts (SME). The bedrock of the approach is the deterministic solution. Therefore, this chapter reviews the concepts, models, and procedure for decision making with multiple competing objectives under certainty. The role of uncertainty and its incorporation is deferred until the next chapter.

This chapter begins with a discussion of models of decision maker preferences. The second section details modeling issues, eliciting the decision maker's individual preference functions, eliciting decision maker tradeoff weights, and constructing a joint additive form of the decision maker preference function.

A. THE MODELING OF DECISION MAKER PREFERENCE UNDER CERTAINTY

Decision makers, in general, have more than one concern in making a decision. They want to choose an alternative CoA that produces the best possible outcome for each concern. Eliciting these issues of concern is not always straight forward and considerable thought is required. (Keeney, 1992). The result is an objectives hierarchy that defines the issues of concern in terms of a set of objectives. These are expressed in terms of the infinitive form of a verb such as "to maximize" or "to minimize." Examples from cyber operations might be "to maximize intelligence gathered" or "to minimize the probability of detection."

Henceforth I assume that this structuring yields the decision maker's valuation of CoA and alternatives as a function of a set of *N* measures, one for each objective, indicated by x_k and collected into a *N*-vector:

$$\mathbb{x}(a) = [x_1(a), x_2(a), \ldots, x_N(a)]',$$

where $x_k(a)$ indicates the dependency on the CoA.

The decision maker expresses preferences over the set of outcomes, $\mathbb{x}(a)$. For example, they may wish to maximize some subset of this collection of outcomes, to the extent possible, through the choice of the CoA. At the same time, they may desire to minimize the remaining set of outcomes. These preferences are represented by a function often called the overall value function:

$$Y(\mathbb{x}(a)) = f(v_1(x_1(a)), \ldots, v_k(x_k(a)), \ldots, v_N(x_N(a))).$$

The $v_k(x_k(a))$ are individual value functions that describe decision maker preferences of x_k, independent of the preferences over the other x_k. In the military context, this function expresses the overall effectiveness of a chosen CoA for the decision maker.

The exact form of this function depends on specific assumptions concerning the structure of decision maker preferences. If these preferences are mutually preferentially independent, the function is additive (Dyer & Sarin, 1979; Keeney & Raiffa, 1976; Keeney, 1992; Kirkwood, 1997). The additive value function is more commonly used in practice, is a good first approximation of decision maker preferences, and is the easiest with which to work. The additive form value function is used in this dissertation. It takes the following form:

$$y = \sum w_k v_k(x_k(a))$$

where w_k are tradeoff weights, or scaling factors, that express decision maker preferences between the v_k. For example, if the decision maker desires to maximize x_k while also wishing to maximize x_j, the decision maker may have greater concern for the

maximization of x_k than the maximization of x_j. In this case, we would find that $w_k > w_j$. These w_k must satisfy two conditions: $0 \leq w_k$ and $\sum w_k = 1$.

B. CONSTRUCTING THE ADDITIVE MODEL OF DECISION MAKER PREFERENCES UNDER CERTAINTY

The construction of an additive value function proceeds in two phases. Preliminary to these phases, a scale of measurement for each of the objective measures $x_k(a)$ will have been established as part of the hierarchical structuring of the individual objectives. First, the individual value functions are constructed. Second, the tradeoff weights are assessed using the perception of values described by the individual value function. Both phases rely on the concept of indifference. The analyst seeks out situations in which the decision maker cannot decide between two choice options. Here is where the decision maker is indifferent between the two options because each is equally preferred.

The construction of the individual value functions is accomplished through a process of repetitive questioning to determine the decision maker's perception of value for each x_k. This dissertation assumes this is executed via the method known as Mid-Value Splitting (Kirkwood, 1997). An example is illustrated below in Section 1, Constructing Decision Maker Value Functions.

Tradeoff weights are assessed using pairs of measures, for example, between two measures, x_k and x_l. The analyst seeks to establish points of indifference between pairs, say $[x_k', x_l']\ and\ [x_k'', x_l'']$, such that the decision maker's value of $[x_k', x_l']$ equals the decision maker's value of $[x_k'', x_l'']$. Within each level of the hierarchy, one must consider as many pairs as the objectives in that level. An example is illustrated below in Section 2, Modeling Decision Maker Tradeoff Weights.

1. Constructing Decision Maker Individual Value Functions

Mid-Value Splitting (Kirkwood, 1997) is illustrated in Figure 2. Here the decision maker prefers more of x_i to less of x_i. The process begins by assigning a value of zero to the least preferred possible outcome for x_i and assigns a value of one to the most preferred possible outcome for x_i. Thus,

$$v_k(least\ preferred\ x_k) = 0$$

and

$$v_k(most\ preferred\ x_k) = 1.$$

In the case depicted in Figure 2, the analyst has found the decision maker is indifferent between the increase in value in going from x_i^L to $x_i^{0.5}$ and the increase in going from $x_i^{0.5}$ to x_i^H. Since the total value between x_i^L and x_i^H equals unity, the value assigned to $x_i^{0.5}$ must equal 0.5 (hence the notation used for the point of indifference). Now we repeat this process for the portion of x_i below $x_i^{0.5}$ and that above it. Indifference means that $v_i(x_i^{.25}) = 0.25$ and $v_i\ (xi^{.75}) = 0.75$. At this stage the analyst can sketch a curve connecting the five points established to get a graphical representation of $v_i(xi)$. For analytical work these five points can serve as input to a least-squares curve fitting exercise on a computer.

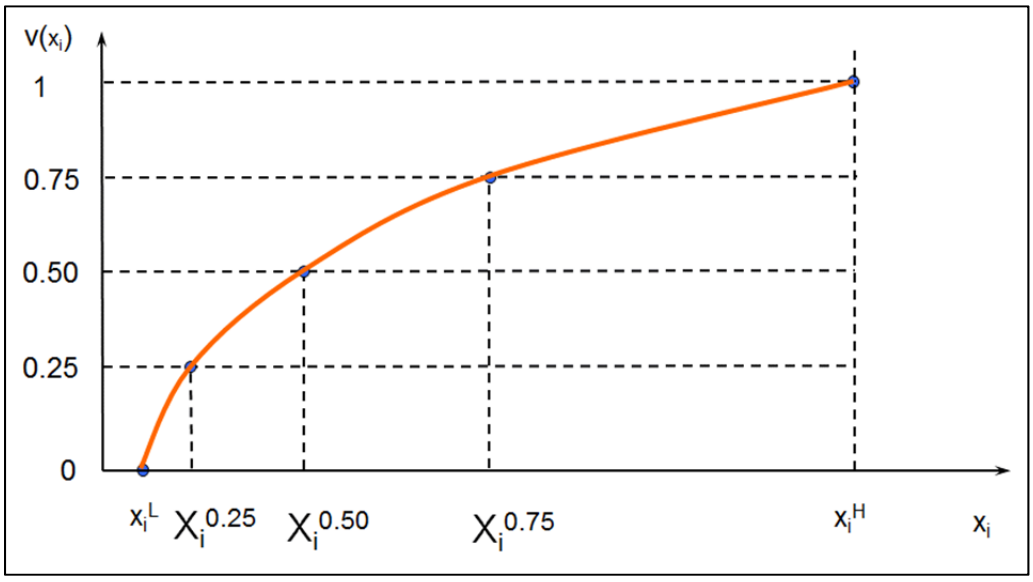


Figure 2. Example Graphical Depiction of Mid-Value Spitting

The curve in Figure 2 can be easily represented, as described by Keeney, Raiffa, and Rajala, by the function

$$v_i(x_i) = K\left[1 - e^{g(x_i)}\right],$$

where

$$g(x_i) = -\rho\left[\frac{x_i - x_{0i}}{S_i}\right]^{m_i} \; and \; mi \; = \; Si \; = \; 1.$$

(Keeney, Raiffa, & Rajala, 1976; Kirkwood, 1997). This value model is very flexible and can accommodate variety. See Figure 3 for a set of decision maker values used in the research for this thesis. The first two represent preference for "more" while the third, fourth and fifth value functions represents preference for "less."



Figure 3. Example Graphing Output of Decision Maker Values for Hierarchy Goals

The decision maker also has preferences for the cost of an alternative. Here preferences are such that "less is preferred to more." Thus, we must not forget to solicit these preferences and include these in our evaluation of a CoA. Indeed, this is explicit when the decision maker wishes to make a choice based on consideration of "cost-effectiveness." The individual value function for cost, denoted as $v_c(a)$ will be similar in shape to those last three examples in Figure 3. Of course, the horizontal axis will be in monetary units and not probability.

2. Modeling Decision Maker Tradeoff Weights

The determination of the tradeoff weights changes the focus of the discussion from preferences relating to a single x_k to pairs of measures x_k *and* x_l. Once again, the analyst seeks to discover points of indifference between choices.

Figure 4 provides an illustration of how indifference between pairs of measures reveals information relating to the tradeoff weights.

Here the question and answer process guided by the analyst finds the decision maker is indifferent between the two pairs shown in the figure. This indifference means that each pair has equal value for the decision maker and is expressed as

$$w_k v_k(x_k + \Delta_k) + w_j v_j(x_j - \Delta_j) = x_k v_k(x_k) + w_j(x_j).$$

Therefore,

$$\frac{w_k}{w_j} = \frac{[v_j(X_j) - v_j(X_j - \Delta_j)]}{[v_k(X_k - \Delta_k) - v_k(X_k)]}.$$

The evaluation of the right-hand side uses the results of the construction of the individual value functions. As an example, if $w_j = 0.6$ and $w_k = 0.4$, then the resulting ratio is .67. Thus, the decision maker only values the change in x_j about $\frac{2}{3}$ the amount of the change in x_k. This ratio and subsequent weighting of value is sometimes erroneously referred to as importance weights. This is incorrect, the weights denote the value of change when comparing between attributes, not the importance relative to the attributes themselves.

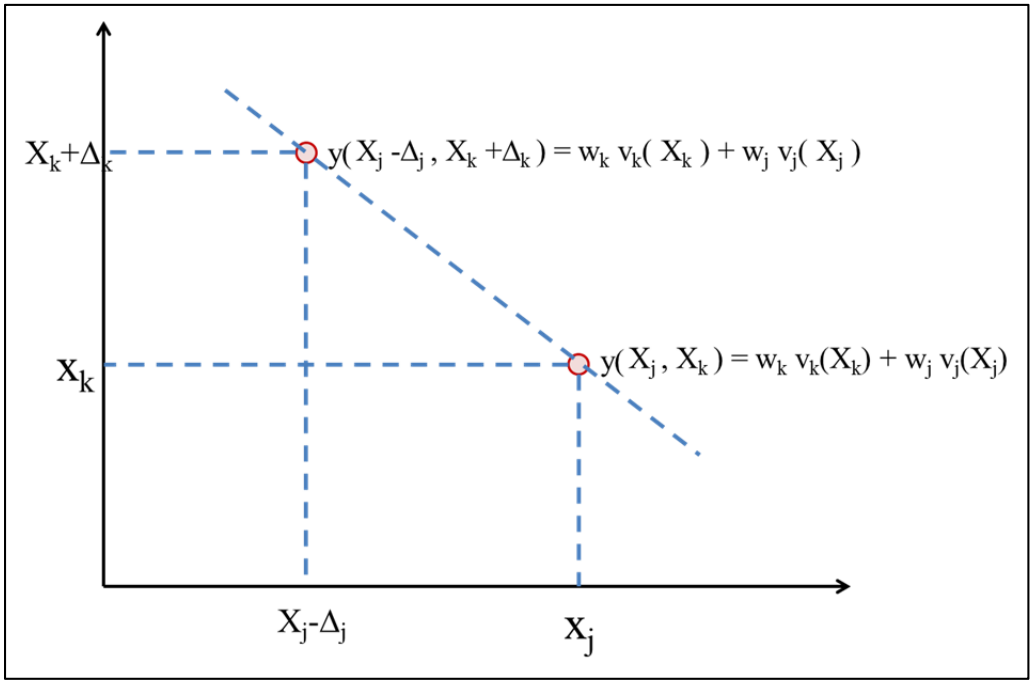


Figure 4. Illustration of Tradeoff Weight Determination

C. CONSTRUCTING AN ADDITIVE MODEL FOR COST-EFFECTIVENESS

A desire to compare CoAs on the basis of effectiveness and cost requires the construction of a measure of cost-effectiveness. Once again the additive form is used to effect. Let Z(a) denote the overall cost-effectiveness of a CoA, then

$$Z(a) = w_E Y\big(\mathbb{x}(a)\big) + w_C v_C\big(C(a)\big),$$

where $w_E + w_c = 1$, and $v_c\big(C(a)\big)$ denotes a "less is preferred to more" value function for cost as defined in Section B1 of this chapter. These tradeoff weights w_E and w_C describe how much cost the commander would be willing to pay to obtain an additional unit of effectiveness.

This thesis assumes that the decision maker has been led through the entire process outlined above. First, the issues of concern have been revealed and structured into an objectives hierarchy with explicit definition of the objectives measures, x_k. Next, individual value functions, $v_k(x_k)$, have been constructed for each of the objectives

measures, x_k. Third, a tradeoff analysis has been completed, yielding tradeoff weights, w_k, that represent decision maker preferences across the individual value functions. Lastly, and an additive form value function has been constructed that adequately represents the overall preferences of the decision maker for choosing a preferred CoA.

Under certainty we would now have the tool by which the decision maker can answer the question: "What's the best CoA?" This thesis, however, recognizes that choosing a CoA is seldom, if ever, performed in a world of certainty. Decision making in cyber operations is immersed in uncertainty. Risk exerts an influence on decision making that must be incorporated in the decision making process. The next chapter addresses this issue.

VI. RISK MODELING

This chapter continues the discussion of decision making with multiple objectives, but introduces conditions of uncertainty. It is within this context that this research advances the body of knowledge. This research incorporates the prospect function to model decision maker values and preferences. Additionally, it incorporates SME estimates of success along with SME estimates their own uncertainty, something previously not done.

This chapter begins with a historical examination of risk and its mitigation. Next, more contemporary definitions of risk are examined along with a quick analysis of why these definitions are inadequate for quantifying risk. The third area of discussion introduces Kaplan and Garrick's seminal work on quantifying risk, which this research aims to expand. Next is a discussion of the four questions that a decision maker must answer when multiple objectives compete in decisions. These four questions then lead into decision making under conditions of uncertainty and how one mathematically models those decisions.

A. A BRIEF HISTORY OF RISK

Throughout history, man has sought to understand and mitigate the hazards of the world to increase success and prosperity. As early as 3000 BC, Chinese merchants sought to prevent losses by spreading their cargo to multiple vessels. The first recorded instances of insurance date back to Babylon - the code of Hammurabi. "Bottomry" was the advancement of money to protect merchants against the loss of a ship and subsequently, the merchant's cargo. The practice of bottomry was continued through the Roman Empire as Justinian restricted advanced interest money to 12% (Vazzano Ltd, 2011).

In 700 BC, the Phoenicians and Greeks observed Rhodian Law, which states: "Let that which has been jettisoned on behalf of all be restored by the contribution of all." This law further stipulated that "A collection of the contributions for the jettison shall be made when the ship is saved" (Vazzano Ltd, 2011). Civil regulations such as the Rhodian example continued, and in 1384 AD, a commercial firm issued the first maritime

insurance policy. This policy covered four bales of textiles as they transited from Pisa to Savona, Italy (Vazzano Ltd, 2011).

Although modern applications of the word risk include the potential for gains occurring from an unmitigated uncertainty, the word risk often has a connotation of loss. Man has struggled with the concept of risk and loss for over 5000 years, and these concepts continue to provide problems. As mentioned in previous chapters, many risk assessment methods employed are qualitative and less helpful than the quantitative methods. It is the concepts of uncertainty and loss that plague decision makers today, particularly when they seek to optimize multiple objectives.

B. CONTEMPORARY DEFINITIONS OF RISK

In contemporary form, the word risk still has a primary connotation of the potential occurrence of bad consequences. Merriam-Webster defines risk as "The possibility of loss or injury" (Merriam-Webster, 2015). Even the Oxford dictionary defines risk simply as "A situation involving exposure to danger" (Oxford University, 2016). Moving to a narrower use of the word, let us examine a professional organization that offers risk certifications, the Information Systems Audit and Control Association (ISACA). What is unique about ISACA is that this organization uses definitions adopted and created by ISO. ISACA shares its definition of risk with ISO 73:2009 (Risk Management—Vocabulary): "The combination of the probability of an event and its consequence" (International Organization for Standardization, 2009).

The U.S. government's standard bearer of operational and research terms, the National Institute of Standards and Technology (NIST), defines risk as "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstances or event would occurs [*sic*]; and (ii) the likelihood of occurrence" (NIST, 2014). Using applications of the word risk that are more closely aligned with this research, the DOD uses the following definition: "Probability and severity of loss linked to hazards" (Department of Defense, 2016). The Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition (2015) clarifies risk in the following manner: "A single

action, event, or hardware component that contributes to an effort's 'Risk'; This is a probability multiplied by an impact."

Although these definitions appear to use mathematics to quantify risks, they are cursory efforts that do not account for uncertainty or decision maker preferences. The ISACA and NIST methods are traditionally used to attain enough insurance or to determine the need for business continuity planning and disaster recovery. None offers a quantifiable method of measuring risk beyond the financial impact to tangible devices. Furthermore, none can accommodate a quantifiable assessment of risk in an adversarial situation. This research effort explores how a better method of quantifying risk could lead to better decisions. This new method considers expert opinion, the experts' uncertainty, and the decision maker's preferences. This method is quantifiable and provides an unbiased evaluation of the alternatives available.

C. A QUANTITATIVE DEFINITION OF RISK

In 1981, Kaplan and Garrick (1981) published their seminal paper, "On the Quantitative Definition of Risk," introducing three simple questions to begin quantifying risk. They are rephrased as the following:

1. What can happen?
2. How likely is it to happen?
3. If it does happen, what are the consequences?

Kaplan and Garrick introduced these questions to provide the information needed by policy makers, or the general public, when making decisions about how best to manage risk. They refer to their work as *risk assessment.* The use of their assessments in decision making involves combining these assessments with decision maker preferences. This process they define as *risk management*. They used the nuclear site cleanup at Hanford, WA as the subject of their investigations. Kaplan and Garrick focused on answering their questions based on facts, expert assessments, and engineering principles. They, however, avoided public preferences and measures of satisfaction, instead letting public debate and decision determine how well the cleanup was executed. Because of this shift of responsibility to the public, a fourth question was not included in the definition:

How do you feel about the consequences? (Garrick, 2008).

This fourth question is especially crucial when a single person or a select group, such as a board, makes decisions. This is the context of this research: a commander making operational decisions using input from the staff. This fourth question seeks the decision maker's preferences, which are required to obtain a complete quantitative representation of the decision maker's sense of risk. These preferences provide the mechanism by which the answers to the first three questions can yield a quantitative representation of decision maker risk.

D. LIMITATIONS OF THE EXPECTED UTILITY THEORY APPROACH TO RISK

Historically, expected utility was the standard used to model preferences under uncertainty to maximize net gains (Ramirez & Levine, 2013). The utility function, introduced by Bernoulli (1738) and popularized in 1944 by John Von Neumann and Oskar Morgenstern, became the cornerstone of the theory for how people are rationally expected to act or react (Bernoulli, 1954; Levin, 2006). The utility function uses preference statements such as "When this occurs, do this" as integral components of a search for mathematically optimal decisions. The expected utility function works well under certainty conditions. However, this function exhibits fatal weaknesses when used for conditions of uncertainty, as Ellsberg demonstrated with the Allais Paradox (1961).

The prospect function, developed by Kahnamen and Tversky (1979; 1992), offers greater functionality and realism to reflect the nature of decision making under uncertainty. This theory better accounts for how people make choices that do not align with the mathematical optimality that expected utility seeks. The prospect function supplants the expected utility function for decision making under uncertainty because of expected utility's shortcomings. These limitations include the Substitution Axiom, loss aversion, the ambiguity effect, and framing effects.

1. Substitution Axiom

The Substitution Axiom refers to well-defined preferences. It holds that two choices will retain their preference order when a third, irrelevant choice, is introduced. In

their adaptation of Allais' experiment, Kahneman and Tversky (1979) developed what is now known as the certainty effect, where people tend to overvalue a sure or a known probability, even though the probability is low, relative to outcomes that are merely probable. This phenomenon is evident in people purchasing lottery tickets but not insurance in flood-prone areas. The certainty effect also describes the situation in which winning a gamble is possible, but not probable. In this situation, when probabilities are low, most people will chose the gamble that offers a larger potential gain (Kahneman & Tversky, 1979; Ramirez & Levine, 2013).

2. Loss Aversion

Expected utility does not account for the decision maker's ability to accommodate loss aversion. Loss aversion describes how preferences for risk depend on a reference point, from which all losses and gains are evaluated. When using expected utility, risks and rewards are reduced to an absolute value without regard for preferences. Additionally, the expected utility model considers risk aversion and the concavity of the utility function as synonymous.

However, "prospect theory introduced the certainty effect, which refers to the decision maker's avoidance of risk" (Kahneman & Tversky, 1979; Ramirez & Levine, 2013; Tversky & Kahneman, 1992). The prospect function thus accounts for the fact that people do not process and evaluate outcomes equally; rather, they focus on the resulting or perceived gains or losses resulting from the pending outcome (Kahneman & Tversky, 1979; Ramirez & Levine, 2013; Tversky & Kahneman, 1992). When considering medium-sized risks, the expected utility model would need a large amount of curvature in the utility function, which would imply a complete aversion to larger risks. Because of this condition, a sigmoid or asymmetrical S-shaped curve is used in the prospect function, with the losses incurring a greater slope of decline than the gain's incline. See Figure 5 for an example of a sigmoid curve.

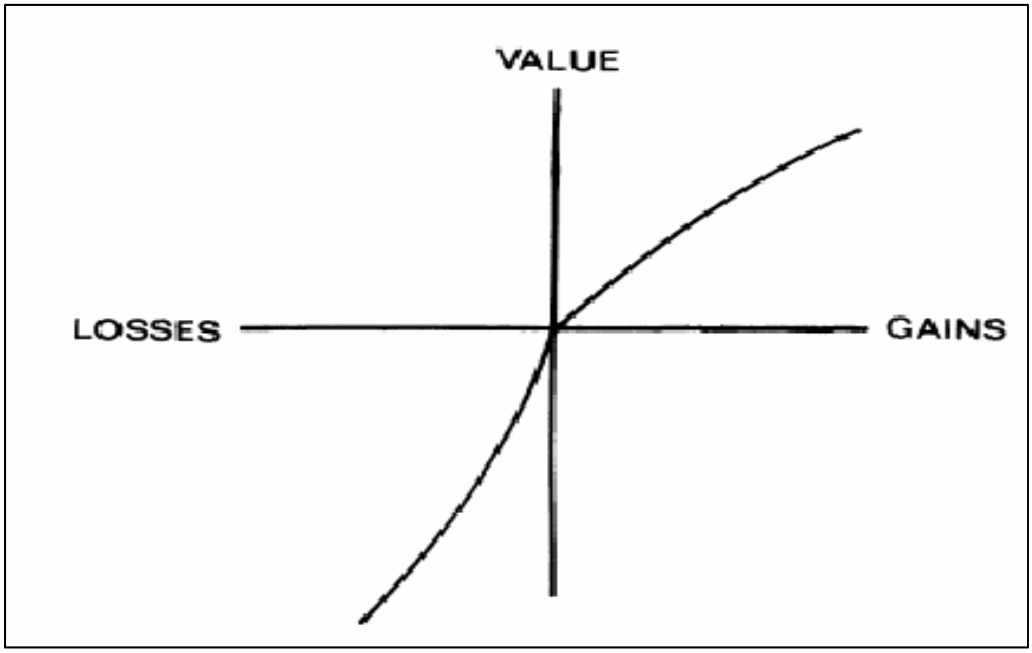


Figure 5. Example Sigmoid Curve of a Prospect Fuction. Source: Kahneman & Tversky (1979).

3. The Ambiguity Effect

Prospect theory also rises above expected utility when gauging ambiguity in a situation or in situations where probabilities cannot be assigned. Consider Ellsberg's 1961 dissertation experiment (Ellsberg, 1961; Levin, 2006; Tversky & Kahneman, 1992). Participants were given an urn with 300 balls; 100 were red, and the remaining 200 were a mix of white and blue. Participants randomly drew a ball under the following conditions:

1. You will receive $100 if you correctly guess the ball's color. Would you guess red or white?
2. You will receive $100 if you correctly guess a color different from that of the ball. Would you rather guess red or white?

Ellsberg demonstrated that people tend to pick the color red in both cases because the probability of drawing a red ball is known while the probability of drawing a white or blue ball is unknown. However, these results violate the utility model's assumption by showing that people often behave as if they know the likelihood of a given outcome.

4. Framing Effects

As discussed in Chapter IV, individuals may interpret information in multiple ways based on how that the information is framed. Previous research has demonstrated that when given multiple alternatives that have the same probability, but are presented as losses and gains with certainty, participants will choose the gain time and time again (Finucane et al., 2000; Kahneman & Tversky, 1979; Ramirez & Levine, 2013; Tversky & Kahneman, 1992). This effect violates the monotonicity axiom of expected value. Monotonicity is defined as the function of ordered sets that maintains the order. This violation is caused by the description of the outcomes, as a loss or gain, not by the probability of occurrence.

E. THE APPLICATION OF THE QUANTITATIVE DEFINITION OF RISK TO CYBER OPERATIONS

The quantitative definition of risk requires specific interpretation for use in cyber operations. First, commanders interpret risk in a negative sense—things that may go wrong—and wish to select a CoA that will avoid undesirable outcomes. Second, the objective hierarchy defines the commander's outcomes of concern. Third, the relevant sense of uncertainty relates to the values actually experienced, ex post, for these outcomes of concern. Commanders have little time to devote to solicitations and exercises for determining their $v(a)$ assessments.

Modeling of decision maker preferences in the context of cyber operations requires specific interpretations of the terms defined previously. The model of decision making under conditions of certainty that is used in this research provides the answers to Kaplan and Garrick's first and third questions. The answer to the second question follows from information provided by SMEs. The answer to the fourth question requires the prospect function because it is the most appropriate model for decision making under conditions of uncertainty.

1. Answering the First Question

The four questions directly relate to contemporary cyber operations. The first "What could happen?" becomes "What could go wrong?" and is used to identify the set

of initial events or circumstances. This first question can embody five different outcomes. "Wrong" can be interpreted as not causing enough damage to an adversary network or not gathering enough required intelligence. Wrong can also be interpreted as having a higher than tolerated likelihood for being detected, attribution of the operation, or compromise of other operations. Fault tree analysis is unnecessary. Risks are expressed directly in terms of unwanted outcomes for elements of the objectives hierarchy.

The answers to this question follow the issues of concern revealed in, and defined by, the objective hierarchy with consequences defined by the decision maker's preferences. See Figure 6 for the first level of the objective hierarchy used in this research.

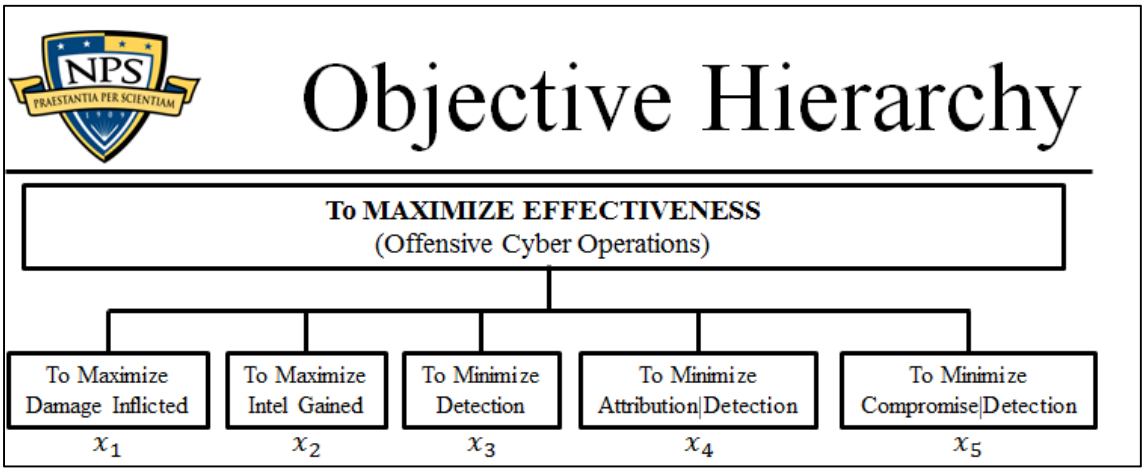


Figure 6. Top Level of Objective Hierarchy Illuminating the Decision Maker's Concerns

For the purposes of this research effort, the following definitions are used:

x_1 = The percentage of desired damage achieved.

x_2 = The percentage of desired intelligence obtained.

x_3 = The probability that the operation is detected.

x_4 = The probability that the operation will lead to attribution, given that the operation is detected.

x_5 = The probability that the operation will lead to compromise of friendly actors, given that the operation is detected.

Concerns within the hierarchy are given measurements or metrics $x_k(a)$. Hence, the answers to the first question follow from what is done in the first step of Chapter V, and the decision maker interprets the answers of this question in terms of $x_k(a)$, where x_k represents the undesirable values the commander wishes to avoid. The collection of concerns $x_k(a)$ combine into the vector $\mathbb{x}(a)$.

Objective hierarchies are constructed to ensure completeness, non-redundancy, decomposability, and operability (Kirkwood, 1997). Completeness means that for each level of the hierarchy, the evaluation considerations, when taken together, will cover all concerns adequately to evaluate the overall objective. Non-redundancy refers to how no two evaluation considerations within the same layer of the hierarchy should overlap. Decomposability requires each evaluation consideration to be expressed in its most basic elements. Lastly, operability refers to the ease by which the hierarchy is understood and relevant to the decision maker. The construction of the objective hierarchy for this research is discussed in the Chapter VII.

The decision maker answers the question "What can go wrong?" in terms of the x_k. For example,

x_1 = The percentage of damage accomplished is less than minimally acceptable; the adversary still has capable systems.

x_2 = The percentage of intelligence obtained is less than minimally acceptable; the decision maker is incapable of understanding the adversary's intentions.

x_3 = The probability that the operation will be detected is more than maximally acceptable.

x_4 = The probability that the operation will lead to attribution, given that the operation is detected, is more than maximally acceptable.

x_5 = The probability that the operation will lead to compromise of friendly actors, given that the operation is detected, is more than maximally acceptable.

2. Answering the Second Question

The second question "How likely is it to happen?" addresses the probabilistic nature of each x_k in the first question. Typically, analysis of historical data would provide objective measurements. SME opinion is elicited, however, due to the relatively new application of cyber operations below the national level, combined with the high classification and compartmentalization of cyber operations. As many SMEs as possible should be queried. "How likely is it to happen?" requires the probability of occurrence for the event defined in the first question, represented as $p(\mathbb{x}(a))$.

The realized values of the vector $\mathbb{x}(a)$ are never known *ex ante* to the decision maker under uncertainty. Information on the uncertainty should be obtained from SMEs in the form of confidence intervals that capture what the SMEs know and what the SMEs "know they do not know." These confidence intervals are extremely important as they provide information for the construction of probabilistic models for each $x_k(a)$ that more accurately mirrors the variability to expect in the outcomes.

3. Answering the Third Question

The third question "What are the consequences?" addresses the ramifications of each x_k, and the measure of overall effectiveness, $Y(\mathbb{x}(a))$, provides the answer. The individual value functions and tradeoff weights express such considerations. For example, a rapidly decreasing $v_3(x_3)$ as x_3 increases can result if the commander is concerned that detection would lead to a potentially damaging retaliatory cyber attack or political embarrassment for the nation, or reveal vulnerabilities in the adversary network. Likewise, a high tradeoff weight for $v_5(x_5)$ could be the result of a strong preference for avoiding any chance of compromising the related efforts of an ally.

4. Answering the Fourth Question

The fourth question "How do you feel about it?" addresses how the decision maker feels about the consequences described by

$$Z(a) = w_Y Y\big(\mathbb{x}(a)\big) + w_C v_C(C(a)),$$

given that the outcomes, $\mathbb{x}(a)$, are uncertain. Uncertainty induces a change in decision maker preferences. If the values of $Z(a)$ are known to be uncertain, then this function becomes the argument, or input variable, of a prospect function (Kahneman & Tversky, 1979; Tversky & Kahneman, 1992).

The prospect function has three components. First is the critical, or reference, value. The decision maker uses the critical value to distinguish gains from losses which is shown in Figure 5 using a vertical line at the point *Z*(a)* where the sigmoid curve crosses the horizontal axis. For our purposes, this axis represents the values taken by $Z(a)$. Second is loss aversion, illustrated in Figure 5 by the kink in the sigmoid curve as it crosses from the region of $Z(a)$ considered gains the region of $Z(a)$ considered losses. The slope of the curve at the origin of the loss region, as it extends to the left, is the loss aversion coefficient. It accounts for the fact that "losses loom larger than gains" in the mind of the decision maker (Kahneman & Tversky, 1979). Third is the prospect, which exhibits decreasing marginal values. This means the rate of increase in the value of the prospect decreases as we increase the amount of the gain. Likewise, the rate of decrease in the value of the prospect decreases as we increase the amount of the loss.

There are several functional forms for the prospect function (Cox, 2002), but the simplest is the exponential form:

$$v\big(Z(a)\big) = v(Z(a))^{+} - v(Z(a))^{-}$$

where

$$v(Z(a))^{+} = |Z(a) - Z^{*}|^{c} \; if Z(a) \geq Z^{*}$$

expresses the preference for gains and

$$v(Z(a))^{-} = \lambda |Z(a) - Z^{*}|^{d} \; if Z(a) < Z^{*}$$

expresses the preference for avoiding losses as indicated by the negative sign in the definition of $v(Z)^{*}$ signifies the critical, or reference, value. The loss aversion coefficient is $\lambda > 1$. Both exponents satisfy $0 < c < 1$ and $0 < d < 1$.

Kahneman and Tversky find that a decision maker can select a CoA that produces a maximum expected value by searching over the set of CoAs. The mathematical statement of this operation is

$$max_{a \in A} E\{v(a)\},$$

where *A* denotes the set of CoAs and *E* denotes expectation. The expectation is taken with respect to the probability distribution describing the uncertainty in *v(a)*.

Identifying this distribution and computing the expectation operation for each CoA, *a*, can represent a daunting theoretical exercise. It has a simple practical implementation, however, using simulation modeling. Recall the answers to the second question.

SMEs provide 90% confidence interval for the likely numerical values of each $x_k(a)$ using three points: (1) the SME most likely estimate, X_{ML}; (2) the 5% quantile, $X_{.05}$; and (3) the 95% quantile, $X_{.95}$. These three points permit the construction of a probability distribution function with statistics matching the SME estimates. SMEs with expertise in cost are solicited for similar 3-point estimates for construction of probability models for the *C(a)*. The research reported here uses the simplest such distribution: the truncated triangular as presented in Figure 7.

The simulation modeling approach to construction of the distribution function for v(a) is as follows:

1. Obtain S samples for each of the $x_k(a)$using their respective triangular distributions and S samples for each of the C(a) using their respective distributions.
2. Insert the S sample values, one set of $\{x_k(a); k = 1 \ldots N\}$ at a time, into the effectiveness function $Y(x(a))$ to obtain S samples values for effectiveness. Do likewise for the cost to obtain S samples of $x_C(C(a))$.
3. Combine these into S sample values for cost-effectiveness using
4. $Z(a) = w_Y * Y(\mathbb{x}(a)) + w_C v_C(C(a))$.
5. Compute the corresponding S values of $Z(a)$ to obtain S sample values of the prospect function, $v_s((Z(a))$ where the subscript *s* denotes the sample value.

6. Compute the expected value of the prospect function using the empirical distribution function arising from the sample:

$$E\{v(a)\} = \frac{1}{S}\sum_{s=1}^{S} v_s(a)$$

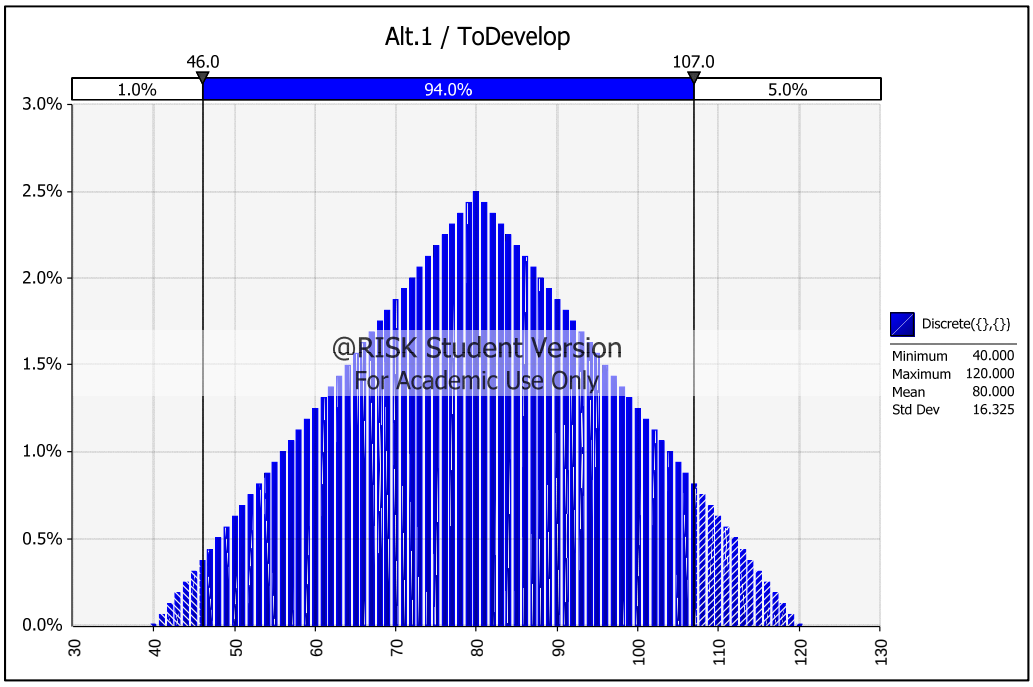


Figure 7. Example of SME Distribution of Costs

This is recognized as nothing more than the simple average of *S* data points randomly selected from the truncated triangular distribution as shown in Figure 7.

F. A PRACTICAL IMPLEMENTATION IN CYBER OPERATIONS

Commanders of cyber forces wish to choose CoAs that are the most effective while simultaneously requiring the least resources, thus, the optimal solution. This perfect solution is rarely, if ever, available. This means that commanders must tradeoff between effectiveness and cost to arrive at an optimal choice. The existence of uncertainties in the actual costs and effectiveness cloud these considerations and induce risk in the mind of the commander.

It is because of this risk that the commander seeks the counsel of SMEs. Typically, a commander will call SMEs together and solicit insights based on experience, knowledge, and intuition. This information results in subjective verbal statements, risk matrices, color coding, and other communications that exhibit bias, heuristics, group think and overconfidence or an overestimation of risk. Please refer to Chapter 4.

The commander now has a better approach. This dissertation provides a quantitative framework using graphics to circumvent the subjective cognitive limitations mentioned above. Chapter 5 illuminates the process of defining decision maker preferences with graphical value functions derived from mid-value splitting. See Figure 3. Figure 4 illustrates how the determination of tradeoff weights provides the weighting of the different individual objectives in relation to one another. See Figure 7's SME generated truncated triangular distribution for an example of the weighting of objectives by a commander. In this example, the decision maker places equal value on the maximization of inflicting damage and the minimization of attribution. All other hierarchy objectives are considered by the decision maker. In this example, these objectives are of no consequence to the decision maker and hence, their relative value is zero. See Figure 8.

This framework uses SME expertise to develop probability models representing their expectations and the uncertainty in this estimate. These models, in concert with simulation software and a model of decision maker preferences under certainty, result in a graphical representation of the uncertainties in the operational environment. This output takes the form of a scatter diagram with $Y(\mathbb{x}(a))$ on the vertical axis and $C(a)$ on the horizontal axis. See Figure 9.

This scatter diagram provides the observations for computing the expected prospect, $E\{v(a)\}$. This requires additional work however. The commander's prospect function parameters must be first elicited. Another way exists.

As described in the previous chapter, Kaplan and Garrick (Kaplan & Garrick, 1981; Wall, 2011) allowed the populace affected by the Hanford cleanup to interpret the data as they saw fit and then make decisions based on their own risk preferences. This

framework allows the commander to do the same based on the graphical outputs of the simulation. The commander is free to evaluate the information against the prospect function in his or her mind. This allows the commander to choose the alternative that maximizes the expected value of their prospect function—their personal evaluation of the expected gain versus the expected loss attributed to each alternative. Here, expected gain occurs when the effectiveness is greater than the minimum acceptable effectiveness and when the resource costs is less than what is maximally acceptable.

The commander may also elect to have the staff conduct an analysis of the simulations and recommend for decision a CoA that best meets predetermined criteria. These outputs then are presented by the staff to the commander as evidence supporting recommendations, as shown in Figure 8. From this evidence, the commander may choose a CoA or better refine his or her criteria of success if no CoA is acceptable. This graphical output allows the commander to assess the likelihood of risk described by the patterns of points in each of the four regions of each CoA. The next chapter discusses the composition and interpretation of the regions of the graph.

These simulation outputs consider the commander's desire to maximize effectiveness and to minimalize cost while illustrating the likelihood of not meeting the commander's criteria. The likelihood of not meeting the commander's criteria constitutes risk. The commander may emphasize different effectiveness objectives as he or she deems.

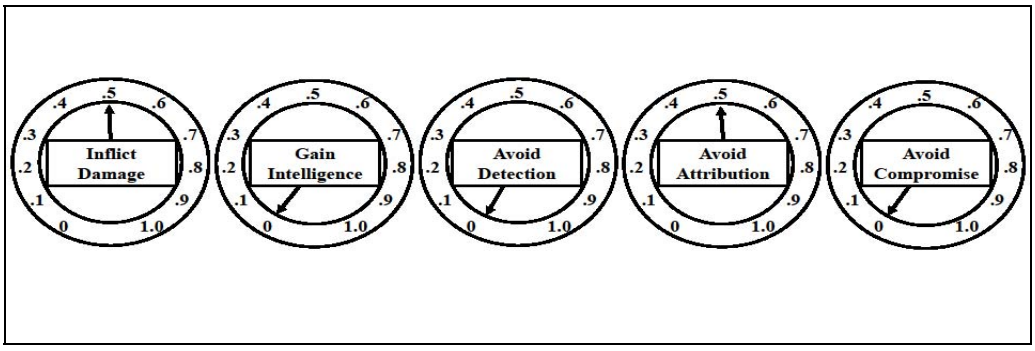


Figure 8. Dials for Adjusting for Decision Maker Weight

The framework presented in this research constructs a visual presentation of all relevant quantified information. This information is presented in the form of a two-dimensional graph and will be therefore be referred to as a graphical aid or depictions of graphical CoAs. This presentation allows the commander the ability to assess each CoA for their perceived value using the principles of quantitative risk assessment and management. This framework engages the commander to provide value statements of objectives and allows him or her to simultaneously view the relative quantitative risk measures for alternatives. The commander gains an understanding of the likelihood of success through pictures depicting the combination of values, risk, and uncertainty. This framework marginalizes the effects of the subjective cognitive limitations discussed in Chapter IV by using a quantitative definition of risk combined with mathematical simulation. This presentation forces the commander to consider all CoAs using quantitative risk management concepts, thus choosing the most effective CoA for the situation.

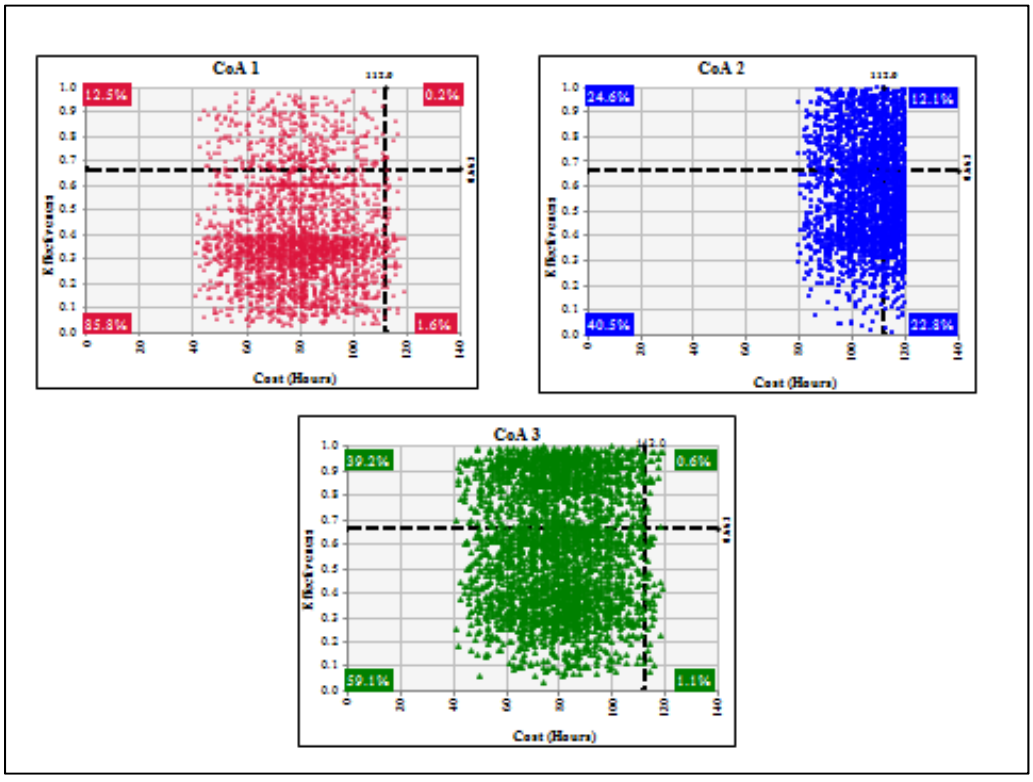


Figure 9. Example Graphical Outputs as Evidence in a Staff Recommendation

VII. METHODS

This research effort incorporated national level SME expertise and uncertainty to model assessments of reality for scenarios of offensive cyber operations within a 90% confidence interval. These assessments were then combined with estimations of cost and decision maker preferences and then converted into a graphical format. The written and graphical formats were presented to offensive cyber planner participants at the CCMDs to choose which would be the most feasible CoA for recommendation to the commander. These results were used to test the null hypothesis using Monte Carlo sampling. The null hypothesis for this research is *No significant change occurs between the written and graphical CoA rank choices for each scenario.*

A. DESIGN

This research endeavor incorporated a correlational design to measure whether a graphical depiction of risk, measured in terms of cost and effectiveness, is preferred and more suitable for decision making than a written format. Information used in this experiment came from elicitations of effectiveness from SMEs working at the national level of cyber operations. These elicitations encompass what each SME considered to be a 90% confidence interval. These SME elicitations then were used to mathematically model alternatives using a simulation engine. This simulation engine also incorporated decision maker weights of values to analyze the tradeoffs of alternative CoAs. The final output was a graphical display that indicated the likelihood of attaining the decision maker's preferences. The results of this experiment then were analyzed using a Monte Carlo technique, or repeated random sampling of computational permutations for an exact p value calculation.

B. RESEARCH QUESTION AND HYPOTHESIS

This research effort attempted to answer the research question: How effective is a simulation framework incorporating both subject matter expertise and assessments of uncertainty at overcoming the inexperience of decision makers in assessing risk and subsequent decision making within new operations? This dissertation advanced the

hypothesis that a framework built on SME knowledge and expertise that incorporated the uncertainty that SMEs acknowledge allowed decision makers to make more informed assessments of risk, and consequently, better decisions regarding unfamiliar and new operations within their organizations.

This effort proposed creating a framework that gives organizations a comprehensive picture to better understand risks in order to facilitate command and control decisions. This proposed framework used multi-objective optimization to account for the multiple factors considered when assessing risk for offensive cyber operations (Keeney & Raiffa, 1976). The proposed framework modified an existing risk assessment framework to incorporate the acknowledged uncertainty of the subject matter experts. Notably, quantitative frameworks have not yet been applied to cyber operations.

C. PARTICIPANTS AND SETTINGS

This study included two types of participants: SMEs and cyber planners at the combatant commands headquarters. SMEs were sought in Phase 1 to record their expertise and uncertainty for mathematical modeling of the framework. Once complete, offensive cyber planners at CCMD headquarters were recruited for Phase 2 to assess the effectiveness of the framework.

1. Subject Matter Experts

In Phase 1 of the research, SMEs provided estimates of risk and uncertainty. SMEs for this research had at least five years of national level cyber experience in planning, conducting operations, or analyzing information from within foreign networks. Warrant officers were predominantly sought for this research. The rationale for this decision was that these warrant officers were often enlisted service members who served as analysts or operators with cyber operations. Having transitioned to become warrant officers, these individuals then returned to these organizations and continued to build on their experience. Unlike commissioned officers, warrant officers typically do not move from an operational assignment to a broadening assignment meant to give more breadth

of experience. Therefore, warrant officers typically exhibit a deeper knowledge and experience base to draw from for this research.

Four civilians were recruited as SMEs. Three of these individuals left active duty Army within the last year. One retired while one chose to leave the military. The third civilian SME retired from the active duty Army in 2014 and was then hired in the same capacity by his Army organization. The fourth SME left active duty in 2009 and was hired by the Army in the same role. This fourth SME left government employment for the private sector within the last year. The rest of the SMEs were active duty military. Five were currently or formerly enlisted service members, twenty were warrant officers, and five were commissioned officers. Experts were nominated by their leadership based on the experts' experiences, in-depth knowledge, and perceived ability to accurately assess risks in operations. Demographics indicated that the SMEs chosen had a range of three to eighteen years' experience with an average of 8.3. See Appendix B for all the SME demographics.

SME elicitations occurred at Fort Meade, Maryland, and at Fort Gordon, Georgia. Both locations house portions of the National Security Agency along with military units conducting cyber operations for their military services. Fort Meade also contains the Cyber National Mission Force (CNMF). The CNMF is a joint military organization that conducts offensive and defensive operations that support national level objectives, as defined by the President. Additionally, Fort Gordon also houses the Army component for cyber operations in support of combatant commands along with the Cyber Warrant Officer Advanced Course. Participating SMEs either currently worked in these organizations or departed these organizations within the last year. SMEs were recruited from national level cyber organizations through the use of intermediaries still in these organizations who previously worked with the author.

2. Scenarios

SME participants were given six scenarios: three focused on CNE and three focused on OCO. Scenarios were designed to simulate one of three categories of adversary: Peer-Nation, Developed Nation, and 3rd World Nation/ Non-State Actor. For

the sake of classification, real nation-states were not used; however, the Islamic State terrorist group was used as a non-state actor in two scenarios. To prevent the inadvertent disclosure of classified capability names, scenario capability names were screened to verify that these names were not in use for operations by an associate working in the National Security Agency. Scenarios were designed to communicate the decision maker tradeoffs. For the SME elicitation, the decision maker value weights were removed. SMEs were instructed to evaluate the likelihood of achieving the objectives of each scenario independently without regard for the potential interplay between the objectives. Additionally, this author sought the SME insights and estimates of success regardless of the decision maker preferences. For the 30 SMEs used in this elicitation, their assessments of the goals were aggregated together into one graphic output for each CoA. Each graphic output consisted of 3,000 rounds of the simulation to provide an accurate assessment of variability.

Scenario 1 consisted of two parts, 1A and 1B, to simulate an escalation of activities. Scenario 1A presents a situation in which a CNE action is ordered to confirm an adversary's hostile intentions against a neighboring U.S. ally. Scenario 1B continued with an escalation of force to an OCO operation in order to dissuade the targeted nation from continuing hostilities on the U.S. ally.

Scenario 2 simulated an operation against the Islamic State by a CCMD in conjunction with the Theater Special Operations Command (TSOC) after the capture and killing of a U.S. service member. The killing of the service member was then recorded for an online propaganda video. In this scenario, the commander sought confirmation of the identity of the people responsible for the service member. The goals of this CNE operation were to gather intelligence to confirm the identities of the five targeted people while avoiding detection so that the adversary does not change routines and procedures.

Scenario 3 introduced a peer-level nation that has used government-backed civilian companies to hack into and steal documents from a CCMD network. These documents are part of the upcoming Theater Security Plan Agreement, which outlines personnel and equipment movements within an allied nation. The goals of this CNE

operation were to retrieve documents from the adversary as proof of the transgression while not being detected.

Scenario 4 reintroduced the Islamic State. This time, the terrorist organization was in the process of publishing an online magazine, Inspire. In the upcoming issue, the editors urged a call to arms for jihad after a recent killing of a U.S. service member and provided a new technique for bomb making. The goal of the operation was to prevent dissemination of the magazine while simultaneously assisting in the identification of online readers.

Scenario 5 introduced a developed nation that is not a technological peer to the United States. This country also used state-sponsored civilian companies for misattribution of activities. The adversarial nation in this scenario has infected both U.S. and an allied nation's networks. The goal of this attack operation was threefold: destruction of adversarial infrastructure while avoiding detection and attribution. See Appendix C for the table of scenario distribution.

3. Combatant Command Cyber Planners

In Phase 2 of the research, CCMD cyber planners were nominated by the leadership of each command and subsequently recruited for participation. For this experiment, 31 planners were military, while 29 were civilian. Of this sample of planners, 31 had worked at the national level. The range of national level experience was one year to 35 years with an average of 2.74 years. Only 14 people within the participants had attended any of the courses specifically used to teach cyber operations or their planning. These courses target a wide range of audiences, from planners nominating the targets and operations, to software developers writing code, to operators exploiting networks and analysts looking for intelligence value in the operations. These demographics do not include the planners at USCYBERCOM even though select later analysis will. Appendix G contains the participant demographics.

Specifically to USCYBERCOM planners, seven were military, while seven were civilian. The range of national level experience was one year to 11 years with an average of 3.78 years. Only six people within the participants had attended any of the courses

specifically used to teach cyber operations or their planning. Later analysis of the group will be conducted both with and without the planners at the other commands and the sample of planners with national level experience.

The planning teams at combatant command headquarters were desired for their lack of experience within cyber operations and to reflect the environment if the capacity to conduct cyber operations is delegated. CCMD planning team members typically consist of five to seven people. These people were promotable O3s to O5s, or civilian GS personnel. The purpose for this design consideration is a greater understanding of the impact of the framework on inexperienced personnel.

The order of participation of the combatant commands was as follows: Special Operations Command (USSOCOM), Central Command (USCENTCOM), Southern Command (USSOUTHCOM), European Command (USEUCOM), Africa Command (USAFRICOM), Northern Command (USNORTHCOM), and Pacific Command (USPACOM). After the combatant commands, national level operational planning teams (OPTs) at U.S. Cyber Command (USCYBERCOM) were used as an experimental control. These teams were used as a control because they have more experience and access to more intelligence sources to aid in their education and expertise for understanding an adversary. Additionally, these teams were screened to ensure that none of the experts whose opinions have already been elicited were now members of the OPTs.

D. INSTRUMENTATION

This section discusses the assessment process to determine if SMEs and CCMD planners were risk seeking or risk averse. Next discussed are the creation of hierarchies for this research. The measures of Effectiveness and Cost are discussed along with how they were mathematically modeled. Next, this section reviews the assessment and modeling of the decision maker values, with their associated weights. Lastly, the graphical output that culminates from the modeling of the above inputs is introduced and explained.

1. Risk Attitude Assessment

SMEs and CCMD planners were supplied with a packet that included the IRB Informed Consent paperwork and a risk attitude assessment. The risk attitude assessment given is the Domain-Specific Risk-Taking (DOSPERT) scale for adult populations modified by Blais and Weber (Blais & Weber, 2006). This assessment used three iterations of 30 one-sentence situations for three different measurements. In the first of three iterations, the 30 questions used determine the likelihood that a participant would engage in the given situation. In the next iteration, the same 30 questions are presented to determine the risk perception that a participant had in the given scenarios. In the third and last iteration, participants evaluated and recorded the anticipated benefits from the questions presented. All iterations are measured using a seven-point Likert scale. The 30 questions are divided into five categories: Ethical, Financial, Health/ Safety, Social, and Recreational. In this evaluation, positive scores indicate a risk-seeking attitude. Negative scores indicate participants are risk averse. Within positive or negative scores, the higher score is more risk seeking. See Appendix E for a sample of the DOSPERT risk assessments. The results of the DOSPERT will be discussed later in the Data Analysis chapter.

2. Objective Hierarchy Construction

In the study, an objective hierarchy was constructed using evaluation criteria obtained from an analysis of offensive cyber operations. This hierarchy was then deconstructed ensuring completeness, non-redundancy, independence, and operability using a top-down approach (Kirkwood, 1997). The hierarchy designed for this experiment sought to balance the effectiveness of cyber operations against the costs of these operations. Effectiveness was measured in five categories: Damage Inflicted, Intelligence Gained, Detection of Friendly Forces, Attribution given Detection, and Compromise given Detection. These Effectiveness measures are tradeoffs against the Costs of cyber operations.

Costs manifested into Personnel, Equipment, Infrastructure, and Time. Personnel, Equipment, and Infrastructure Costs are monetized costs that have great variance between

locations. Additionally, when discussing cyber operations, these costs are typically classified to prevent disclosure of friendly capabilities and capacity. For the purposes of this research, Time is non-monetized (Bell, 1982) and is measured as an eight-hour work day, occurring seven days a week. For simplicity, the pause of work for weekends does not occur. Figure 9 through Figure 13 illuminate the objectives and sub-objectives that, when taken together, construct the goal of "Maximizing Effectiveness." Figure 17 illuminates the aspects of the "Cost" aspects of the proposed framework. Since natural scales for this research do not exist, scales were constructed following the methodology prescribed in Kirkwood (1997).

3. Effectiveness

Effectiveness was measured in five categories: Damage Inflicted, Intelligence Gained, Detection of Friendly Forces, Attribution given Detection, and Compromise given Detection. Figure 10 illustrates the objective hierarchy for maximizing the damage inflicted in a computer network attack. Maximizing Damage included maximizing disruption, destruction, degradation, or manipulation of information systems, or resident information. These effects are part of the doctrine currently used in cyber operations (Department of Defense, 2013). Damage is measured as a percentage of the total goal of the operation. For the elements of Maximizing Damage, disruption is the complete but temporary loss of access to or operation of a resource for a specified period of time. Destruction is a permanent and irreparable denial to an operation or resource. Degradation is the diminishment of access to an operation or resource. Manipulation is to control or change information, information systems, or networks.

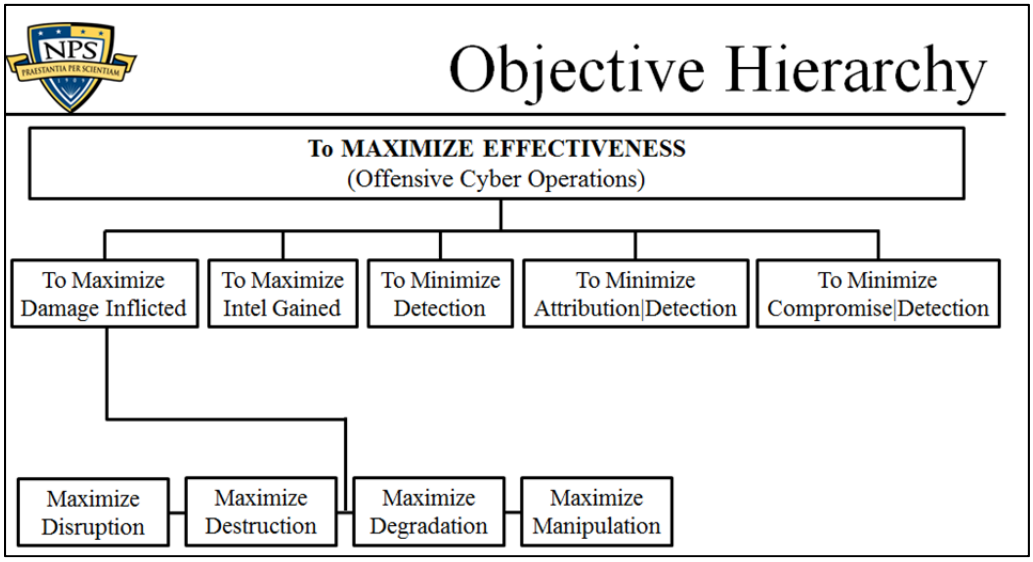


Figure 10. Maximizing Damage Hierarchy

Figure 11 illustrates the hierarchy for maximizing the intelligence gained regarding an adversary. Maximizing Intelligence implied maximizing the amount of discovered and/or potentially retrieved information. Moving to the next level is the sub-goal of Maximizing the Range of Targets. This is accomplished at the next lower level by using alternatives spanning the many hardware and software configurations and using alternatives that have been tested in virtual environments. The last, and lowest level of this hierarchy, ensured capabilities evade security products and minimized the use of zero-day capabilities. Intelligence is measured as a percentage of the total goal of the operation. Maximizing the range of potential targets, reduced the number of capabilities needed for operations. As an example, as of September 2016, Windows operating systems controlled 90.52% of the devices that connected to the Internet. This overshadowed the 7.37% for Mac systems and 2.11% for Linux systems (Netmarketshare, 2016). To achieve this goal, capabilities must maximize the number of hardware (HW) and software (SW) systems for which the capability is compatible. This compatibility is accomplished using modeling of the target adversary environment. Descending another level, modeling also accounted for PSP characteristics and vulnerabilities if known and able to be modeled. The modeling of the adversary's network also provides an opportunity to research the effects of a zero-day. The use of

zero-day capabilities must be minimized. This requirement has two rationales. First, the use of a zero-day is attributable to a sophisticated actor, most likely a nation-state. Secondly, the use of a zero-day should occur only when no other option is available for a sophisticated adversary (Axelrod & Iliev, 2014).

Figure 12 illustrates the hierarchy associated with the risks encountered for detection of a friendly operation or capability. Minimizing Detection is defined as minimizing the likelihood of being discovered by administrators or security products, or any capability incompatibility that could cause the target to malfunction. Detection is measured in terms of the percentage of the likelihood of being discovered.

Minimizing Attribution given that Detection occurs implied minimizing the likelihood of attribution of friendly actors and their cyber operations infrastructure, as well as possible retaliatory actions. Attribution is measured in terms of the percentage of the likelihood of being detected and the operation being attributed to the conducting organization. See Figure 13.

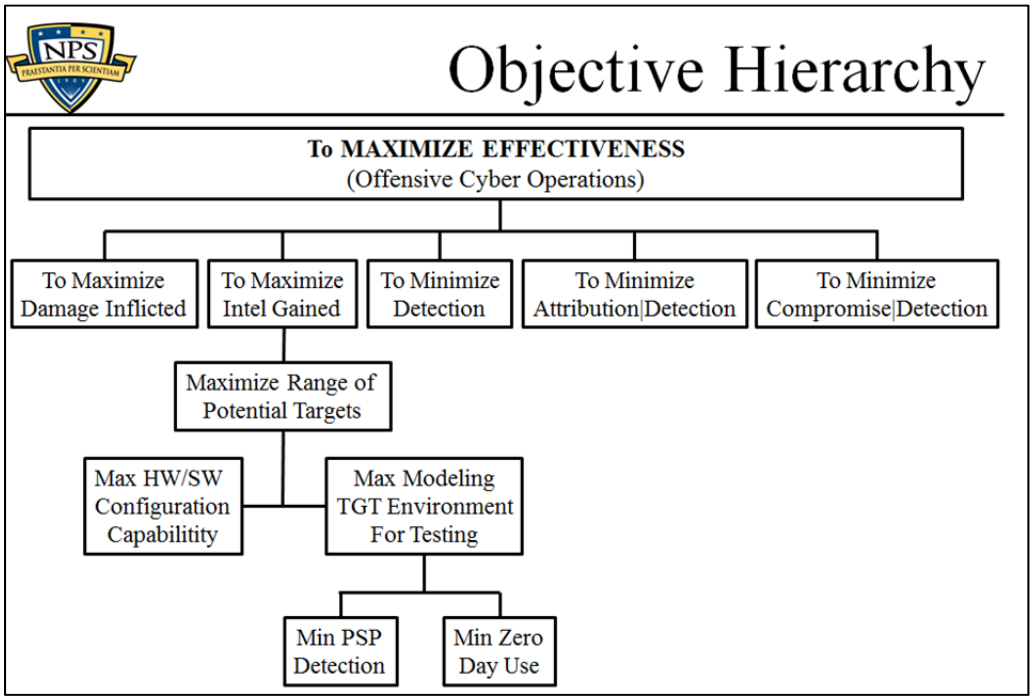


Figure 11. Maximizing Intelligence Hierarchy

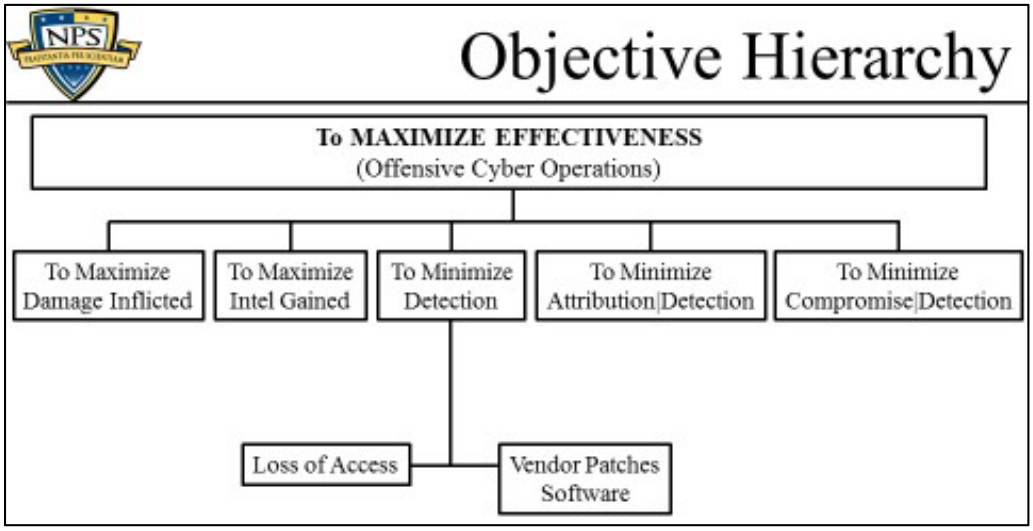


Figure 12. Minimizing Detection Hierarchy

Minimizing Compromise given Detection implied minimizing the likelihood of detection of this cyber operation, which may lead to implication of other operations in the target space or detection of friendly actors. Compromise is measured in terms of the percentage of the likelihood of being detected and the operation being compromised. See Figure 14.

An analysis of the objective hierarchy was undertaken to determine if value dependence existed between objectives. When implementing the SME values in the simulation, the probabilities of Damage Inflicted, Intelligence Gained, and Avoiding Detection are considered value independent, as one is not required to predicate the invocation of another. However, the measures for the probability of Attribution and the probability of Compromise are value dependent upon the probability of Detection. Therefore, this research uses conditional probabilities: the probability of Attribution given Detection and the probability of Compromise given Detection. This makes the value independence of the three probabilities justified.

4. SME Elicitation

The instructions for expertise elicitation stated that, for each goal of the scenario, the SMEs were to provide a 90% confidence interval of likely values. Three points were

solicited for each goal: most likely value, an upper value, and a lower value. The three values would then, in the mind of the SME, represent the values likely to be expected 90% of the time in the real world. The range provided by the Upper and Lower Values thus constitute the 90% confidence interval. SMEs used their own internal estimation to obtain information concerning the amount of uncertainty they believe is inherent in an outcome measure for each CoA. This is required to take the form of a quantile triple:

$$\{x_k(a)^{0.05}, x_k(a)^{ML}, x_k(a)^{0.95}$$

where

$$P\{x_k(a) \leq x_k(a)^{0.05}\} = 0.05$$

for the lower level value with

$$P\{x_k(a) \geq x_k(a)^{0.95}\} = 0.05$$

for the upper level value and $x_k(a)^{ML}$ is the value the SME believes is most likely to occur; for all $x_k^{min} \leq x \leq x_k^{max}$ we have $x_k(a)^{ML} = \max p(x_k(a))$ where $\mathrm{p}(x_k(a))$ is the conditions in the probability density function for the $\left(x_k(a)\right)$.

Two examples of elicitation were provided to the SMEs. The first example illustrated high confidence in the SME values as the range was relatively narrow. The second example illustrated less confidence in the SME-provided values as the range was significantly wider. See Appendix F for the SME elicitation packet and Appendix D for the SME elicitation scores. Figure 15 provides an example of an elicitation with less uncertainty. Figure 16 provides an example of an elicitation with more uncertainty.

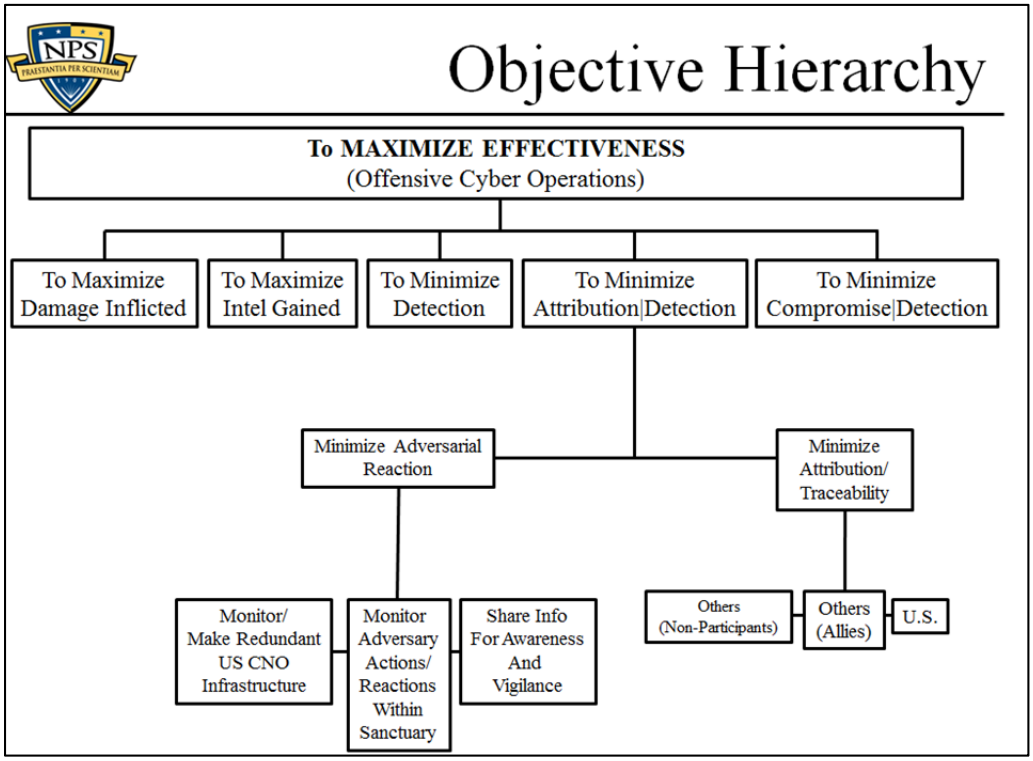


Figure 13. Minimizing Attribution Given Detection Hierarchy

5. Modeling Effectiveness

The SME elicitations of success were entered into an Excel spreadsheet. See Figure 17 for an example. Elicitations were categorized for each scenario based on the desired objectives of the commander. Monte Carlo sampling was then used to randomly select SME elicitations of success and use these estimates for the simulation. For each iteration of the simulation, a SME would randomly be selected and that individual's elicitations for all objectives of the scenario would be used for all CoA. The SME elicitations became the Effectiveness measure of the framework.

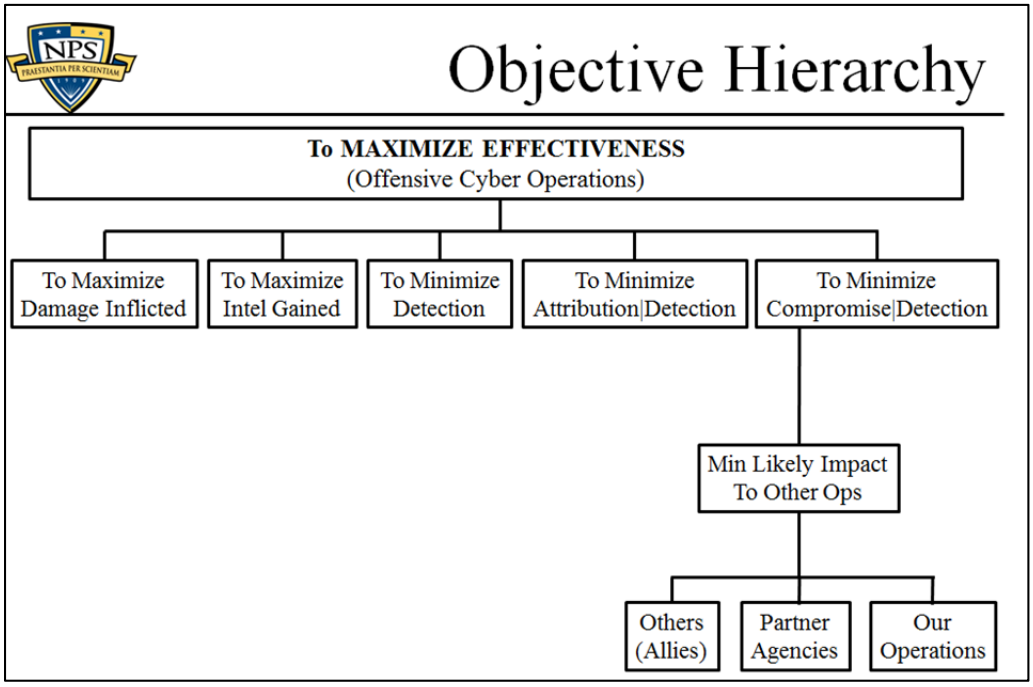


Figure 14. Minimizing Compromise Given Detection Hierarchy

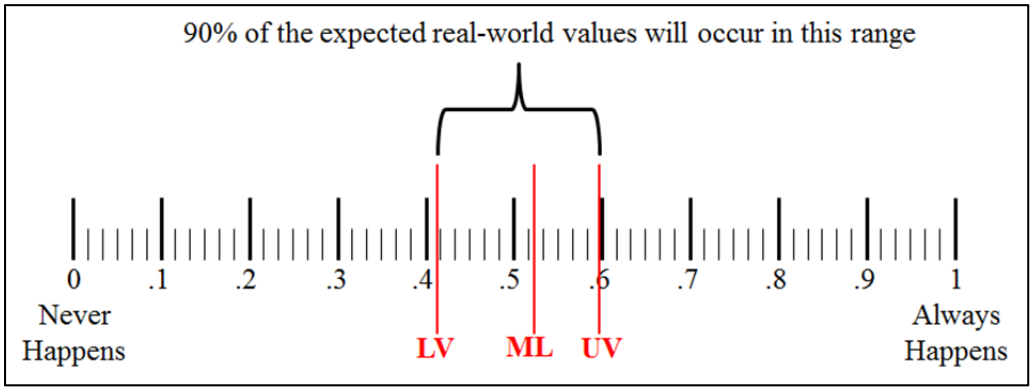


Figure 15. Example of an Elicitation with Less Uncertainty

SME expertise and operational costs were modeled using the Palisade @Risk software. This software is commercial modeling software that plugs into Microsoft Excel. SME values for each measure of effectiveness were entered for each scenario. The simulation then used a Monte Carlo process to randomly select a set of SME values to implement for each iteration of the simulation for a given scenario. A selected SME thus

provides all the effectiveness measurements of CoAs for that particular scenario in that particular iteration. Each graphical output presented to the participants resulted from 3,000 simulation iterations. Graphical outputs containing more than 3,000 iterations lacked the ability to discern individual iterations and appeared as one solid cloud mass. Graphical outputs will be discussed in depth later in this chapter.

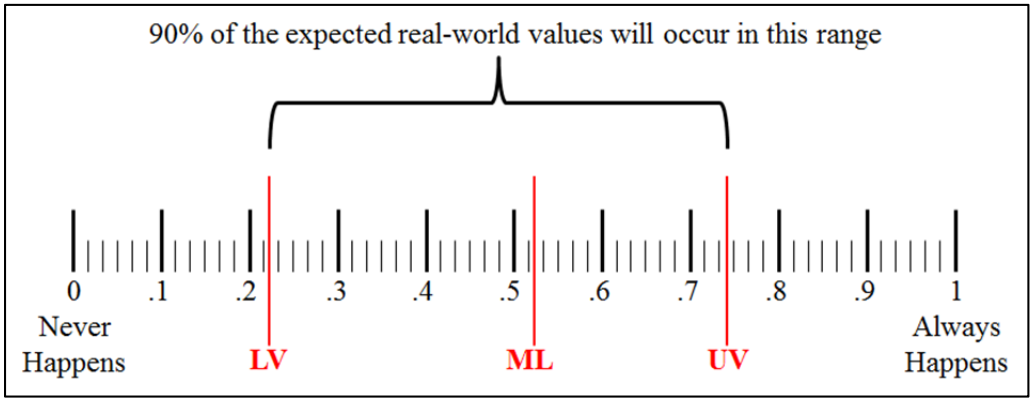


Figure 16. Example of an Elicitation with More Uncertainty

	SCENARIO 1A																	
	COA 1						COA 2						COA 3					
	INTELLIGENCE			DETECTED			INTELLIGENCE			DETECTED			INTELLIGENCE			DETECTED		
SME NUMBER	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV
SM001	0.200	0.500	0.700	0.600	0.700	0.800	0.200	0.300	0.400	0.400	0.500	0.800	0.700	0.800	0.900	0.600	0.800	0.900
SM002	0.000	0.250	0.300	0.500	0.800	0.900	0.350	0.660	0.850	0.250	0.330	0.850	0.000	0.050	0.200	0.750	0.920	1.000
SM003	0.410	0.540	0.700	0.500	0.600	0.700	0.400	0.500	0.650	0.350	0.530	0.700	0.300	0.430	0.600	0.300	0.440	0.630
SM004	0.300	0.400	0.500	0.420	0.500	0.700	0.200	0.300	0.400	0.300	0.400	0.500	0.420	0.500	0.620	0.200	0.300	0.400
SM007	0.700	0.900	1.000	0.500	0.730	1.000	0.700	0.900	1.000	0.100	0.200	0.300	0.700	0.900	1.000	0.850	0.900	1.000
SM009	0.230	0.530	0.730	0.480	0.580	0.680	0.350	0.650	0.725	0.250	0.380	0.450	0.350	0.450	0.560	0.550	0.680	0.720
SM010	0.750	0.800	0.850	0.400	0.500	0.700	0.670	0.700	0.730	0.050	0.100	0.200	0.760	0.800	0.900	0.650	0.750	0.860
SM011	0.250	0.300	0.500	0.500	0.750	0.900	0.500	0.600	0.900	0.100	0.200	0.400	0.000	0.250	0.500	0.500	0.750	1.000
SM012	0.500	0.900	1.000	0.500	0.550	0.700	0.300	0.400	0.450	0.500	0.600	0.700	0.600	0.700	0.800	0.200	0.300	0.350
SM013	0.100	0.600	0.800	0.200	0.400	0.900	0.100	0.300	0.500	0.100	0.400	0.600	0.100	0.400	0.700	0.100	0.400	0.700
SM014	0.500	0.750	0.850	0.400	0.500	0.750	0.300	0.400	0.700	0.050	0.200	0.250	0.700	0.800	0.950	0.500	0.800	0.950
SM016	0.700	0.750	0.950	0.500	0.700	0.750	0.700	0.750	0.950	0.100	0.200	0.210	0.700	0.750	0.950	0.700	0.750	0.990
SM017	0.750	0.800	0.900	0.250	0.350	0.400	0.800	0.850	0.950	0.000	0.150	0.200	0.800	0.850	0.950	0.150	0.400	0.410
SM018	0.000	0.200	0.500	0.400	0.600	1.000	0.400	0.600	1.000	0.000	0.200	0.400	0.300	0.500	1.000	0.400	0.700	1.000
SM019	0.000	0.250	0.500	0.650	0.820	1.000	0.750	0.000	1.000	0.010	0.050	0.250	0.000	0.250	0.400	0.650	0.800	0.900
SM020	0.250	0.500	0.750	0.300	0.500	0.850	0.500	0.700	0.800	0.100	0.200	0.300	0.800	0.850	0.900	0.800	0.900	1.000
SM022	0.300	0.400	0.550	0.500	0.700	0.800	0.600	0.700	0.800	0.200	0.300	0.500	0.600	0.700	0.850	0.750	0.800	0.850
SM024	0.300	0.500	0.600	0.300	0.500	0.600	0.200	0.300	0.400	0.350	0.400	0.450	0.600	0.700	0.900	0.400	0.500	0.600
SM026	0.250	0.350	0.480	0.700	0.800	0.900	0.600	0.700	0.800	0.300	0.400	0.500	0.800	0.900	0.950	0.100	0.200	0.300
SM028	0.600	0.700	0.900	0.400	0.500	0.600	0.700	0.800	1.000	0.200	0.300	0.500	0.500	0.700	0.800	0.600	0.800	0.900
SM029	0.450	0.650	0.850	0.200	0.600	0.900	0.250	0.500	0.700	0.150	0.400	0.550	0.500	0.800	0.950	0.550	0.750	0.950
SM030	0.330	0.420	0.500	0.620	0.700	0.750	0.230	0.300	0.320	0.400	0.510	0.600	0.540	0.620	0.650	0.310	0.330	0.400
SM032	0.700	0.800	0.900	0.400	0.500	0.600	0.800	0.900	1.000	0.200	0.300	0.400	0.800	0.900	1.000	0.400	0.500	0.600
SM033	0.400	0.500	0.800	0.300	0.500	0.700	0.200	0.300	0.500	0.000	0.100	0.200	0.600	0.750	0.900	0.700	0.900	1.000
SM035	0.800	0.900	1.000	0.300	0.400	0.600	0.300	0.500	0.700	0.300	0.500	0.700	0.700	0.800	1.000	0.500	0.700	0.900
SM036	0.400	0.700	0.800	0.520	0.550	0.570	0.600	0.700	0.800	0.100	0.300	0.500	0.700	0.800	0.900	0.600	0.700	0.800
SM037	0.300	0.400	0.700	0.600	0.800	0.900	0.600	0.700	0.800	0.200	0.300	0.500	0.500	0.700	0.800	0.600	0.700	0.800
SM038	0.500	0.700	0.800	0.500	0.650	0.800	0.400	0.500	0.600	0.200	0.340	0.430	0.600	0.700	0.800	0.700	0.800	0.900
SM040	0.100	0.250	0.300	0.750	0.850	1.000	0.750	0.850	0.950	0.000	0.200	0.500	0.000	0.250	0.300	0.750	0.900	1.000
SM042	0.500	0.620	0.780	0.400	0.800	0.850	0.200	0.500	0.800	0.150	0.500	0.600	0.500	0.620	0.900	0.100	0.600	0.900

Figure 17. Example Table of SME Elicitations for a Given Scenario

Using the three SME values for each measure of effectiveness, the simulation then applied a probability distribution. The lower, most likely, and upper values for a measure of effectiveness form the probability distribution for a course of action within a scenario. All SME data for each course of action then formed the 90% confidence interval for the course of action distribution. All effectiveness probability distributions were truncated to prevent values exceeding the limits of 0 and 1. These effectiveness values were then weighed against the decision maker's tradeoff weights as provided in the scenario and the decision maker's minimum overall effectiveness as designated by the researcher. The method for modeling the decision maker weighted values is discussed later within this chapter.

6. Cost

Figure 18 illuminates the Cost aspect of the proposed framework using a one-level hierarchy. Budgetary Costs include Personnel, Equipment, and Infrastructure Costs. Non-budgetary Costs for this research included Time. Personnel Costs included labor costs associated with the creation of a capability such as task and priority management or time needed to create or modify a capability, automation of resources, the use of virtualized testing, and continuing education for personnel. Personnel Costs are measured in dollars or labor hours. For this research, the only cost involved was the time to create or modify a capability. This choice of expenses is due to the wide range of salaries of software programmers, the varied costs of individual equipment and licenses, and the classified costs of the infrastructure currently used in cyber operations.

Equipment Costs included distributed resources available for more than one individual. Equipment Costs entailed the associated costs of the hardware and software required for creating the software capabilities and modeling the adversary networks and PSPs. Such resources are required for creating the software capabilities and modeling the adversary networks and PSPs. These resources included shared software repositories, virtualized environments for localized software testing, common use of development platforms, etc. This portion of the hierarchy does not include the initial costs of purchasing

equipment, only purchases specifically for this operation. An example is the purchase of a new PSP to incorporate into the modeling. Equipment Costs are measured in dollars.

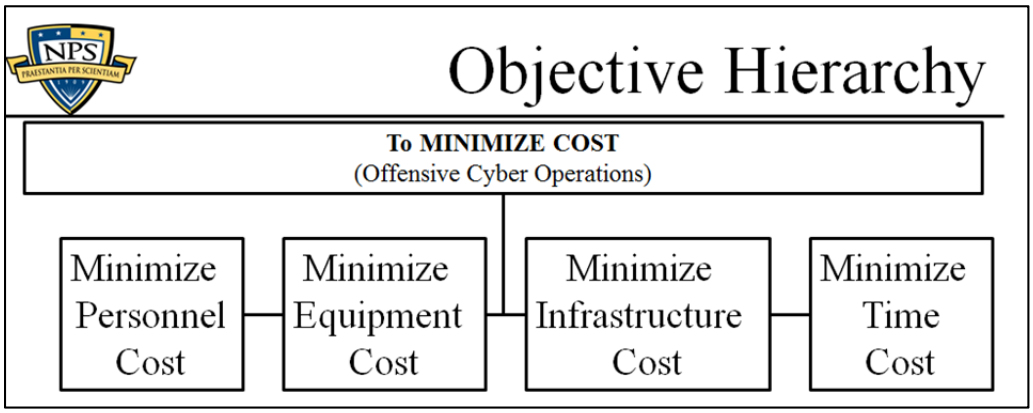


Figure 18. Minimizing Cost Hierarchy

Infrastructure Costs included technical actions taken to protect the cyber operations infrastructure from attribution, including the eventual replacement of infrastructure for redundancy or because of attribution. Infrastructure Costs are measured in dollars. This portion of the hierarchy does not include the initial costs of purchasing equipment used in the construction of the infrastructure, only purchases specifically for this operation. Infrastructure Costs are measured in dollars.

Time Costs are the last element of the hierarchy. Although time may be monetized for the purposes of arriving at an incurred cost, such as labor rates, this approach uses a non-monetized definition. In this research, Time Costs are viewed as the length, in days, for a capability to be prepared before an operation commences. In the specific scenarios provided to the Phase 2 participants, the commander gave an operation commencement deadline and an overview of the rationale behind this timeline. This deadline then became the maximum cost to be incurred for this operation within the simulation. Research participants weighed the perceived effectiveness of a capability against the time needed to prepare the capability for the given operation.

Non-Monetized costs are captured within each course of action via statements such as “This capability can be configured and tested for this specific operation in between one

and three weeks with a most likely completion at two weeks." From this information, the simulation randomly selected the number of days required for the capability modifications. That selection is then compared against the commander's constraint.

7. Modeling Costs

Costs of a CoA were modeled using a distribution created by *p* and *x* tables in @Risk. *P* tables represent the probability of occurrence. *X* tables represent the development time needed for the software capability, in accordance with the scenario. Each CoA contained statements such as "This capability can be configured and tested for this specific operation in between one and three weeks with a most likely completion at two weeks." Another potential statement was "This capability can be configured and tested for this specific operation in between one and two weeks with a most likely completion at two weeks." Each CoA had its own development time associated. This timeline information then formed a triangular distribution with the most likely being the highest probability of occurrence. Costs in the simulation were measured in hours while the scenario stated times in days or weeks. In the simulation, all measurement was converted to eight-hour periods. These statements of time needed formed the *x* table for the Cost of the capability used in the framework. See Figure 19 for an example of a distribution modeled for the Cost of an alternative.

The mathematical modeling of the SME elicitations of success, the costs of a CoA, and the weights of the values of the decision maker were then used by the simulation to create a graphical output of the CoA. The decision maker value weights and a more in-depth discussion of the graphical output of CoAs will be discussed later in the chapter.

All Cost distributions used both p tables and x tables to mathematically define the distributions to reflect the constraints of the scenario costs. Costs within the simulation were measured in hours of time to configure, modify, or create a capability for use in a particular operation. Within the scenarios provided to participants, time is measured in days for ease of conceptualizing. Days are considered to be an eight-hour day of software development. Work days are continuous and do not suffer from weekend interruptions.

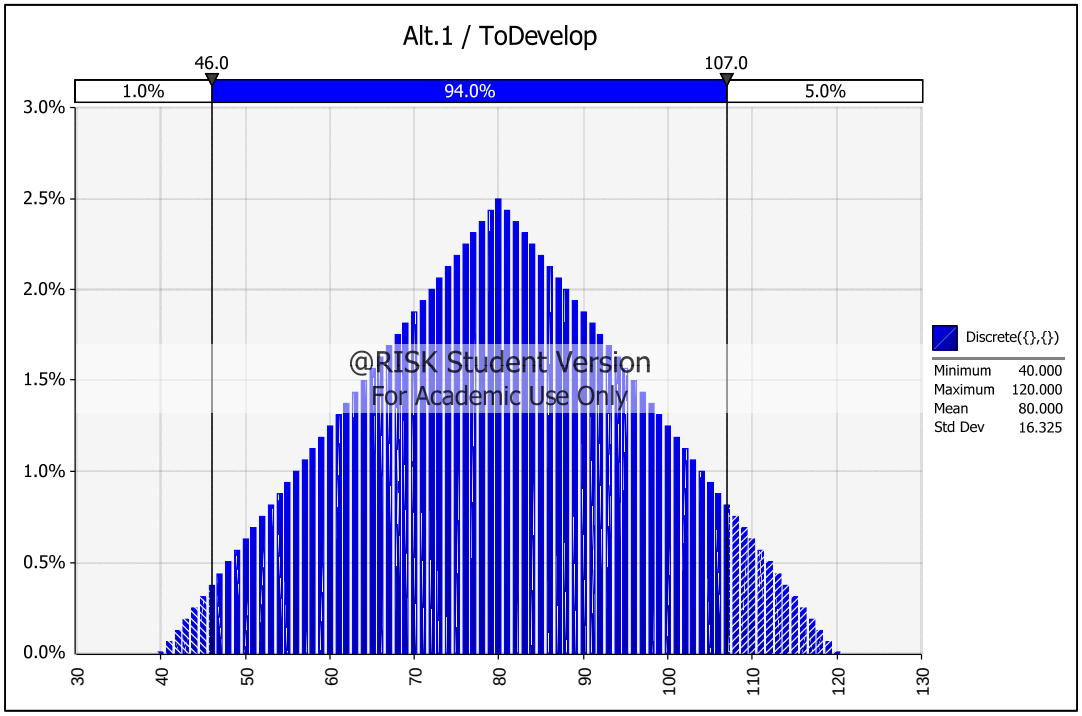


Figure 19. Example Distribution of Costs for a Given Alternative

8. Graphic Output

Figure 20 is an example of the graphical simulation output. The vertical portion of the graphic depicts the effectiveness of the course of action. Effectiveness starts at "Zero Effectiveness" at the origin and moves to "Maximum Effectiveness." Effectiveness is measured from zero to one. The decision maker value for the minimum effectiveness is depicted with a horizontal dashed line on the Effectiveness axis. The horizontal axis is used to depict the costs incurred with the course of action. Costs start at the origin with "Zero Costs" and continue to "Maximum Costs." Cost is measured from the least possible value of the three courses of action simulations to the maximum possible to encompass all values within the scenario. The decision maker value for the maximum costs to be incurred is depicted with a vertical dashed line on Cost axis. These decision maker inputs are what divide the graphic into four quadrants.

Graphical outputs are divided into four quadrants starting with Region 1 in the upper left corner and then progressing in a clockwise manner. Region 1 is the preferred region. In this area, the evaluated course of action met or exceeded the minimum

effectiveness and did not exceed the maximum cost. Moving to the top right is Region 2. In this region, the course of action met the minimum effectiveness but has broken the cost constraint. Below Region 2 is Region 3. In this area, the minimum effectiveness has not been met and the maximum cost has been breached. This is the worst area for a course of action. In the bottom left is Region 4. In this area, the minimum effectiveness has not been met but the maximum cost has not been exceeded. Figure 20 illustrates a sample simulation of a single course of action with 3,000 simulation iterations. As demonstrated in this example, Region 4 has the highest probability of occurrence with 67.2% of the simulation results, and therefore, this CoA will stay under the cost cap, but fail to meet the minimum effectiveness as it is currently defined.

E. PROCEDURES

Decentralization of authority to conduct cyber operations would first fall to CCMD organizations from U.S. Cyber Command. This experiment incorporated the scenarios used for SME elicitation along with the SME expertise. However, during this phase of the experiment, three additional pieces of information are added: decision maker preferences and values, the commander's deadline for operations to commence, and the simulated results of the SME elicitation (Dyer & Sarin, 1979).

As an example, in Scenario 3, the goal presented to the SMEs was maximizing intelligence while also minimizing detection. In the same scenario during this phase, participants were informed that the commander weighted the goals as 40% for maximizing intelligence with 60% for minimizing detection. The commander additionally stipulated that this operation would commence in nine days.

Participant scenarios were structured in the following manner once the DOSPERT risk questionnaire was completed: scenario, three courses of action presented in prose, and the same three courses of action graphically represented by the simulation. This order was used to prevent bias by first gathering the participants' honest evaluations and rankings of the traditionally written CoAs. Additionally, to prevent participants from establishing associations between the written and graphical CoAs, graphical CoAs were placed in a randomized order when compared to the written CoAs.

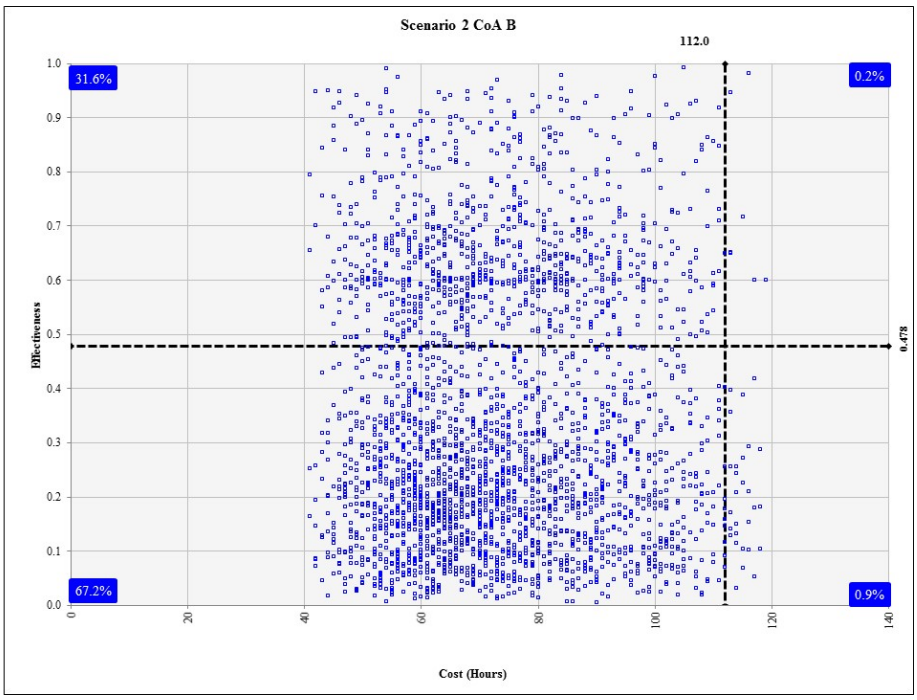


Figure 20. Sample Simulation Output

Randomization was accomplished by giving the numbers 1, 2, and 3, representing the courses of action, a random value between 0 and 1 in Microsoft Excel using native functionality. These values were then sorted from least to greatest value repeatedly. Each sorting of the data resulted in a new random number being assigned to the courses of action, thus changing the order of the courses of action. Based on feedback from SMEs and analysis of the SME elicitation, numbering of CoA from 1, 2, and 3 was switched to A, B, and C to eliminate confusion in numbers and rank preferences. See Figure 21 for the mapping of written to graphical courses of action. In this mapping, both the number and letter assigned to a course of action is denoted.

Participants were instructed that each scenario would include two groups of courses of action: one in written form and one in a graphical form. Participants were to rank the courses of action within each group highlighting those that best met the commander's needs in the scenario. These courses of action were to be rank ordered by individuals from the most preferred to the least preferred. The instructions specifically stated that the written and graphical CoAs were to be considered independently as these

two groups were not related and had no bearing on one another. However, both the written and graphical courses of action are relevant to the background information provided in the scenario.

F. EXPERIMENTAL PROCESS

Planners at the CCMD and national level OPTs first encountered the scenarios and written CoA. These scenarios included language to describe the fictitious adversary such as "which is a technological peer to…" along with past actions of the adversary that describe the events leading to the "present-day" in the scenario.

Scenario	Written COA	Graphical COA	Scenario	Written COA	Graphical COA
1A	A(1)	A	3	A(1)	C
	B(2)	C		B(2)	B
	C(3)	B		C(3)	A
1B	A(1)	B	4	A(1)	C
	B(2)	A		B(2)	A
	C(3)	C		C(3)	B
2	A(1)	C	5	A(1)	B
	B(2)	A		B(2)	C
	C(3)	B		C(3)	A

Figure 21. Mapping of Written CoA to Graphical CoA

From this language, the participants determined the threat posed by the adversary for their own use later in judging CoA. In a traditional risk assessment for these operations, the adversary would be rated as a high, moderate, or low risk. After mentally assessing the adversary and the threat in the scenario, three written CoA were presented to the participants. Each CoA described the strengths and limitations of the potential choice and the time needed to create or modify the capability for operational use. Participants then were asked to annotate their assessment of the most preferred CoA to the least preferred CoA. Immediately following, the participants then considered the

randomized presentation of the three graphical CoA for rank ordering, in terms of the most preferred to the least preferred. Once complete with this step, the next scenario would begin. This iterative method carried through all six scenarios. To reflect a realistic environment, no one CoA would satisfy the commander's wishes entirely. As stated by one SME with over six years of national level cyber experience who validated the scenarios, "These scenarios reflect real life. These are all shitty choices!"

G. EXPERIMENTAL DATA OUTPUTS

For this experiment, the results from each scenario were bootstrapped in accordance with Ernst (2004) as part of a Monte Carlo sampling to measure an exact amount of change. For bootstrapping to occur, the results of the written and graphical rank preference were available to be shifted. Shifting in this case is defined as a transposition between the written and graphical rankings and were recorded intact as triplets. Notably, rankings within the written and graphical answers were not reordered. For example, if selected, Participant 03's written rankings would be placed into the simulation's graphical rankings. Conversely, Participant 03's graphical rankings would be placed into the simulation's written rankings. Selection of transposition was a 50% - 50% random occurrence within the simulation. Each refresh of the screen or data change would trigger another round of random selection of data.

Below the data for the Monte Carlo simulation is a tabulated record of the change between the rankings of written CoAs and the rankings of the graphical CoAs. Each row of the tabulation counts the number of times a given CoA was selected for the first, second, or third choice. Each column tabulated the distribution of rankings across the CoAs. Both rows and columns totaled to the same number. See Figure 22 for an example of a simulation's record of change between the written and graphical CoA rankings. The participant-provided data allowed this author to determine an absolute value of the amount of change between the written and graphical CoAs. This was accomplished through a cross tabulation of the rows and columns. See Figure 23. Total change for a scenario considered both between groups change, for example, changing from CoA B to CoA C, and within group change, such as changing CoA B from first choice to second

choice. The grand total of change in the lower right corner of the example of Figure 23 combines the two amounts.

SCENARIO 5 CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	TOTAL
A	6	6	0	12
B	8	6	2	16
C	2	0	2	4
TOTAL	16	12	4	32

Figure 22. Example of Amount of Sum of Rank Order Changes in Monte Carlo Simulation Analysis

SCENARIO 5 CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	11	-5	-6	22
B	-14	8	6	28
C	3	-3	0	6
	28	16	12	56

Figure 23. Example of Cross Tabulation of Participant-Provided Data

Next, the simulation ran 10,000 iterations using a Monte Carlo sampling, each iteration receiving a new randomized set of rankings. The output was a non-parametric distribution that was used for comparison to the original data. See Figure 24. Following the insights of Ernst (2004), this technique provides an exact *p* value, allowing for direct comparison between the participant provided data and the Monte Carlo sampled simulation. This technique also precludes the need for a sample size to be generated as an

exact value is computed. Additionally, this research attained the population of combatant command offensive cyber planners at the combatant command level of the DOD.

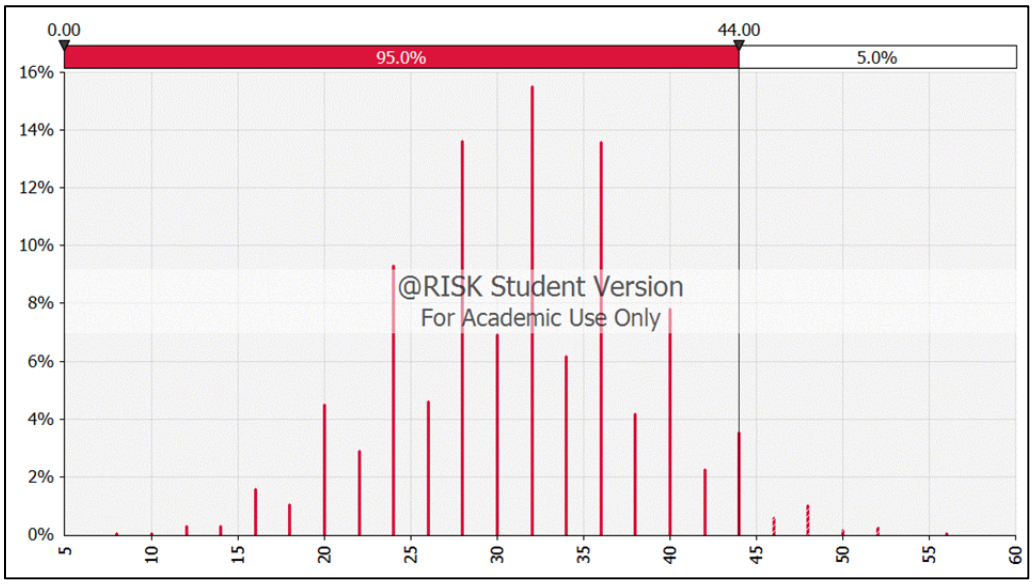


Figure 24. Example Monte Carlo Sampling Simulation Output Distribution

The observed value gained from the participant data is then compared to the distribution of the simulation results. The null hypothesis is rejected if the observed data falls outside of the 95% confidence area, thus p = .05 or less. Figure 23 illustrates the cross tabulated number from the Monte Carlo sampled simulation, 32, as being the mode within the distribution. The original data cross tabulated number, 56, is found well into the tail of the distribution, when using the 5% delineation on the ruler above the distribution, and satisfies the $p \leq .05$ requirement for rejection of the null hypothesis. Thus, a significant change is found between the written and graphical rankings.

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. DATA ANALYSIS

This research effort investigates how beneficial a framework with graphical outputs of risk is for aiding personnel who lack the necessary experience. In this effort, the personnel examined were two groups: personnel with national level cyber experience and personnel without. The experiment focused on the amount of change between rankings of written and graphical CoAs using the null hypothesis: *No significant change occurs between the written and graphical CoA rank choices for each scenario.* The following analysis examines the results of six scenarios that participants encountered: three whose purpose was to gather intelligence and three whose purpose was to inflict damage.

Each scenario is analyzed in six different ways. The first three are population-centered analyses. These three, in order, are as follows: all participants with no one group, either national level experienced or inexperienced, held constant; all participants with personnel with national level experience held constant; and all participants with personnel lacking national level experience held constant. These three analyses are used for two reasons. The first is to determine if the framework benefits the population, as a whole. The second is to determine if the increased participant *N* affects the outcome of the experiment.

The fourth and fifth analyses are sample-centered. The fourth is a sample consisting of only the participants that previously had national level experience. The fifth is the converse: personnel lacking national level experience. These analyses are conducted to determine if the null hypothesis is to be accepted or rejected. The sixth analysis will focus on the USCYBERCOM participants. This analysis examines how effective this framework is for planners currently working at the national level, in addition to being used as the control for comparison against inexperienced personnel. See Appendix H for the participant packet containing the scenarios and graphics discussed in this chapter.

Analysis used simulation modeling in the @Risk software. Each contained the participant provided data and the sum of all rank order changes from the written to the graphic rankings. The sum of all rank changes was used to capture both the change between groups and within groups. An example of a between group change for this research is the change in the preferred CoA from A to C. An example of a within group change is the number of participants shifting votes for a particular CoA to another rank order position.

All 36 simulations consisted of 10,000 iterations. Participant data for the written and graphic rankings were considered an intact group of three values, or a triplet. This triplet contained the first, second, and third choice for CoA rankings for each participant. For the simulation, written and graphic triplets had equal probability, $p = 0.5$, of being the basis of rank assignment. In other words, it is equally likely that the written became the graphic CoA rankings and the graphic triplet assumed the written rankings role. For analyses where groups were held constant, the .5 chance of swapping triplets was removed.

Simulations then produced a relative frequency histogram approximating the nonparametric distribution of the sum of rank order changes to occur. The participant-observed sum of changes then was compared to the distribution. This method of bootstrap simulation using a Monte Carlo simulation allows an exact p-value to be computed, instead of an approximation. This method produces an accurate approximation to the true sampling distribution to arrive at the sampling distribution for N equaling the number of possible combinations (M. D. Ernst, 2004). However, before the participants encountered scenarios, they completed three questionnaires to assess their risk attitude and profile.

A. RISK ATTITUDES AND PROFILES

Each packet presented the participant with a questionnaire to ascertain risk attitudes and profiles. These profiles generalized to a person being risk seeking or risk averse. This research used the Domain Specific Risk Taking (DOSPERT) (Blais & Weber, 2006). See Appendix E for a sample questionnaire. This scale measures the likelihood of being risk seeking or risk averse in five domain areas: ethics, financial,

health and safety, recreational, and social. Six questions in each domain comprise the assessment and are answered using a 1 through 7 Likert scale by the participant. Positive scores are risk seeking while negative scores are risk averse.

For this research, the five domains were then aggregated together to provide a more holistic profile of the individual. Individuals were then aggregated again into one of four groups: SME; personnel having national level experience working at the CCMD level, also known as Experienced, Inexperienced personnel, and the USCYBERCOM planners. This aggregation provided a more generalizable analysis for the distinct populations.

In the first analysis, an unexpected trend appeared. The groups consisting of the SMEs and the experienced personnel, minus the USCYBERCOM planners, scored mildly risk seeking and approximately the same value. However, the inexperienced personnel and the USCYBERCOM planners also both scored approximately the same but almost doubled the score of the SMEs and experienced personnel, hence being almost twice as risk seeking. This result however does not have a p-value of less than .05, so more analysis followed. Please see Figure 25.

Groups	*Count*	*Sum*	*Average*	*Variance*		
SME	30	10.00495	0.333498	0.200744		
Experienced	17	7.692472	0.452498	0.146395		
Inexperienced	29	17.64442	0.608428	0.18439		
USCYBERCOM	14	8.493226	0.606659	0.262975		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	1.355174	3	0.451725	2.319929	0.080986	2.710647
Within Groups	16.74549	86	0.194715			
Total	18.10066	89				

Figure 25. ANOVA Results of Risk Seeking Tendencies for Four Groups of Participants

Following the data led to grouping the SMEs and the Experienced groups together and the Inexperienced and USCYBERCOM groups. Another ANOVA was calculated and in this analysis, a p-value of 0.014224 was attained. Again, the SME and Experienced group was approximately half of the risk seeking attitude of the Inexperienced and the USCYBERCOM planners. See Figure 26.

These analyses point to the backgrounds of the personnel. The members of the SME and Experienced groups primarily worked within the Intelligence Community of the government. This community is responsible for gathering the sensitive intelligence from which strategic estimates and decisions at the highest levels of government are made. Operations within the Intelligence Community often occur during times of peace or beginnings of tension escalation in an attempt to defuse the situation. Operations within the Intelligence community employ sources, methods, and techniques that are highly sensitive and would cause grave damage to the nation's ability to gather intelligence, if caught. As such, these operations are highly meticulous and often err on the side of caution to avoid the loss of assets.

Groups	*Count*	*Sum*	*Average*	*Variance*		
SME and EXP Personnel	47	17.69743	0.376541	0.180816		
Inex Personnel and USCYBERCOM	43	26.13765	0.607852	0.204324		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	1.201483	1	1.201483	6.256549	0.014224	3.949321
Within Groups	16.89918	88	0.192036			
Total	18.10066	89				

Figure 26. ANOVA Results of Risk Seeking Tendencies for Two Groups of Participants

The second group comprised of the Inexperienced and USCYBERCOM planners possess backgrounds primarily in traditional military operations. Operations planned by the military community traditionally focus on environments in which deterrence has failed and an adversary must be brought to their knees under conditions deemed

satisfactory to the United States. This mentality has no need for sensitive operations where sources, methods, and techniques may be lost. Falling bombs do not require operational sensitivity. As such, many personnel within the military consider OCO as analogous to or as an enabler of kinetic operations.

B. SCENARIO 1A

Scenario 1A introduced the participants to a future situation in which CCMDs have been partially delegated authority for conducting intelligence and attack cyber operations. In this first scenario, the combatant commander needs intelligence to ascertain the intentions of an adversary that is threatening a U.S. ally and escalating tensions. Intelligence from other sources indicates that the adversary may invade the ally, and the combatant commander wishes to confirm or deny that report. In this scenario, the commander places values of 60% for avoiding detection and 40% for gathering the required intelligence. Success in this operation is defined as the exfiltration of a Microsoft Word document outlining the adversary's attack plans, at a minimum.

1. Scenario 1A with All Participants

This analysis produced a test statistic with a p-value of .686 constituting little or no evidence for rejection of the null hypothesis. Remember that the simulation provides and exact p-value, not an approximation (Ernst, 2004). In this analysis, all personnel, regardless of national level experience, chose graphical choices that corresponded with their written CoA choices. For Scenario 1A, only 24 participant choices changed, tying Scenario 4 for the least change of the six scenarios. In fact, Scenario 1A analysis resulted in a confidence interval of 32%, depicted by the blue line in Figure 27. Follow-on interviews to determine how participants made choices were not possible due to operations. See Figure 28 for the choices and amount of change for Scenario 1A. As mentioned in the previous chapter, the highlighted number in the figures depicting the sum total of rank changes reflects the total amount of change both within ranks, for example changing from changing CoA C from first choice to second choice, and between ranks, such as changing from CoA B to CoA C.

As the amount of participant change within the scenarios does not change within the population analysis, only the introductory analysis will display the amount of change. Individual sample analyses for experienced personnel only, inexperienced personnel only, and USCYBERCOM personnel only will include the total tabulated amount of change within only these groups.

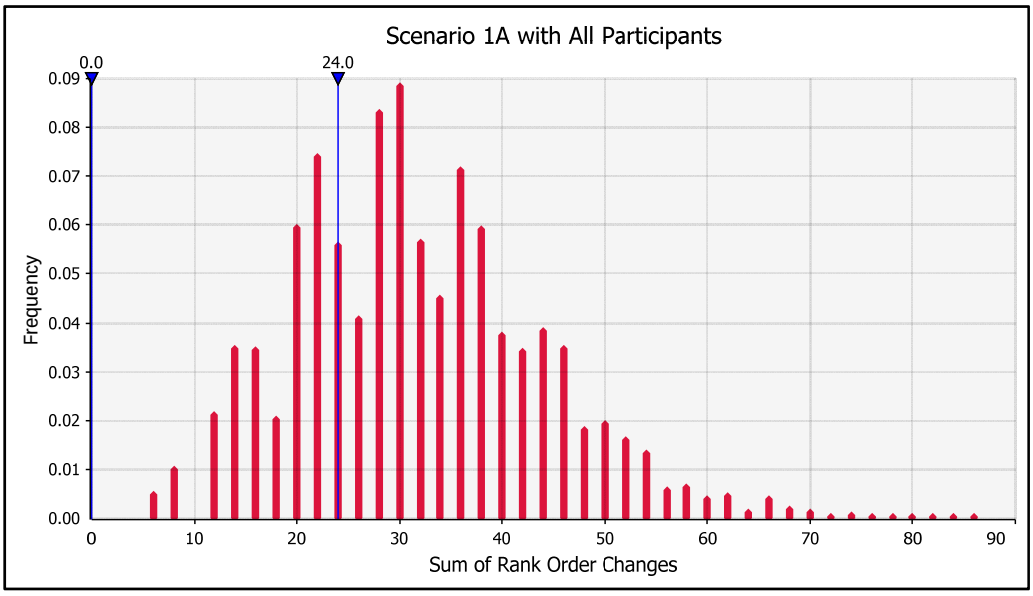


Figure 27. Scenario 1 with All Participants

	SCENARIO 1A TOTALS					
	Written			Graphic Deciphered		
	1st	2nd	3rd	1st	2nd	3rd
A	9	22	29	11	19	30
B	38	15	7	41	16	3
C	13	23	24	8	25	27

	SCENARIO 1A CHANGE			
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	2	-3	1	6
B	3	1	-4	8
C	-5	2	3	10
	10	6	8	24

Figure 28. Scenario 1A Choices and Change for All Participants and Nothing Held Constant

a. Scenario 1A with All Participants and Experienced Personnel Held Constant

This case produced a test statistic with a p-value of .677, providing little or no evidence to reject the null hypothesis. Holding experienced personnel constant for a higher participant count was ineffective as this analysis of Scenario 1A was not statistically significant. This Scenario 1A analysis provided a 32.4% confidence interval again as depicted by the blue line in Figure 29. Analysis suggests that all the participants lacking national level experience in this scenario evaluated CoAs based on the percentage of simulation outputs in Region 1 and Region 2, the regions that satisfied the effectiveness requirements from the commander.

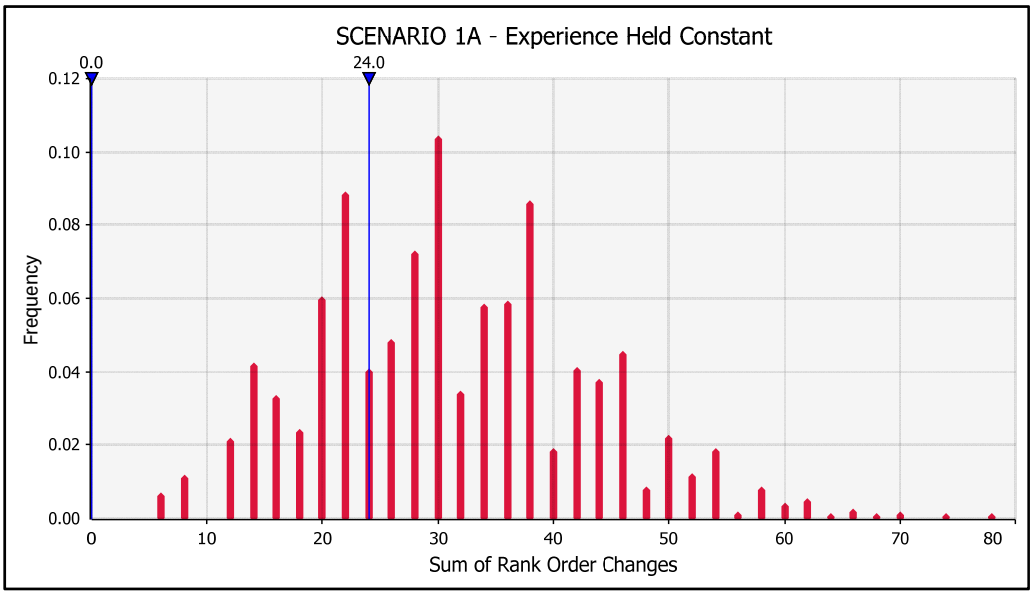


Figure 29. Scenario 1A with Experienced Personnel Held Constant

b. Scenario 1A with All Participants and Inexperienced Personnel Held Constant

This analysis produced a test statistic with a p-value of .897, again, providing little or no evidence for rejection of the null hypothesis. Scenario 1A with inexperienced personnel held constant fared better, but was not statistically significant. This analysis provided a confidence level of 85.1%, as depicted by the blue line in Figure 30, suggesting that personnel with national level experience received more value. Analysis suggests that all the participants with national level experience in this scenario evaluated CoAs based on the percentage of simulation outputs in Region 1 and Region 2, the regions that satisfied the effectiveness requirements from the commander.

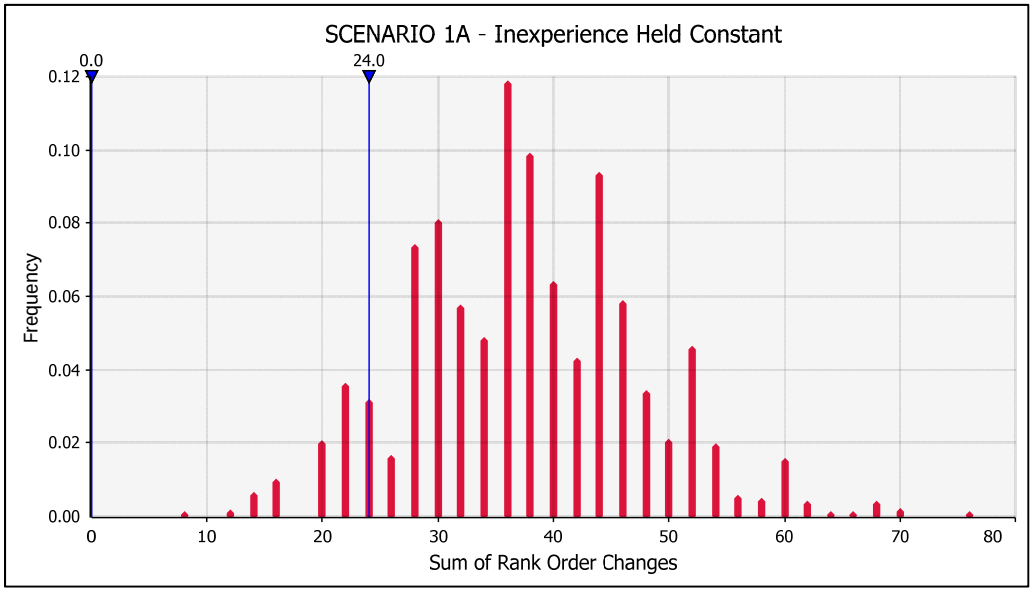


Figure 30. Scenario 1A with Inexperienced Personnel Held Constant

2. Scenario 1A with Experienced Personnel Removed

This analysis produced a test statistic with a p-value of .107, indicating inconclusive evidence for rejection of the null hypothesis. One would not reject the null hypothesis in this case when using the traditional 95% confidence region. Scenario 1A analysis of only personnel lacking national level experience was not statistically significant. Scenario 1A analysis provided an 89.8% confidence level, as depicted by the blue line in Figure 31. Analysis suggests that all the participants lacking national level experience in this scenario evaluated CoAs based on the percentage of simulation outputs in Region 1 and Region 2, the regions that satisfied the effectiveness requirements from the commander. See Figure 32 for the choices and amount of change for this analysis of Scenario 1A.

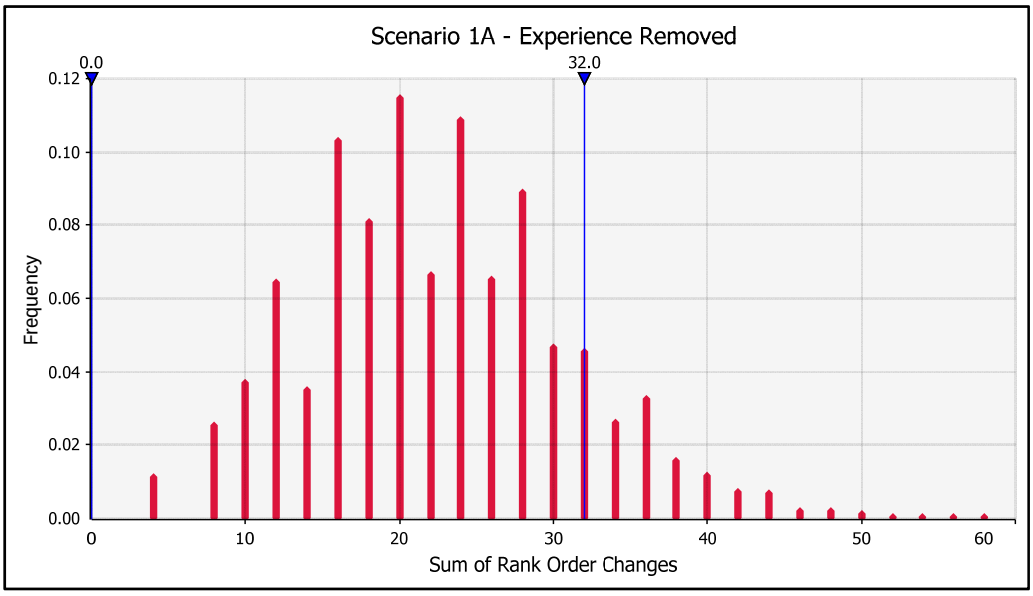


Figure 31. Scenario 1A with Experienced Personnel Removed

	SCENARIO 1A TOTALS					
	Written			Graphic Deciphered		
	1st	2nd	3rd	1st	2nd	3rd
A	3	12	14	8	5	16
B	18	6	5	16	12	1
C	8	11	10	5	12	12

SCENARIO 1A CHANGE				
	Graphic Deciphered			
CHOICE	**1st**	**2nd**	**3rd**	
A	5	-7	2	14
B	-2	6	-4	12
C	-3	1	2	6
	10	14	8	**32**

Figure 32. Scenario 1A Choices and Change with Experienced Personnel Removed

3. Scenario 1A with Inexperienced Personnel Removed

This analysis of Scenario 1A produced a test statistic with a p-value of .378 constituting little or no evidence for rejecting the null hypothesis. Scenario 1A analysis of only personnel with national level experience was not statistically significant with a

resulting 61.1% confidence level as depicted by the blue line in Figure 33. Analysis suggests that all the participants with national level experience in this scenario evaluated CoAs based on the percentage of simulation outputs in Region 1 and Region 2, the regions that satisfied the effectiveness requirements from the commander. See Figure 34 for the choices and amount of change for this analysis of Scenario 1A. For this analysis, experienced participants demonstrated a greater propensity to choose CoA B as the first choice, suggesting that the graphics influenced them.

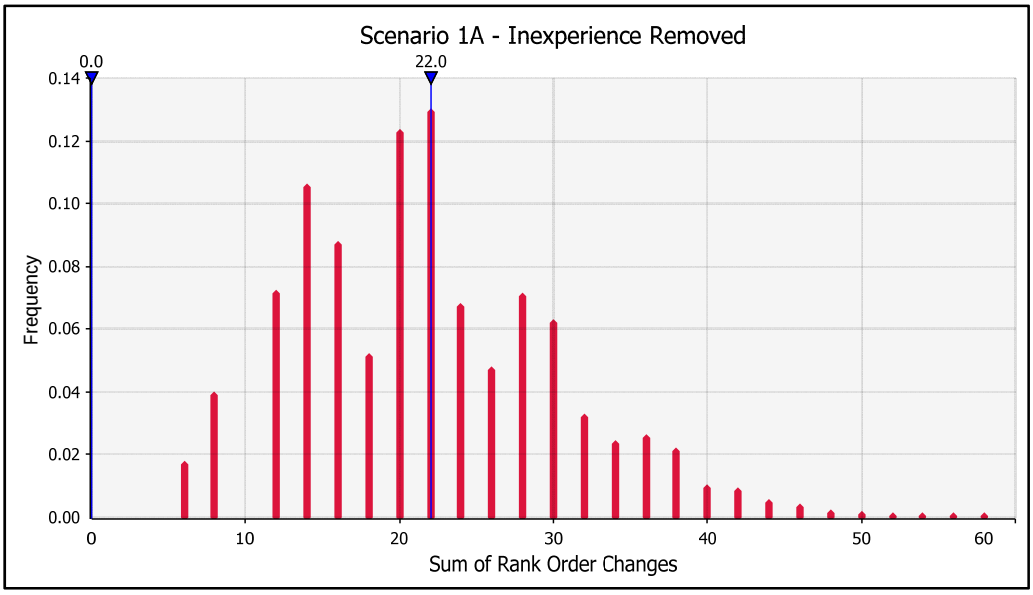


Figure 33. Scenario 1A with Inexperienced Personnel Removed

	SCENARIO 1A TOTALS					
	Written			Graphic Deciphered		
	1st	2nd	3rd	1st	2nd	3rd
A	6	10	15	3	14	14
B	20	9	2	25	4	2
C	5	12	14	3	13	15

SCENARIO 1A CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	-3	4	-1	8
B	5	-5	0	10
C	-2	1	1	4
	10	10	2	22

Figure 34. Scenario 1A Choices and Change with Inexperienced Personnel Removed

4. Scenario 1A with USCYBERCOM Personnel Only

This analysis produced a test statistic with a p-value of .057, indicating weak evidence against the null hypothesis. One would not reject the null hypothesis outright, however, using the traditional 95% confidence region. However, this analysis reached a 94.7% confidence as depicted by the blue line in Figure 35. Analysis suggests that all the USCYBERCOM participants in this scenario evaluated CoAs based on the percentage of simulation outputs in Region 1 and Region 2, the regions that satisfied the effectiveness requirements from the commander. See Figure 36 for the choices and amount of change for Scenario 1A. Please note the agreement of opinion regarding graphic recommended for the first choice, CoA B, in the upper graph of Figure 35 with 12 selections as opposed to one selection for each of the other two choices.

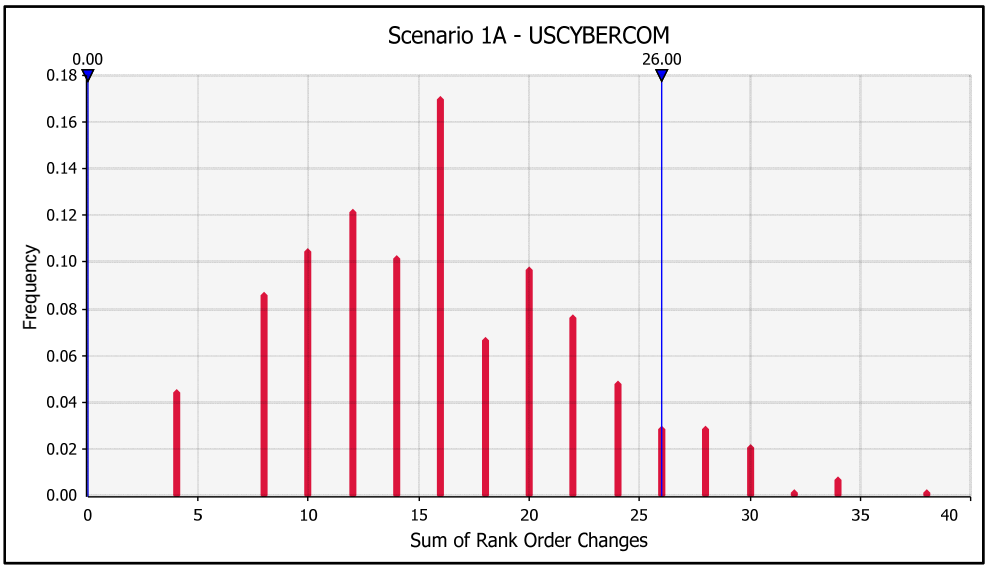


Figure 35. Scenario 1A with USCYBERCOM Personnel Only

	SCENARIO 1A TOTALS					
	Written			Graphic Deciphered		
	1st	2nd	3rd	1st	2nd	3rd
A	4	2	8	1	7	6
B	8	4	2	12	2	0
C	2	8	4	1	5	8

SCENARIO 1A CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	-3	5	-2	10
B	4	-2	-2	8
C	-1	-3	4	8
	8	10	8	26

Figure 36. Scenario 1A Choices and Change with USCYBERCOM Personnel Only

5. Scenario 1A Conclusions

In retrospect, the CoAs for this scenario may have been too similar in their predicted probability of success. Multiple participants noted the potential for detection in the written CoAs. CoA B, the most popular first choice, was not detected in virtualized testing. The next most popular written CoA choice was CoA C, which had been used in

operations in the past undetected, but virtualized testing indicated that it would be detected. The least popular choice, CoA A, was a modified open-source tool with a known signature that offered a 50/50 chance of detection. This information also aligns with the Graphic CoA choices.

Analysis of the graphical choices made by participants demonstrates that CoA B, presented to the participants as CoA 3, was the overwhelming first choice in every analysis. CoA B had a combined 27.7% predicted effectiveness when Regions 1 and 2 were combined. The second choice in all but two analyses was CoA A, also presented as CoA A. Not enough data exists in this scenario to accurately account for choices made between the other two CoAs when examining second and third choices. As statistical significance was not attained in any of the analyses in this scenario, no further analysis will be conducted to illustrate support for the advanced hypothesis.

C. SCENARIO 1B

Scenario 1B is the continuation and escalation of Scenario 1A. In this scenario, the combatant commander has attained the required information. Analysis has determined that the adversary intends to erode the trust between the United States and its ally by conducting small-scale guerilla attacks. The commander wishes to conduct a computer network attack for two purposes: to disrupt the planning for guerilla attacks and to demonstrate the network vulnerabilities to the adversary, suggesting that the United States is aware of its intentions. The commander places 60% of his value on destruction and 40% on avoiding attribution. Success in this operation is achieved when all information residing on the target containing a 1 terabyte hard drive is rendered inaccessible and unrecoverable.

1. Scenario 1B with All Participants

This analysis produced a test statistic with a p-value less than .000001; indicating strong evidence against the null hypothesis and certain rejection is using the traditional 95% confidence interval. In this analysis, statistical significance was attained at more than a 99% confidence level as depicted by the blue line in Figure 37. Analysis suggests

that CoA B, presented as CoA 1, was chosen by participants due to the 27.4% prediction of meeting both Effectiveness and Cost constraints as compared to the 21.7% CoA C, presented as CoA 3. Interestingly, 27 of 60 participants chose CoA A as the first or second choice in the written format; however, this dramatically changed with the graphical presentation with 55 of 60 participants ranking this CoA in last place. See Figure 38 for the participant choices and the amount of change.

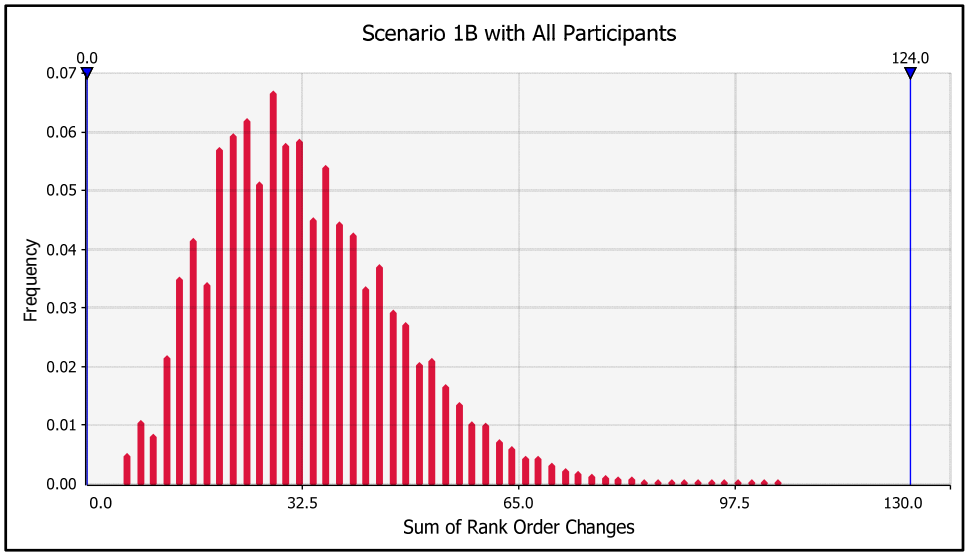


Figure 37. Scenario 1B with All Participants

SCENARIO 1B TOTALS					
Written			Graphic Deciphered		
1st	2nd	3rd	1st	2nd	3rd
2	25	33	5	0	55
49	5	6	34	25	1
9	30	21	21	35	4

SCENARIO 1B CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	3	-25	22	50
B	-15	20	-5	40
C	12	5	-17	34
	30	50	44	124

Figure 38. Scenario 1B Choices and Change for All Participants and Nothing Held Constant

a. Scenario 1B with All Participants and Experienced Personnel Held Constant

Again, this analysis produced a test statistic with a p-value less than .000001; indicating strong evidence against the null hypothesis and certain rejection is using the traditional 95% confidence interval. This form of analysis again exceeded a 99% confidence level, making it statistically significant, as depicted by the blue line in Figure 39. Analysis suggests that all the participants lacking national level experience in this scenario evaluated CoAs based on the percentage of simulation outputs in Region 1, the region that satisfied both the Cost and Effectiveness requirements from the commander.

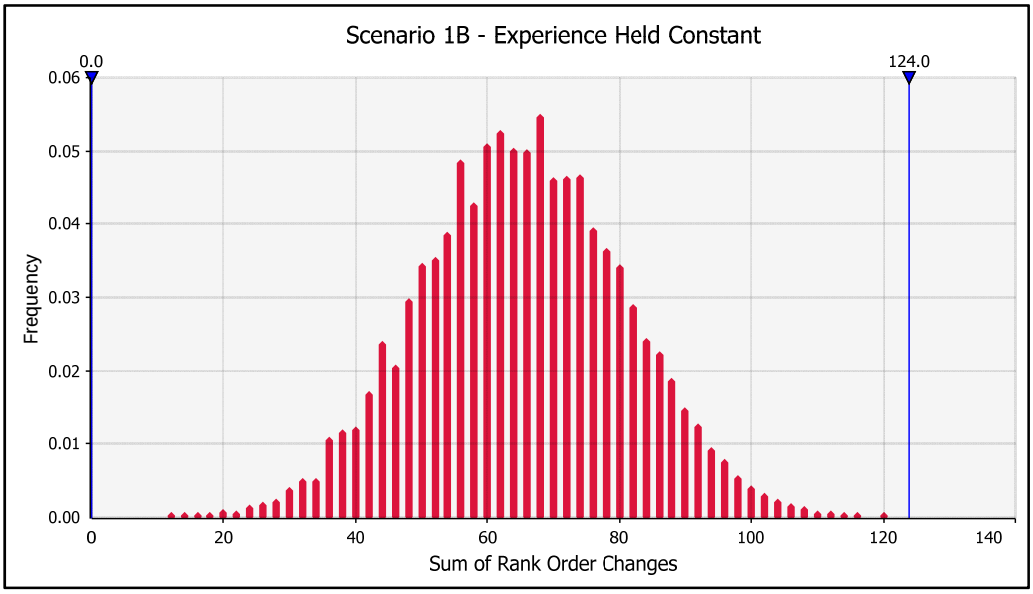


Figure 39. Scenario 1B with Experienced Personnel Held Constant

b. Scenario 1B with All Participants and Inexperienced Personnel Held Constant

This analysis of Scenario 1B produced a test statistic with a p-value less than .00018; indicating strong evidence against the null hypothesis and certain rejection is using the traditional 95% confidence interval. The analysis of all personnel while holding inexperienced personnel constant begins to illuminate an unexpected consequence of this research: the application of this framework to be effective for personnel with national

level experience. This analysis also exceeds a 99% confidence level, however, this analysis more easily exceeds the 95% confidence standard than when experienced personnel were held constant. Notice the upper limit of the 95% range in each of the two analyses. The previous analysis with experienced personnel held constant required 90 choice changes to be significant. This analysis required only 64 changes, thus farther exceeding the minimal level of significance. See Figure 40.

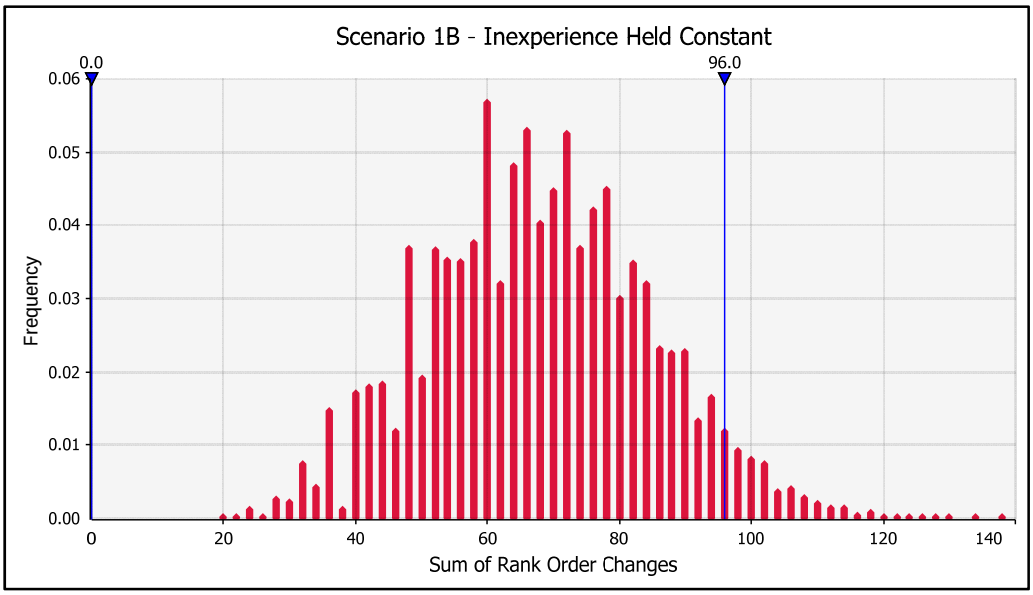


Figure 40. Scenario 1B with Inexperienced Personnel Held Constant

2. Scenario 1B with Experienced Personnel Removed

Analysis of Scenario 1B with experienced personnel removed produced a test statistic with a p-value of .00002; indicating strong evidence against the null hypothesis and certain rejection is using the traditional 95% confidence interval. Scenario 1B analysis of only personnel lacking national level experience was statistically significant at a greater than 99% confidence level, as depicted by the blue line in Figure 41. Analysis suggests that all the participants lacking national level experience in this scenario evaluated CoAs based on the percentage of simulation outputs in Region 1, as observed earlier in this section. In fact, the choice of CoA B as the recommended CoA increased by 33% from the written to the graphic ranking. Additionally, the recommended graphic

votes nearly bested the second place CoA by 77%. See Figure 42 for the choices and amount of change in this analysis.

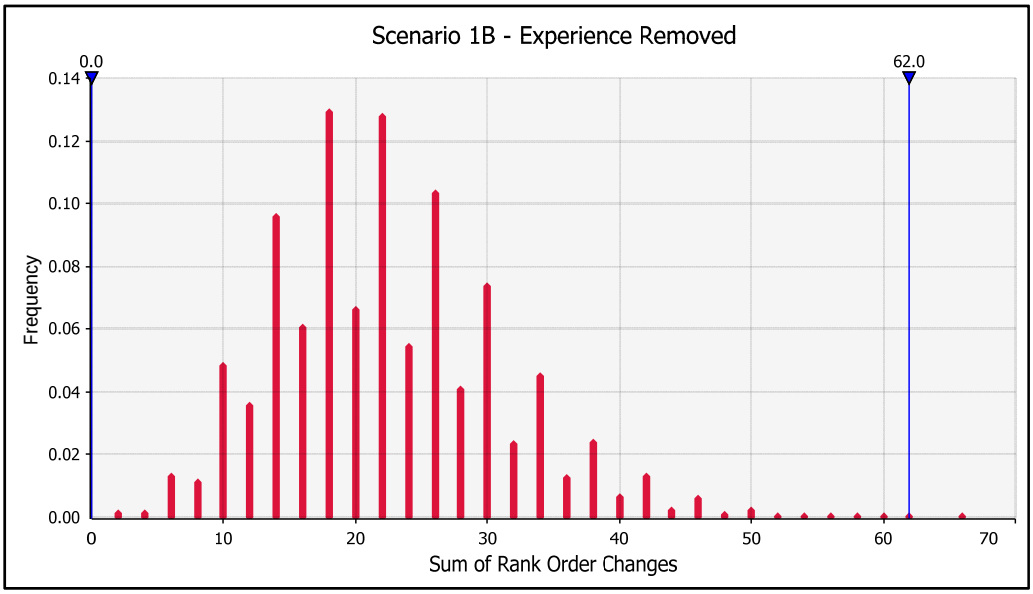


Figure 41. Scenario 1B with Experienced Personnel Removed

	SCENARIO 1B TOTALS					
	Written			Graphic Deciphered		
	1st	2nd	3rd	1st	2nd	3rd
A	12	13	15	4	0	25
B	12	0	5	16	12	1
C	5	16	9	9	17	3

SCENARIO 1B CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	-8	-13	10	31
B	4	12	-4	20
C	4	1	-6	11
	16	26	20	62

Figure 42. Scenario 1B Choices and Change with Experienced Personnel Removed

3. Scenario 1B with Inexperienced Personnel Removed

This analysis produced a test statistic with a p-value less than .00074, indicating strong evidence against the null hypothesis and certain rejection if using the traditional 95% confidence region. Scenario 1B analysis of only personnel with national level experience was statistically significant, exceeding the 99% confidence level, as depicted by the blue line in Figure 43. Analysis suggests that all the participants with national level experience in this scenario evaluated CoAs the same as the personnel lacking experience, based on the percentage of simulation outputs in Region 1. See Figure 44 for the choices and amount of change in this analysis. Although the level of aggregated agreement diminished by 28% from the written to the graphic rankings, a strong enough aggregated consensus remained to allow CoA B to remain the recommended CoA.

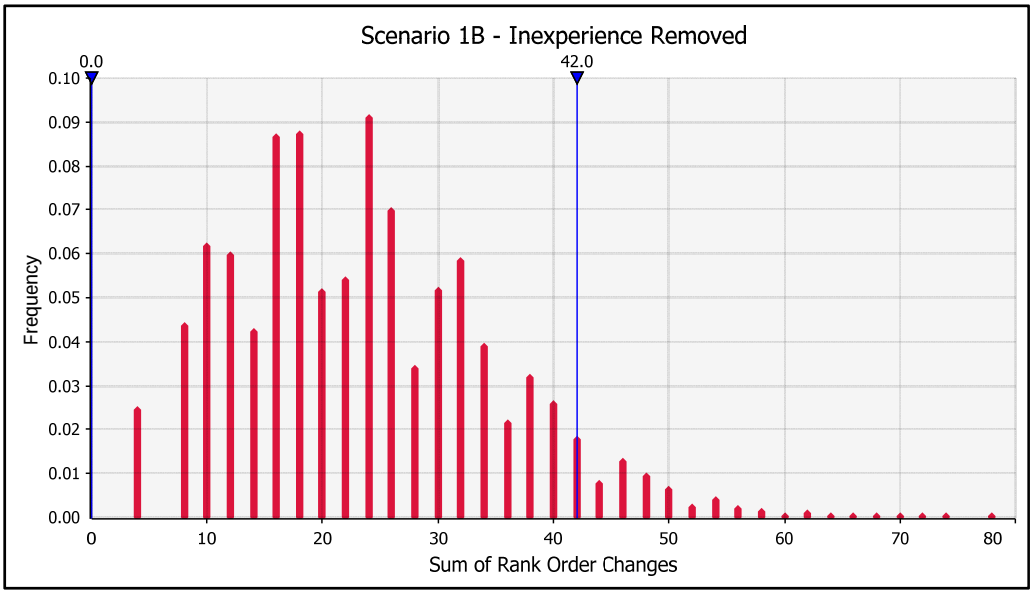


Figure 43. Scenario 1B with Inexperienced Personnel Removed

	SCENARIO 1B TOTALS					
	Written			Graphic Deciphered		
	1st	2nd	3rd	1st	2nd	3rd
A	1	12	18	1	0	30
B	25	5	1	18	13	0
C	5	14	12	12	18	1

SCENARIO 1B CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	0	-12	12	24
B	-7	8	-1	16
C	7	4	-11	22
	14	24	24	62

Figure 44. Scenario 1B Choices and Change with Inexperienced Personnel Removed

4. Scenario 1B with USCYBERCOM Personnel Only

Analysis of the USCYBERCOM planners produced a test statistic with a p-value less than .000001 indicating strong evidence against the null hypothesis and certain rejection if using the traditional 95% confidence region. For this level of analysis, Scenario 1B was highly statistically significant, exceeding the 99% as depicted by the blue line in Figure 45. Analysis suggests that the USCYBERCOM participants evaluated CoAs the same as the personnel in the other analyses, based on the percentage of simulation outputs in Region 1. See Figure 46 for the choices and amount of change for Scenario 1B. Interestingly enough, the USCYBERCOM planners decreased in agreement by almost half but also shifted to a unanimous agreement that CoA was the last choice for a recommended CoA.

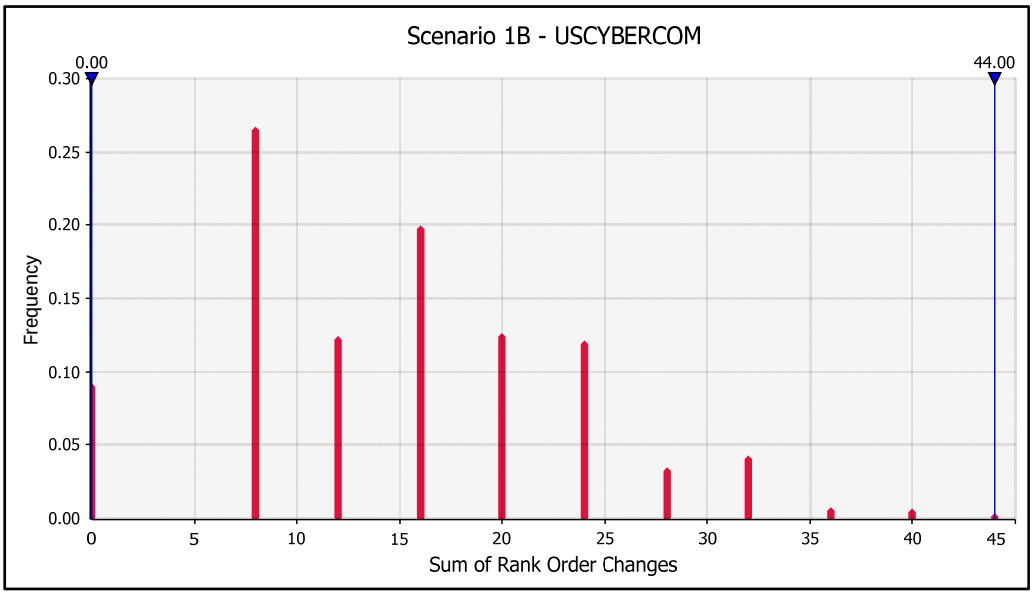


Figure 45. Scenario 1B with USCYBERCOM Personnel Only

	SCENARIO 1B TOTALS					
	Written			Graphic Deciphered		
	1st	2nd	3rd	1st	2nd	3rd
A	0	8	6	0	0	14
B	13	1	0	7	7	0
C	1	5	8	7	7	0

SCENARIO 1B CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	0	-8	8	16
B	-6	6	0	12
C	6	2	-8	16
	12	16	16	44

Figure 46. Scenario 1B Choices and Change with USCYBERCOM Personnel Only

5. Scenario 1B Conclusions

This scenario demonstrated the ability to aid personnel with national level experience in understanding risk, not just the inexperienced. Additionally, this scenario demonstrated how a CoA may be interpreted as feasible in a written format while having little to no potential for success when mathematically modeled. Remember that 30 SMEs

evaluated the different CoAs and provided their 90% confidence intervals. This insight further demonstrates the need for a quantified risk analysis. Participants, regardless of the method of analysis, continued to make decisions of preference ranking based off of Region 1 of the charts, as was observed in Scenario 1A.

Since this scenario was statistically significant, further examination is warranted into the overall effectiveness of the framework. This researcher proposed that a framework that quantified risk, based on SME knowledge, would mitigate the inexperience of personnel lacking national level experience. In Scenario 1B, this hypothesis is supported. When presented with graphics that provide less subjective information, 58% of all personnel possessing national level experience and 50% of the USCYBERCOM only sample chose the same first preferred CoA. Additionally, 55% of the inexperienced personnel chose the same first preferred CoA, suggesting that Scenario 1B supports this research's hypothesis. The majority of both experienced and inexperienced personnel chose the same CoA.

D. SCENARIO 2

Scenario 2 changes focus to combating a non-state actor. In this scenario, the actor in question uses the Internet to recruit, to spread propaganda, to orchestrate command and control of operations. The non-state actor escalates the situation by posting a video of a captured U.S. service member being killed as a propaganda tool. The combatant commander, working in coordination with the Theater Special Operations Command (TSOC), designated five personnel as high payoff targets. These targeted personnel are instrumental to operations and are believed to be directly connected to the service member's death. For this operation, the combatant commander orders that online intelligence operations are to commence for the purpose of gathering information for ascertaining the patterns of life of the five targets. Once enough information has been attained, the TSOC will coordinate for capture/ kill operations to commence. The combatant commander has placed equal value on gaining the intelligence while avoiding being detected.

1. Scenario 2 with All Participants

Analysis of Scenario 2 began with production of a test statistic with a p-value less than Scenario 2 .000005814, indicating strong evidence against the null hypothesis and certain rejection is using the traditional 95% confidence region. This analysis of all participants exceeded the 99% confidence level as shown with the blue line in Figure 47. Participants in this scenario appeared to continue to examine and compare the percentage of simulation iterations in Region 1 of the graphics for rank ordering preferences. See Figure 48 for the choices and amount of change between the written and graphic CoA choices. Please note the overwhelming coalescence of choice for CoA A as the first choice in the graphic presentations when compared to the written CoAs. The same observation holds true for the second preferred CoA, C. The least preferred CoA, B, has a total of 0.3% predicted success meeting the required effectiveness, as mathematically modeled using the SME insights. Interestingly, the shift in agreement from the written to graphic rankings in this analysis was nearly unanimous, with only eight disagreeing for the first place recommended CoA and seven for the second place.

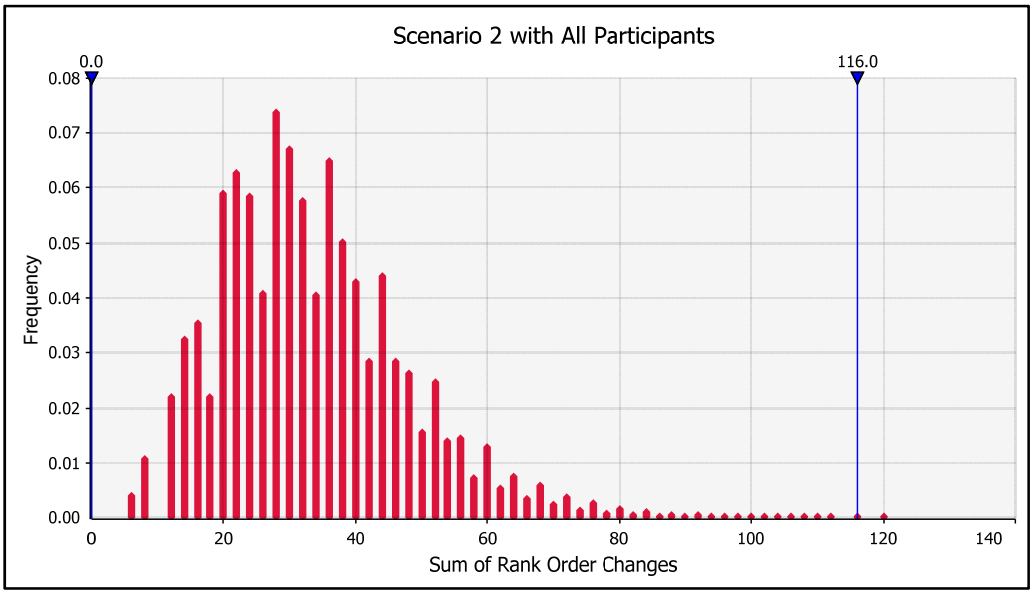


Figure 47. Scenario 2 with All Participants

SCENARIO 2 TOTALS					
Written			Graphic Deciphered		
1st	2nd	3rd	1st	2nd	3rd
32	14	14	52	1	7
6	18	36	5	6	49
22	28	10	3	53	4

SCENARIO 2 CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	20	-13	-7	40
B	-1	-12	13	26
C	-19	25	-6	50
	40	50	26	116

Figure 48. Scenario 2 Choices and Change for All Participants and Nothing Held Constant

a. Scenario 2 with All Participants and Experienced Personnel Held Constant

This analysis produced a test statistic with a p-value less than .01888, indicating strong evidence against the null hypothesis and certain rejection if using the traditional 95% confidence region. Although this analysis is less striking than the previous one, this examination still is significant at a near 98% confidence, as indicated by the blue line in Figure 49. Analysis suggests that all the participants lacking national level experience in this scenario evaluated CoAs based on the percentage of simulation outputs in Region 1—the region that satisfied both the cost and effectiveness requirements from the commander.

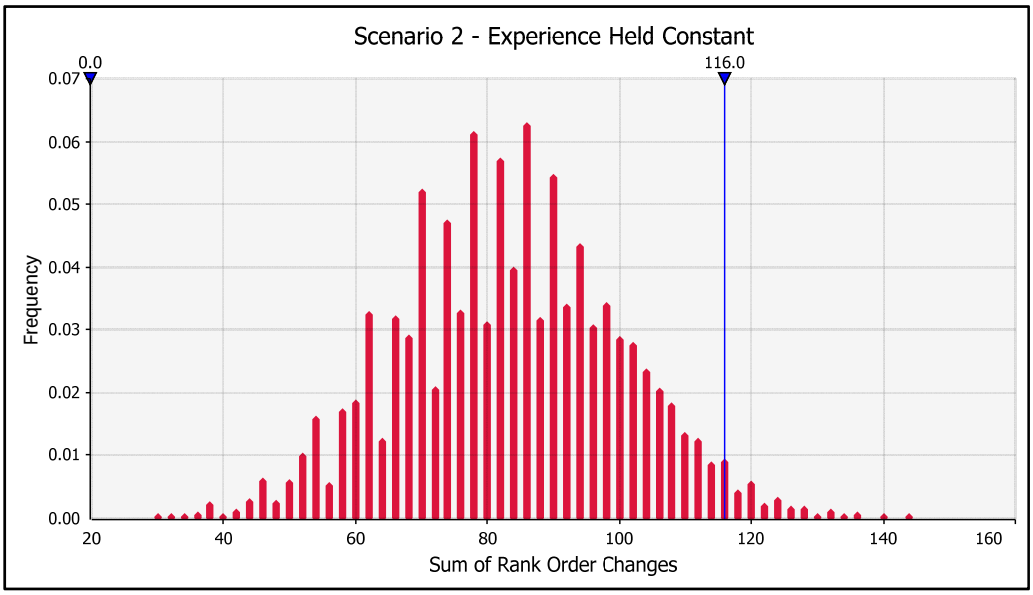


Figure 49. Scenario 2 with Experienced Personnel Held Constant

b. Scenario 2 with All Participants and Inexperienced Personnel Held Constant

Figure 50 produced a test statistic with a p-value less than 000088., indicating strong evidence against the null hypothesis and certain rejection if using the traditional 95% confidence region. This analysis illuminates the extreme results of this analysis when participants with national level personnel are the focus of analysis. As with the previous scenario, this analysis further suggests the framework's value to personnel with national level experience.

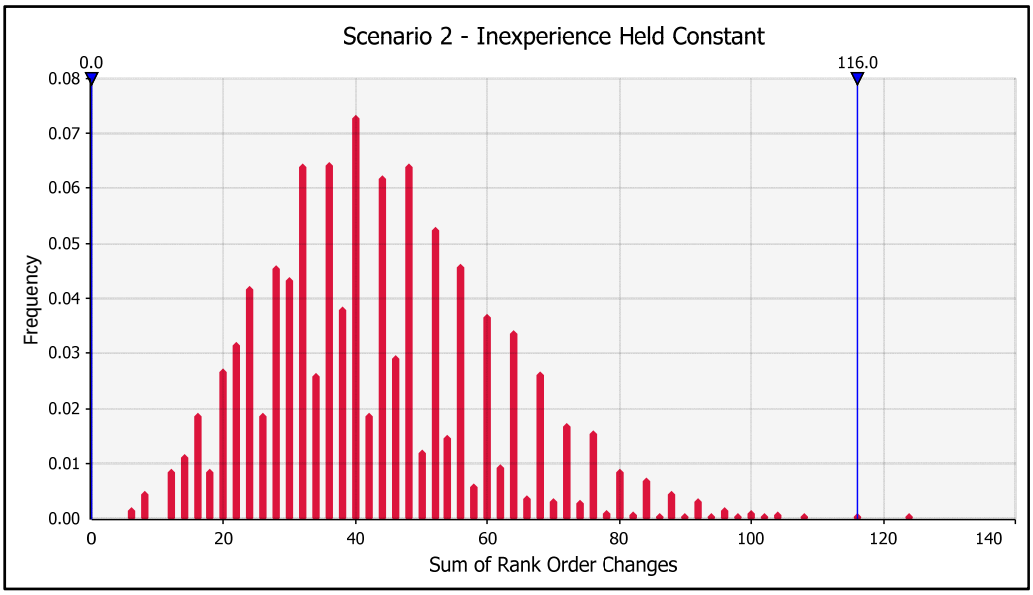


Figure 50. Scenario 2 with Inexperienced Personnel Held Constant

2. Scenario 2 with Experienced Personnel Removed

Although not as impactful, this form of analysis still produced a test statistic with a p-value less than .04682, indicating strong evidence against the null hypothesis and certain rejection if using the traditional 95% confidence region, as indicated by Figure 51. However, given that these results are now on the cusp of statistical significance, this scenario with experienced personnel removed further begs the question of how much value is brought to personnel with national level experience. Nevertheless, the personnel lacking experience did generally agree on their recommendations to the commander, and notably, these participants reside at seven different commands in five different geographical locations. Therefore, this scenario suggests that the framework has the ability to make information more "standardized" to users, mitigating the ambiguity of the qualitative information. This is evident as the choice of graphic CoA rankings have only four personnel out of 29 disagreeing with the choice of the recommended CoA and only five disagreeing with the second place choice. See Figure 52.

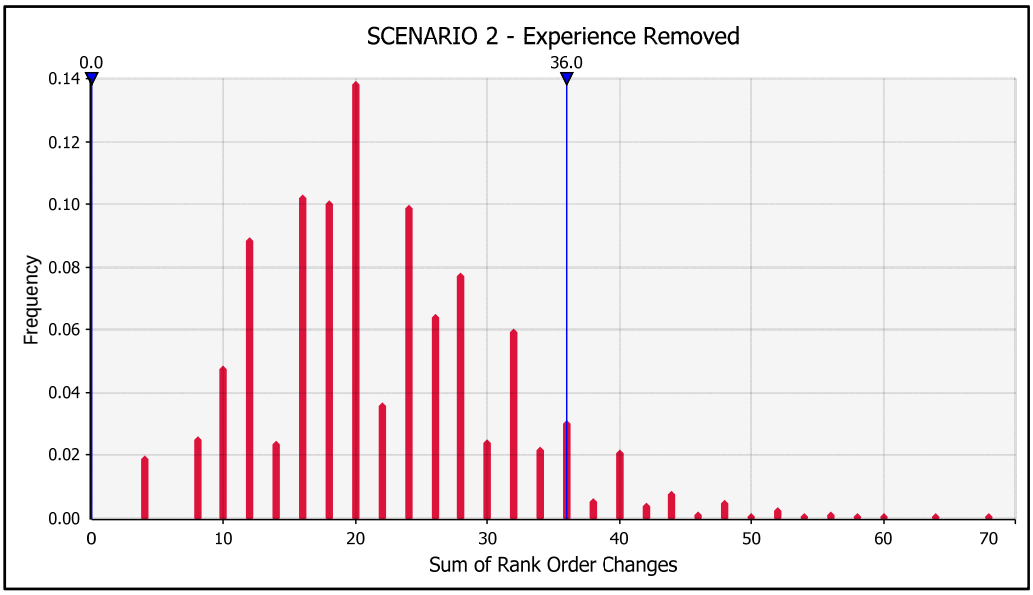


Figure 51. Scenario 2 with Experienced Personnel Removed

	SCENARIO 2 TOTALS					
	Written			Graphic Deciphered		
	1st	2nd	3rd	1st	2nd	3rd
A	17	6	6	25	0	4
B	4	6	19	2	5	22
C	8	17	4	2	24	3

SCENARIO 2 CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	8	-6	-2	16
B	-2	-1	3	6
C	-6	7	-1	14
	16	14	6	**36**

Figure 52. Scenario 2 Choices and Change with Experienced Personnel Removed

3. Scenario 2 with Inexperienced Personnel Removed

The removal of inexperienced personnel produced a test statistic with a p-value less than .0000435, indicating strong evidence against the null hypothesis and certain rejection if using the traditional 95% confidence region. Again, this scenario highlights

the utility of the proposed framework as an effective tool for personnel with and without national level experience. This analysis of Scenario 2 further reinforces the observed unintended consequence of value for experienced personnel. When inexperienced personnel are removed, this analysis still exceeds a 99% confidence level. See Figures 53 and 54. Here the shift in choice from written to graphic rankings nearly doubles in agreement concerning the recommended CoA. Of particular note, 58% of the inexperienced personnel in the last analysis of the scenario chose the same first preferred CoA. These participants then increased to 86% agreement in the first preferred CoA. Compare these percentages to those of the experienced personnel, who began at 48% agreement for the first preferred CoA and then increased to 87%.

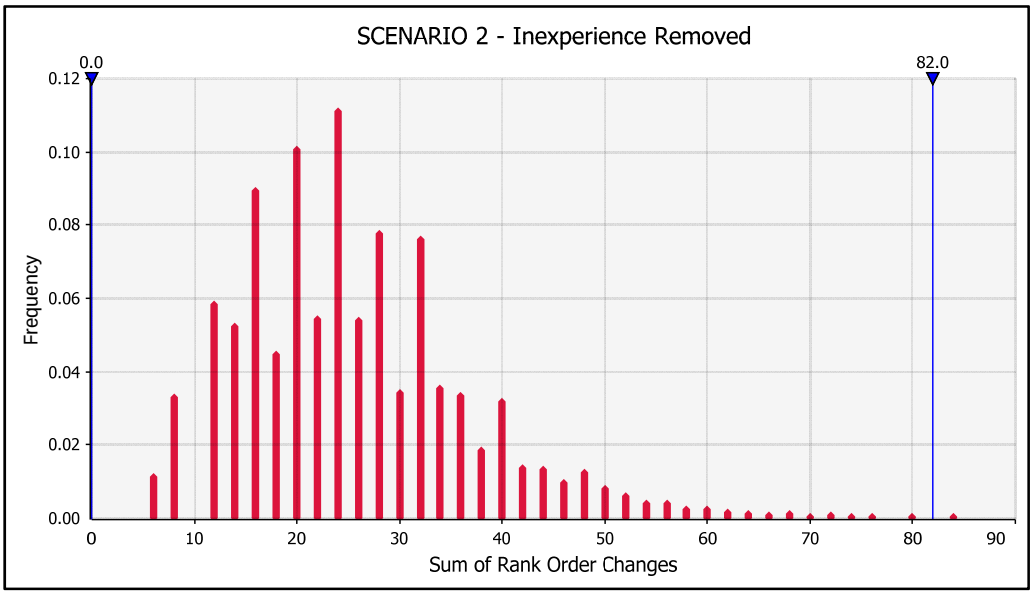


Figure 53. Scenario 2 with Inexperienced Personnel Removed

	SCENARIO 2 TOTALS					
	Written			Graphic Deciphered		
	1st	2nd	3rd	1st	2nd	3rd
A	15	8	8	27	1	3
B	2	12	17	3	1	27
C	14	11	6	1	29	1

SCENARIO 2 CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	12	-7	-5	24
B	1	-11	10	22
C	-13	18	-5	36
	26	36	20	82

Figure 54. Scenario 2 Choices and Change with Inexperienced Personnel Removed

4. Scenario 2 with USCYBERCOM Personnel Only

This analysis produced a test statistic with a p-value less than .005571, indicating strong evidence against the null hypothesis and certain rejection if using the traditional 95% confidence region. The test is statistically significant at a 99.4% confidence level, as depicted by the blue line in Figure 55. Analysis suggests that the USCYBERCOM participants evaluated CoAs the same as the personnel in the other analyses, based on the percentage of simulation outputs in Region 1. See Figure 56 for the choices and amount of change for Scenario 2. Please notice the split agreement of a recommended written CoA becoming a near unanimous decision, with only two of 14 disagreeing, for the recommended graphic CoA. Please also note in this analysis how the second and third recommended CoA rankings each had only one dissenter out of 14 participants.

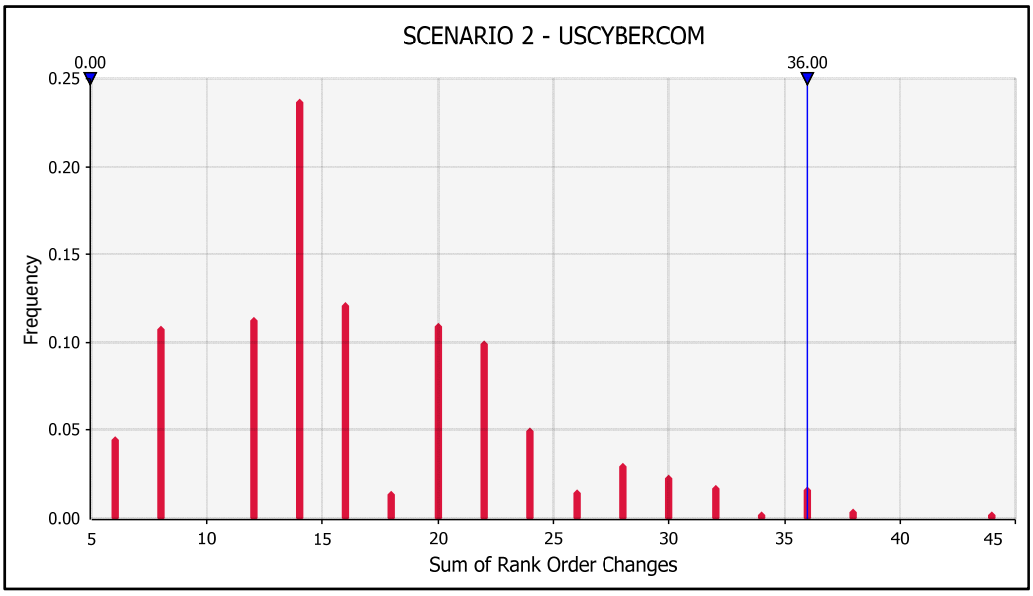


Figure 55. Scenario 2 with USCYBERCOM Personnel Only

	SCENARIO 2 TOTALS					
	Written			Graphic Deciphered		
	1st	2nd	3rd	1st	2nd	3rd
A	6	4	4	12	1	1
B	2	4	8	1	0	13
C	6	6	2	1	13	0

SCENARIO 2 CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	6	-3	-3	12
B	-1	-4	5	10
C	-5	7	-2	14
	12	14	10	36

Figure 56. Scenario 2 Choices and Change with USCYBERCOM Personnel Only

5. Scenario 2 Conclusions

As in previous scenarios, results suggest that participants use Region 1 of the graphics as a tool for assessing preference. This scenario further reinforces the hypothesis that a framework built on SME insights, that quantifies risk, and that presents results in a

graphical output can mitigate the inexperience of cyber planners when compared to those with national level experience. In the graphic CoAs, 86% of the inexperienced personnel chose the same first preferred CoA. This percentage is comparable to the 87% of the overall national level experienced planners and the 85% for the USCYBERCOM only planners.

E. SCENARIO 3

Scenario 3 presents the participants with another intelligence gathering operation. In this scenario, an adversarial government uses state-sponsored contracted companies to work on the government's behalf in an attempt to avoid attribution. Intelligence indicates that the contracted company has infiltrated the combatant command networks and exfiltrated documents that update the Theater Security Cooperation agreements, to include personnel and equipment movement schedules and locations.

The commander orders an intelligence operation to confirm or deny the presence of sensitive U.S. documents within the adversary's network. Confirmation in this operation is defined as the identification of the 400mb of the non-public portion of the Theater Security Agreement, which ranges in classification from SECRET to TOP SECRET. This operation will be considered a success if all 400mb of the sensitive portion of the document is identified, copied, and downloaded. Notably, OCO action is not authorized at this time.

Analysis of the command's networks indicates that at least two adversary entry points exist and that more are probable. As such, the commander places a value of 60% on avoiding attribution due to the sophistication of the adversary. As the adversary uses state-sponsored contracted companies for operations, the commander also wishes to avoid attribution to the company that works on the adversary's behalf. The remaining 40% of the commander's value comes from the intelligence potentially gained.

1. Scenario 3 with All Participants

Figure 57 illuminates how Scenario 3 with all participants produced a test statistic with a p-value less than .0049; indicating strong evidence against the null hypothesis and

certain rejection is using the traditional 95% confidence region. This analysis attained a 99.5% confidence level, as shown by the blue line in Figure 57. Participants in this scenario continued to examine and compare the percentage of simulation iterations in Region 1 of the graphics to rank order their preferences. See Figure 58 for the choices and amount of change between the written and graphic CoA choices. Please note the overwhelming majority of agreement of CoA B as the first choice in the graphic presentations when compared to the written CoAs. In this analysis, the level of agreement of CoA B being recommended increased 70% from the written to the graphic rankings.

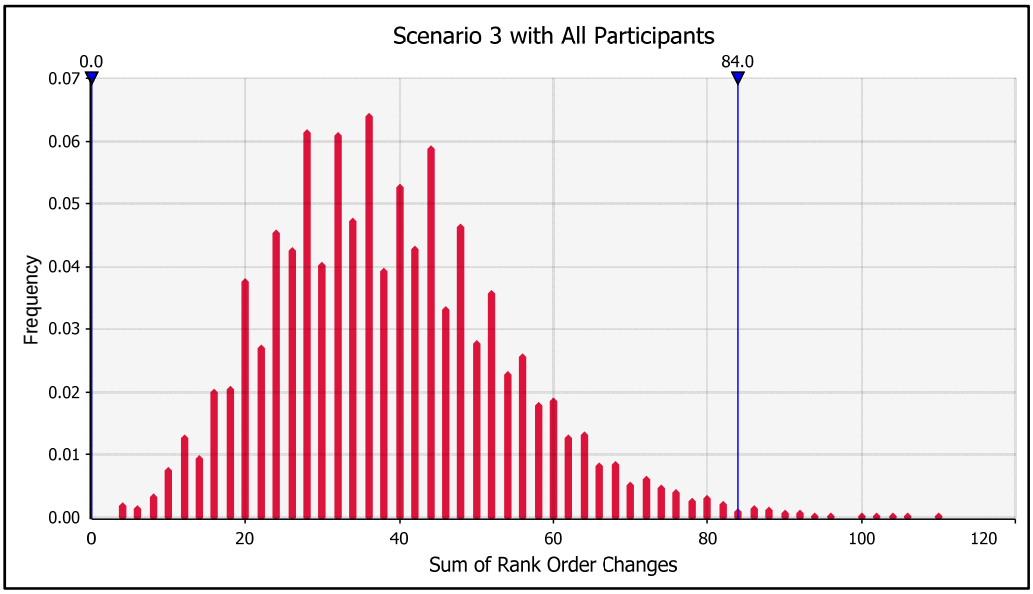


Figure 57. Scenario 3 with All Participants

SCENARIO 3 TOTALS					
Written			Graphic Deciphered		
1st	2nd	3rd	1st	2nd	3rd
26	19	15	8	31	21
24	22	14	41	17	2
10	19	31	11	12	37

SCENARIO 3 CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	-18	12	6	36
B	17	-5	-12	34
C	1	-7	6	14
	36	24	24	84

Figure 58. Scenario 3 Choices and Change for All Participants and Nothing Held Constant

a. Scenario 3 with All Participants and Experienced Personnel Held Constant

This analysis produced a test statistic with a p-value less than .0222, indicating strong evidence against the null hypothesis and certain rejection if using the traditional 95% confidence region, as depicted by the blue line in Figure 59. Analysis suggests that all the participants lacking national level experience evaluated CoAs based on the percentage of simulation outputs in Region 1—the region that satisfied both the cost and effectiveness requirements from the commander, ignoring Region 2. This region fulfills the effectiveness requirement of the commander, however, fails to meet the cost requirement. The staff may recommend a CoA that normally would not be the first choice given that it requires more resources, in this case, time. If the additional resources are attainable, the commander may choose this less than optimal CoA. This potential is outlined in the instructions for this scenario with the inclusion of the sentence "If this deadline cannot be met, the staff must inform the commander as soon as possible and provide a timeline of events."

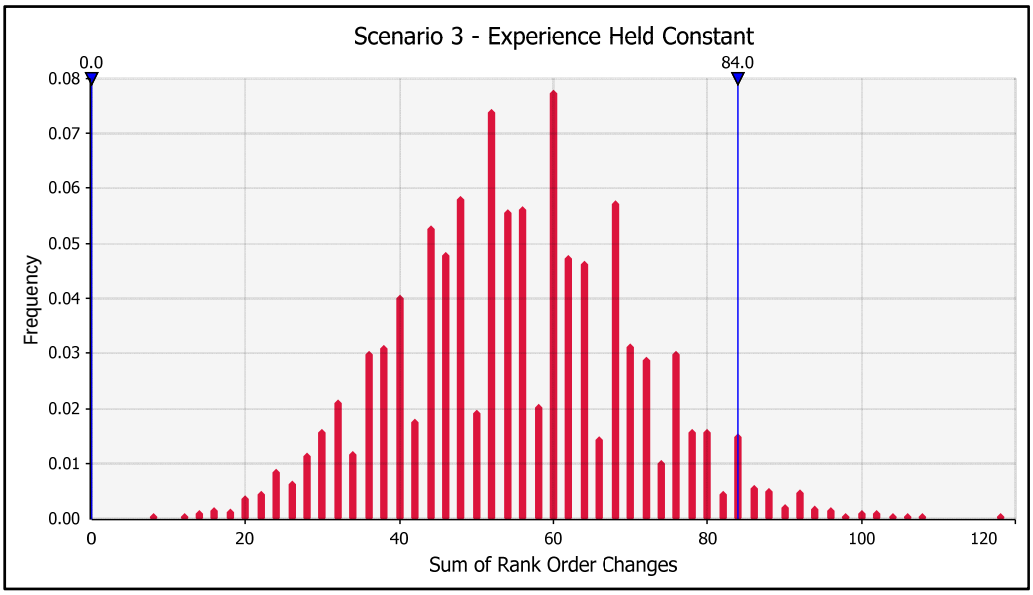


Figure 59. Scenario 3 with Experienced Personnel Held Constant

b. Scenario 3 with All Participants and Inexperienced Personnel Held Constant

Holding inexperienced personnel constant produced a test statistic with a p-value less than .0134; indicating strong evidence against the null hypothesis and certain rejection is using the traditional 95% confidence region. This analysis produced a 98.8 confidence interval. This analysis continues to reinforce previous examples for the value to personnel with national level experience. Coincidently, the amount of participant change in this analysis coincided with the last analysis. See Figure 60.

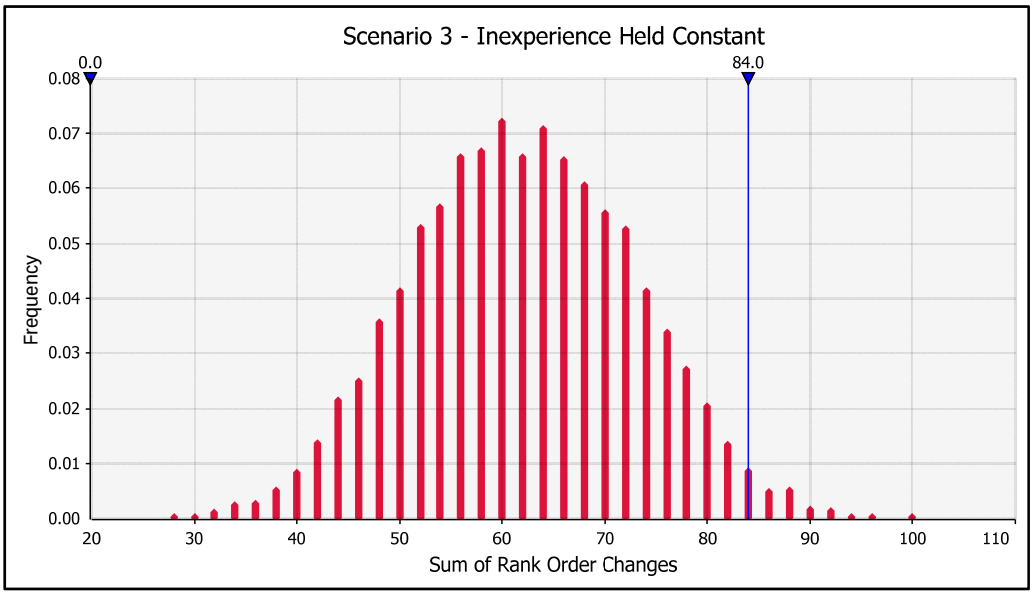


Figure 60. Scenario 3 with Inexperienced Personnel Held Constant

2. Scenario 3 with Experienced Personnel Removed

Analysis of Scenario 3 with experienced personnel removed produced a p-value less than .0218; indicating strong evidence against the null hypothesis and certain rejection if using the traditional 95% confidence region. This analysis resulted in a 98% confidence level as indicated with the blue line in Figure 61. This result continues to add validity to the value for planners lacking national level experience, thus supporting the hypothesis. As in the other analyses, this sample demonstrated increased agreement in CoA choice of the first preferred recommendation. See Figure 62. Please note how in this analysis, the inexperienced personnel had a split agreement between CoA A and CoA B in the written rankings and a clear decision, CoA B, emerged in the graphic rankings. Additionally, the decision to recommend CoA B also increased in agreement by 38% from the written rankings, more than doubling CoA C, the runner up for the recommendation.

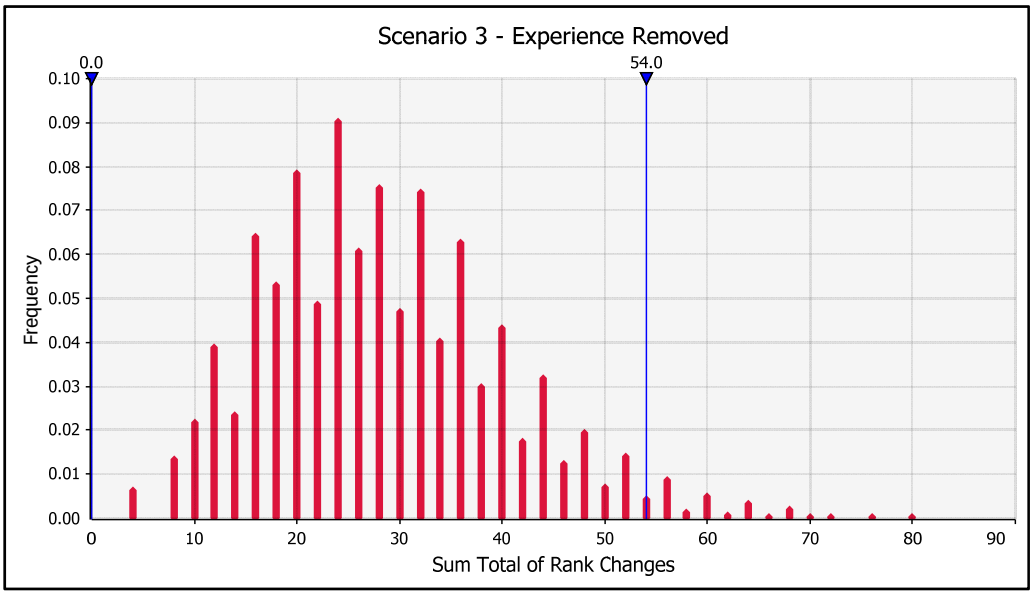


Figure 61. Scenario 3 with Experienced Personnel Removed

	SCENARIO 3 TOTALS					
	Written			Graphic Deciphered		
	1st	2nd	3rd	1st	2nd	3rd
A	13	7	9	3	15	11
B	13	8	8	18	10	1
C	3	14	12	8	4	17

SCENARIO 3 CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	-10	8	2	20
B	5	2	-7	14
C	5	-10	5	20
	20	20	14	54

Figure 62. Scenario 3 Choices and Change with Experienced Personnel Removed

3. Scenario 3 with Inexperienced Personnel Removed

This scenario analysis continues to advance the utility of the proposed framework as an effective tool for personnel both with and without national level experience by production of a test statistic with a p-value less than .0266. This value indicates strong

evidence against the null hypothesis and certain rejection is using the traditional 95% confidence region. This analysis of Scenario 3 further reinforces the observed unintended consequence of value to experienced personnel. When inexperienced personnel are removed, the analysis attains a 97.4% confidence level, as depicted by the blue line in Figure 63. Figure 64 illustrates the choices and changes for the experienced personnel comparing the written and graphic CoAs. In the written rankings, CoA B narrowly lost the recommended position to CoA A. In the graphic CoA rankings however, CoA A is the runner up to CoA B. Note how the level of agreement of CoA B as the recommended CoA doubles, besting CoA by a more than 400% difference.

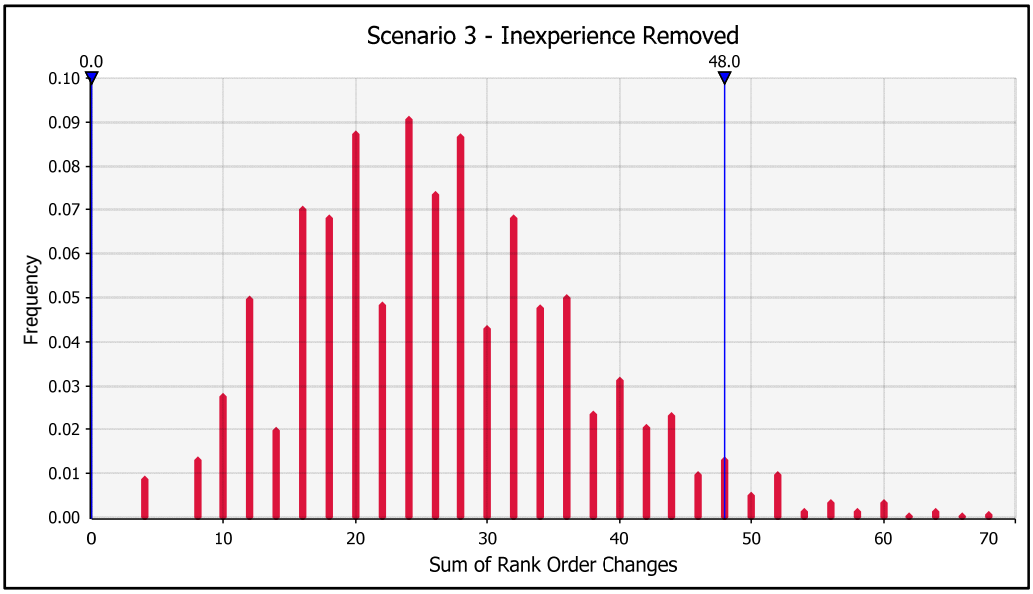


Figure 63. Scenario 3 with Inexperienced Personnel Removed

	SCENARIO 3 TOTALS					
	Written			Graphic Deciphered		
	1st	2nd	3rd	1st	2nd	3rd
A	13	12	6	5	16	10
B	11	14	6	23	7	1
C	7	5	19	3	8	20

SCENARIO 3 CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	-8	4	4	16
B	12	-7	-5	24
C	-4	3	1	8
	24	14	10	48

Figure 64. Scenario 3 Choices and Change with Inexperienced Personnel Removed

4. Scenario 3 with USCYBERCOM Personnel Only

This analysis produced a test statistic with a p-value of .24; constituting little or no evidence against the null hypothesis. For this level of analysis, Scenario 3 did not exceed the traditional 95% confidence interval and would not be statistically significant, as depicted by the blue line in Figure 65. Analysis does not suggest that the USCYBERCOM participants evaluated CoAs the same as the personnel in the other analyses, based on the percentage of simulation outputs in Region 1. In fact, no significant agreement of the CoA recommendations emerged from the USCYBERCOM planners in this scenario as evident by the lack of coalescence of opinion for any COA. See Figure 66 for the choices and amount of change for Scenario 3.

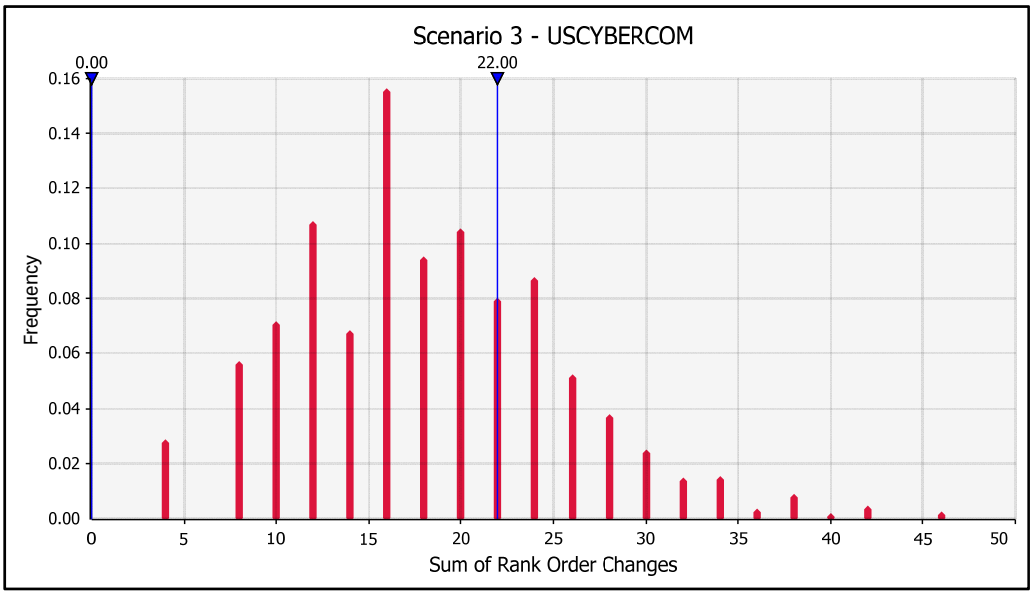


Figure 65. Scenario 3 with USCYBERCOM Personnel Only

	SCENARIO 3 TOTALS					
	Written			Graphic Deciphered		
	1st	2nd	3rd	1st	2nd	3rd
A	6	6	2	3	5	6
B	4	7	3	8	5	1
C	4	1	9	3	4	7

SCENARIO 3 CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	-3	-1	4	8
B	4	-2	-2	8
C	-1	3	-2	6
	8	6	8	22

Figure 66. Scenario 3 Choices and Change with USCYBERCOM Personnel Only

5. Scenario 3 Conclusions

As in previous scenarios, indications suggest that participants continue to use Region 1 of the graphics as a tool for assessing preference. In this scenario, the recommended graphic CoA had only a 12% predicted success from the simulation compared to 7.1% for the second choice and 2.3% for the third. In the graphic CoAs,

62% of the personnel lacking national level experience chose the same first preferred CoA. This result is comparable to the 74% of the overall national level experienced planners and the 57% for the USCYBERCOM only planners. Due to the groups' 33% increased aggregated agreement on CoA B being the recommended CoA, Scenario 3 again supports the hypothesis advanced by this research.

F. SCENARIO 4

In this scenario, the CCMD, in coordination with the CIA, plans to conduct OCO against a non-state actor's online magazine before being published in two weeks. This operation serves two purposes: to prevent disseminating bomb making information in the magazine and to facilitate the CIA identification of the magazine's readers. Due to other unrelated CIA activities within web forums, the commander has been directed to not bring attribution to U.S. or CIA efforts. Because of this directive, the commander values the outcomes of this operation at 40% for the destruction or denial to the online material, 30% for avoiding attribution, and 30% for avoiding compromise.

1. Scenario 4 with All Participants

This analysis produced a test statistic with a p-value of .667 constituting little or no evidence against the null hypothesis. As previously mentioned, this scenario tied for the least amount of change within the six scenarios. See Figure 67. As with Scenario 1A, written CoA rank preferences matched the graphic choices. In fact, both written and graphic choices were greatly agreed upon by all participants, thus the near-center blue line representing the participant choice and changes. See Figure 68.

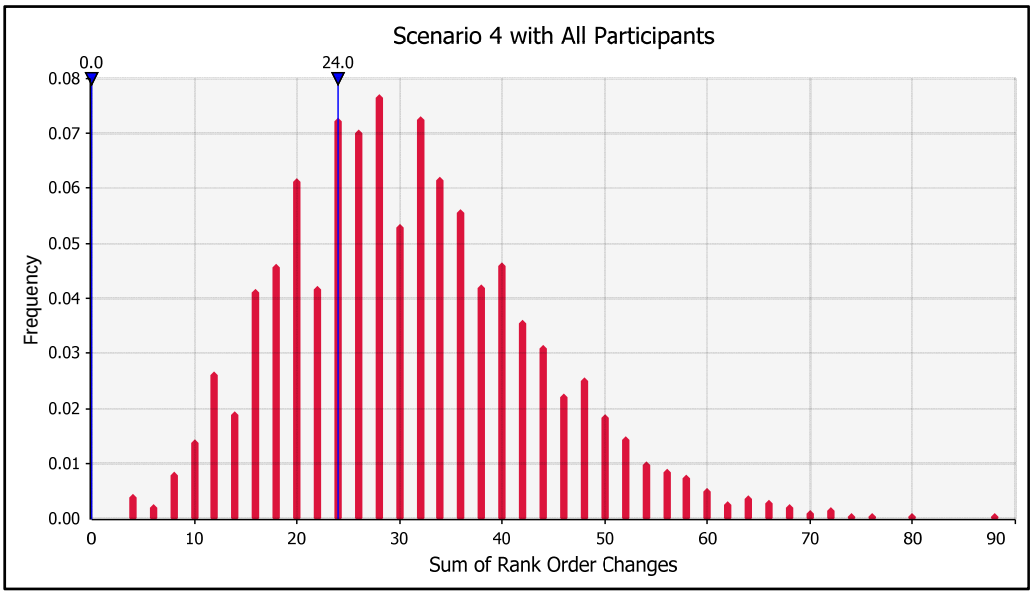


Figure 67. Scenario 4 with All Participants

SCENARIO 4 TOTALS					
Written			Graphic Deciphered		
1st	2nd	3rd	1st	2nd	3rd
15	36	9	13	38	9
39	12	9	41	15	4
6	12	42	6	7	47

SCENARIO 4 CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	-2	2	0	4
B	2	3	-5	10
C	0	-5	5	10
	4	10	10	24

Figure 68. Scenario 4 Choices and Change for All Participants and Nothing Held Constant

a. Scenario 4 with All Participants and Experienced Personnel Held Constant

Again, this analysis produced a test statistic with a p-value of .732 constituting little or no evidence against the null hypothesis. In this analysis, experienced personnel were held constant to attain a higher participant count; however, was not statistically

significant. This Scenario 4 analysis provided a dismal 27.6%, again as depicted by the blue line in Figure 69. Analysis suggests that all the participants lacking national level experience in this scenario evaluated CoAs based on the percentage of simulation outputs in Region 1, the region that satisfied the cost and effectiveness requirements from the commander.

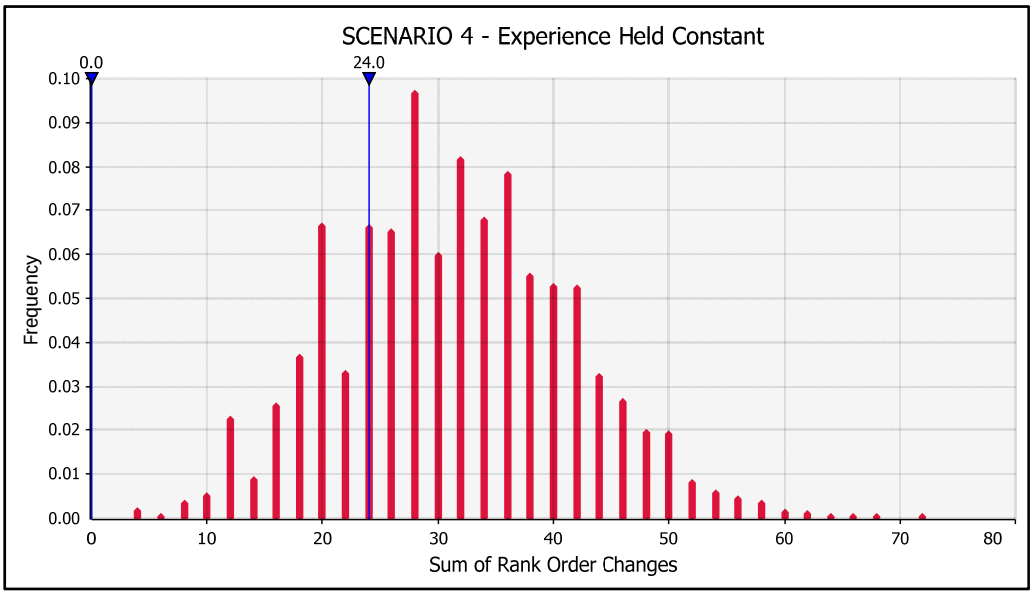


Figure 69. Scenario 4 with Experienced Personnel Held Constant

b. Scenario 4 with All Participants and Inexperienced Personnel Held Constant

Scenario 4 analysis with only personnel lacking national level experience produced a test statistic with a p-value of .573 constituting little or no evidence against the null hypothesis. This Scenario 4 analysis provided a 42.5% confidence level depicted by the blue line in Figure 70. Analysis suggests that all the participants lacking national level experience in this scenario evaluated CoAs based on the percentage of simulation outputs in Region 1, the region that satisfied the cost and effectiveness requirements from the commander.

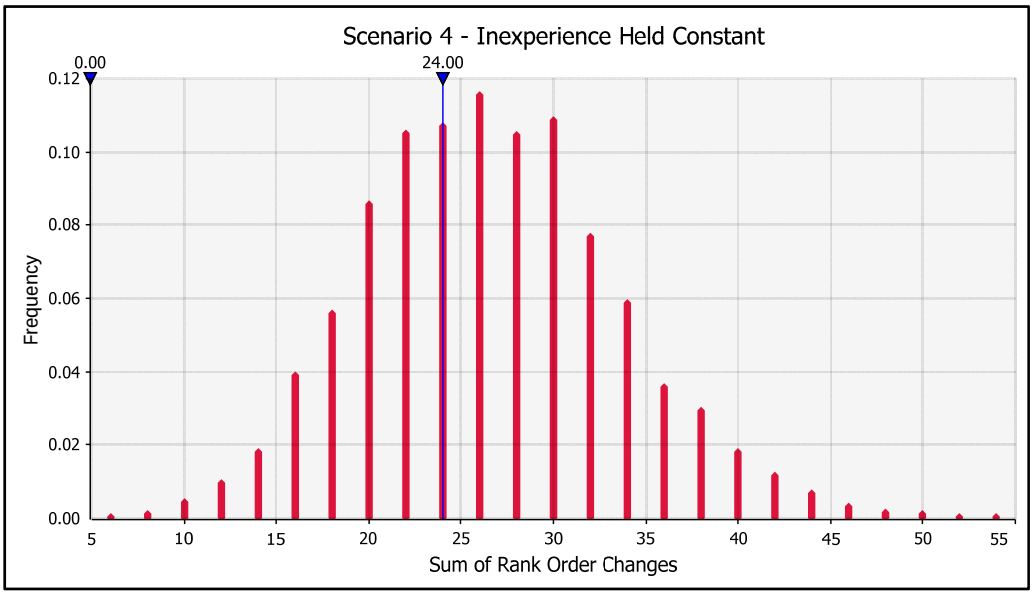


Figure 70. Scenario 4 with Inexperienced Personnel Held Constant

2. Scenario 4 with Experienced Personnel Removed

Scenario 4 analysis of only personnel lacking national level experience produced a test statistic with a p-value of .661 constituting little or no evidence against the null hypothesis. Scenario 4 analysis provided a 34.7% confidence level as depicted by the blue line in Figure 71. As previously mentioned, analysis suggests that all the participants lacking national level experience in this scenario evaluated CoAs based on the percentage of simulation outputs in Region 1. See Figure 72 for the choices and amount of change for this analysis of Scenario 4.

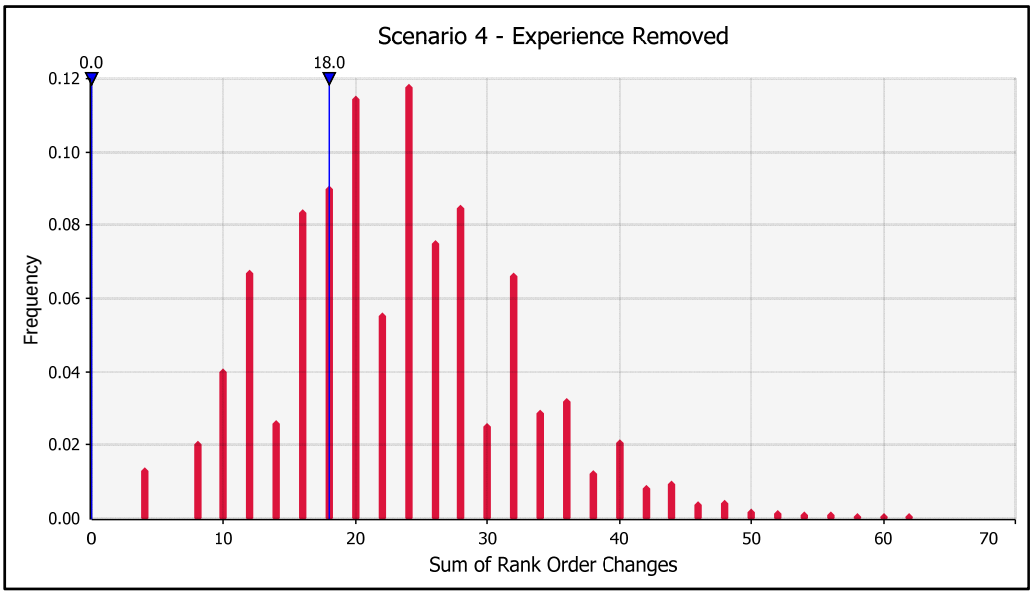


Figure 71. Scenario 4 with Experienced Personnel Removed

	SCENARIO 4 TOTALS					
	Written			Graphic Deciphered		
	1st	2nd	3rd	1st	2nd	3rd
A	9	17	3	5	17	7
B	16	8	5	19	9	1
C	4	4	21	5	3	21

	SCENARIO 4 CHANGE			
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	-4	0	4	8
B	3	1	-4	8
C	1	-1	0	2
	8	2	8	18

Figure 72. Scenario 4 Choices and Change with Experienced Personnel Removed

3. Scenario 4 with Inexperienced Personnel Removed

Scenario 4 analysis of only personnel with national level experience produced a test statistic with a p-value of .353 constituting little or no evidence against the null hypothesis. This analysis resulted in a 63.9% confidence level as depicted by the blue line

in Figure 73. As previously mentioned, analysis suggests that all the participants lacking national level experience in this scenario evaluated CoAs based on the percentage of simulation outputs in Region 1. See Figure 74 for the choices and amount of change for this analysis of Scenario 4.

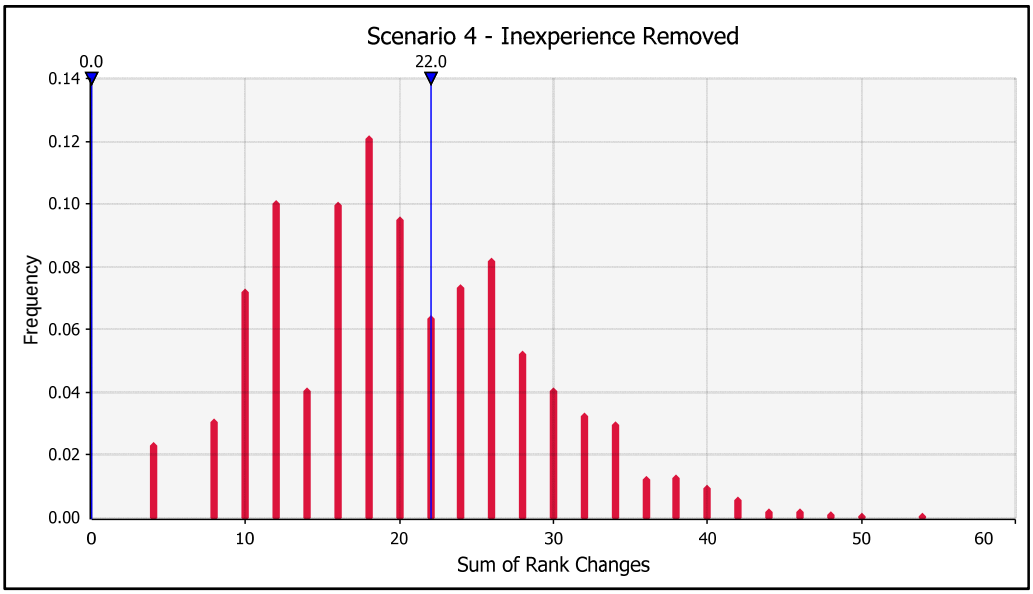


Figure 73. Scenario 4 with Inexperienced Personnel Removed

	SCENARIO 4 TOTALS					
	Written			Graphic Deciphered		
	1st	2nd	3rd	1st	2nd	3rd
A	6	19	6	8	21	2
B	23	4	4	22	6	3
C	2	8	21	1	4	26

SCENARIO 4 CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	2	2	-4	8
B	-1	2	-1	4
C	-1	-4	5	10
	4	8	10	22

Figure 74. Scenario 4 Choices and Change with Inexperienced Personnel Removed

4. Scenario 4 with USCYBERCOM Personnel Only

For this level of analysis, Scenario 4 produced a test statistic with a p-value of .37 constituting little or no evidence against the null hypothesis. This analysis resulted with a 61.8% confidence level as depicted by the blue line in Figure 75. As previously mentioned, analysis suggests that all the participants lacking national level experience in this scenario evaluated CoAs based on the percentage of simulation outputs in Region 1. See Figure 76 for the choices and amount of change for this analysis of Scenario 4.

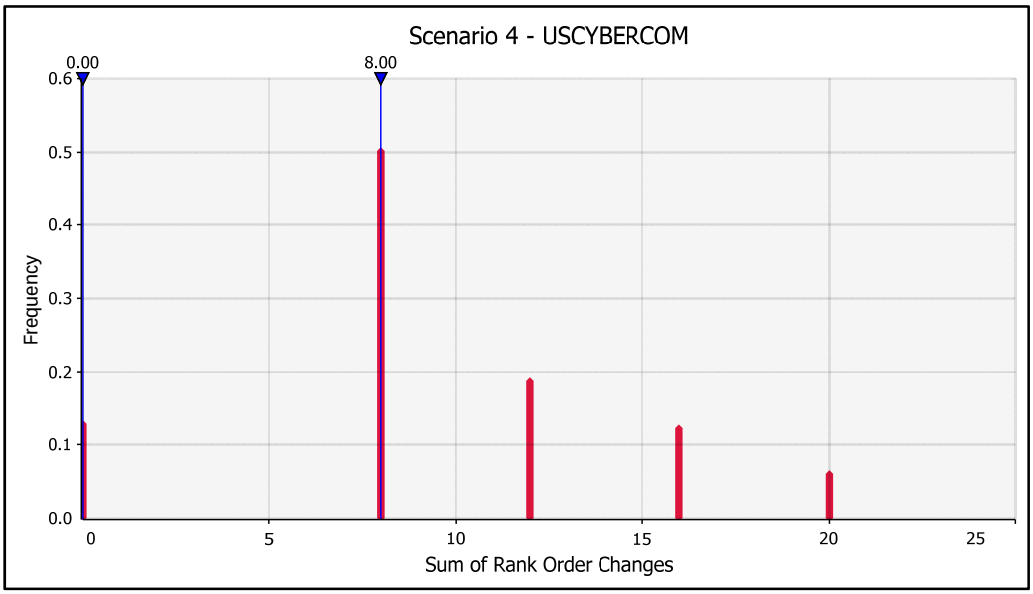


Figure 75. Scenario 4 with USCYBERCOM Personnel Only

	SCENARIO 4 TOTALS					
	Written			Graphic Deciphered		
	1st	2nd	3rd	1st	2nd	3rd
A	2	11	1	4	9	1
B	12	1	1	10	3	1
C	0	2	12	0	2	12

SCENARIO 4 CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	2	-2	0	4
B	-2	2	0	4
C	0	0	0	0
	4	4	0	8

Figure 76. Scenario 4 Choices and Change with USCYBERCOM Personnel Only

5. Scenario 4 Conclusions

Analysis of the outcomes of this scenario suggest two pieces of information were used to rank order CoAs. First, the graphic Region 1 prediction matches the written CoA ranking. This was not intentional on the part of the researcher. Second, the participant packets showed that participants indicated—using underlining, circling, and highlighting—key information in the written CoAs used for decision making. This information pertained to the likelihood of a capability being detected in the operation. The rankings given, from least likely to be detected to most likely, matched the written rankings and the graphical Region 1 prediction of success, from most likely to least. Thus, the participants were able to assume the proper ranking of CoAs most likely to based on the written format, suggesting that this scenario suffers from a design flaw.

G. SCENARIO 5

The last scenario for the participants portrays another OCO operation. An adversary of the United States uses a state-sponsored business to conduct operations on its behalf. The business in question has targeted U.S. and allied nation systems with malware for the purposes of intelligence gathering and denial of service. Additionally,

these attacks have been highly publicized in the media but not publicly attributed due to U.S. intelligence equities.

The planned OCO operation will demonstrate to both the adversary and the state-sponsored business that the United States is knowledgeable of the adversary's activities. However, U.S. cyber operations must prevent the adversary from discovering and attributing the network infrastructure used for these operations. For these reasons, the commander places 50% of the value of the operation on attaining destruction, 30% on avoiding detection, and 20% on avoiding attribution.

1. Scenario 5 with All Participants

Figure 77 illuminates how Scenario 5 with all participants produced a test statistic with a p-value less than .000004285; indicating strong evidence against the null hypothesis and certain rejection is using the traditional 95% confidence region. This analysis produced a confidence interval exceeding 99% as depicted by the blue line in Figure 77. To attain a 99% confidence level, 88 participant choice changes were required. These first population analyses of Scenario 5 garnered 114 participant changes. See Figure 78 for the choices and amount of change between the written and graphic CoA choices. Interestingly in this analysis, a dramatic shift from the written recommendation of CoA B to the graphic CoA occurred, suggesting that the graphics were more informative than the subjective words in the written choices.

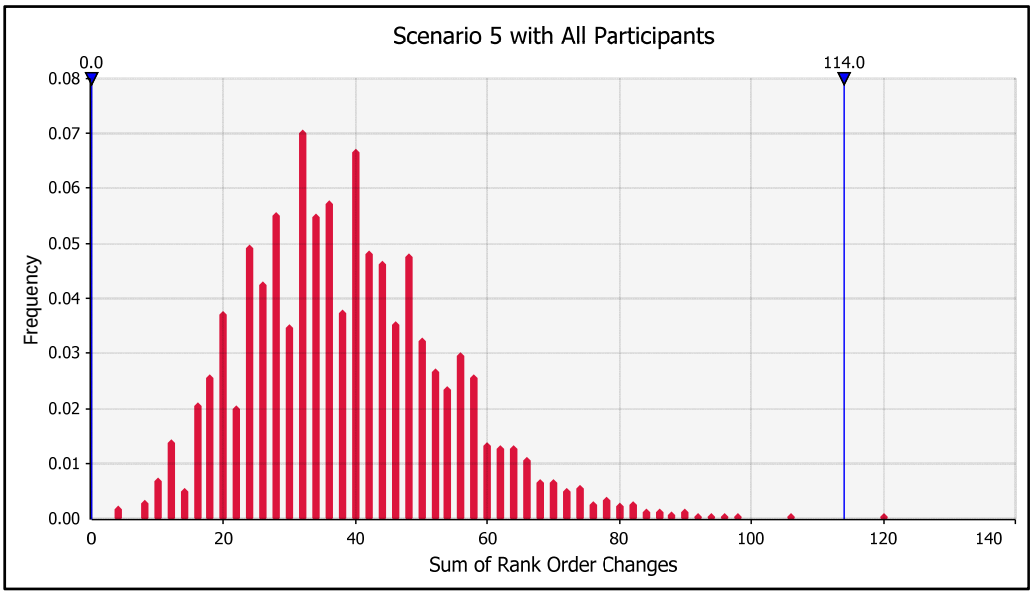


Figure 77. Scenario 5 with All Participants

SCENARIO 5 TOTALS					
Written			Graphic Deciphered		
1st	2nd	3rd	1st	2nd	3rd
10	34	16	30	20	10
35	15	10	7	28	25
15	11	34	23	12	25

SCENARIO 5 CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	20	-14	-6	40
B	-28	13	15	56
C	8	1	-9	18
	56	28	30	114

Figure 78. Scenario 5 Choices and Change for All Participants and Nothing Held Constant

a. Scenario 5 with All Participants and Experienced Personnel Held Constant

This form of analysis produced a test statistic with a p-value less than .0003; indicating strong evidence against the null hypothesis and certain rejection is using the traditional 95% confidence region. This analysis attained a 99.9% confidence level as depicted by the blue line in Figure 79. Analysis suggests that all the participants lacking national level experience in this scenario evaluated CoAs based on the percentage of simulation outputs in Region 1 the region that satisfied both the Cost and Effectiveness requirements from the commander. This scenario suggests that only Region 1 was considered as the last choice, CoA C, presented as CoA B to the participants, had a greater combined Region 1 and Region 2 prediction of success with 35.4%, of which, 13.4% resided in Region 1. Contrast that to the second choice of the participants with a combined Region 1 and Region 2 total of 14.7%, with 13.7% residing in Region 1.

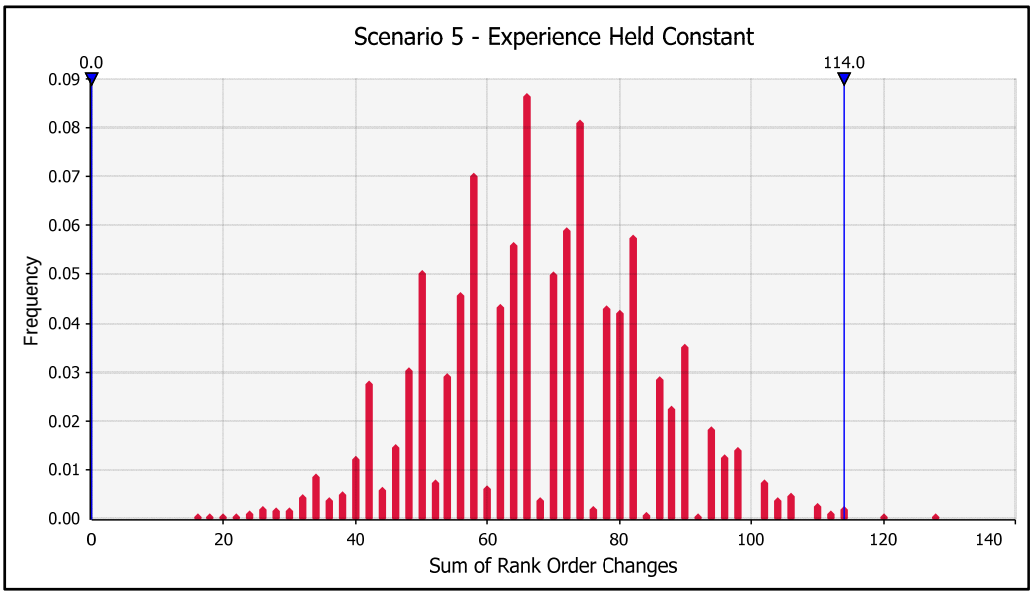


Figure 79. Scenario 5 with Experienced Personnel Held Constant

b. Scenario 5 with All Participants and Inexperienced Personnel Held Constant

This analysis produced a test statistic with a p-value less than .0005; indicating strong evidence against the null hypothesis and certain rejection is using the traditional 95% confidence region. This analysis continues to illuminate the examples in the previous scenario for the value to personnel with national level experience. In fact, this form of analysis far more exceeded the minimum for statistical significance when compared to the previous analysis of this scenario with a confidence level that exceeds 99.9%. See Figure 80.

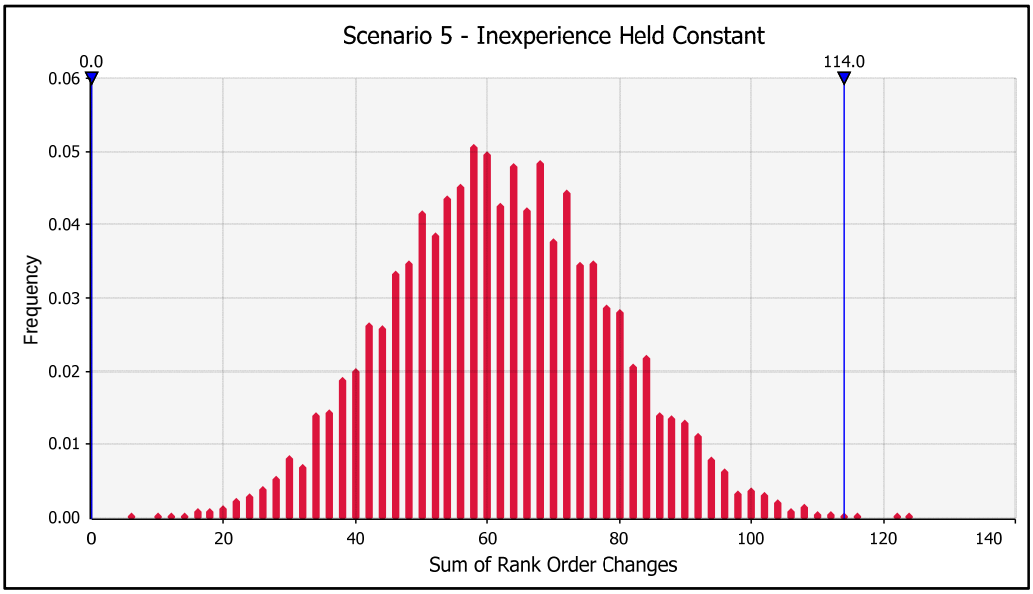


Figure 80. Scenario 5 with Inexperienced Personnel Held Constant

2. Scenario 5 with Experienced Personnel Removed

The analysis of Scenario 5 with experienced personnel removed produced a test statistic with a p-value less than .0062; indicating strong evidence against the null hypothesis and certain rejection is using the traditional 95% confidence region. This analysis of the scenario resulted in a 99.2% confidence level as indicated with the blue line in Figure 81. This result continues to add validity to the value for planners lacking national level experience. Although a split in consensus of the graphical CoA first choice

occurred, the two predominant graphical choices reflect the first and second mathematically probable choices. CoA A, presented to participants as CoA B possesses 13.4% in Region 1 and 22% in Region 2. Compare this to CoA A, presented as CoA C to participants with 26.1% in Region 1 and 0% in Region 2. This observation suggests that both Region 1 and Region 2 were considered by some personnel. See Figure 82. Interestingly again, the participants in this analysis completely away from the recommended CoA choice from the written CoAs, suggesting that the written format is not as informative as the graphic.

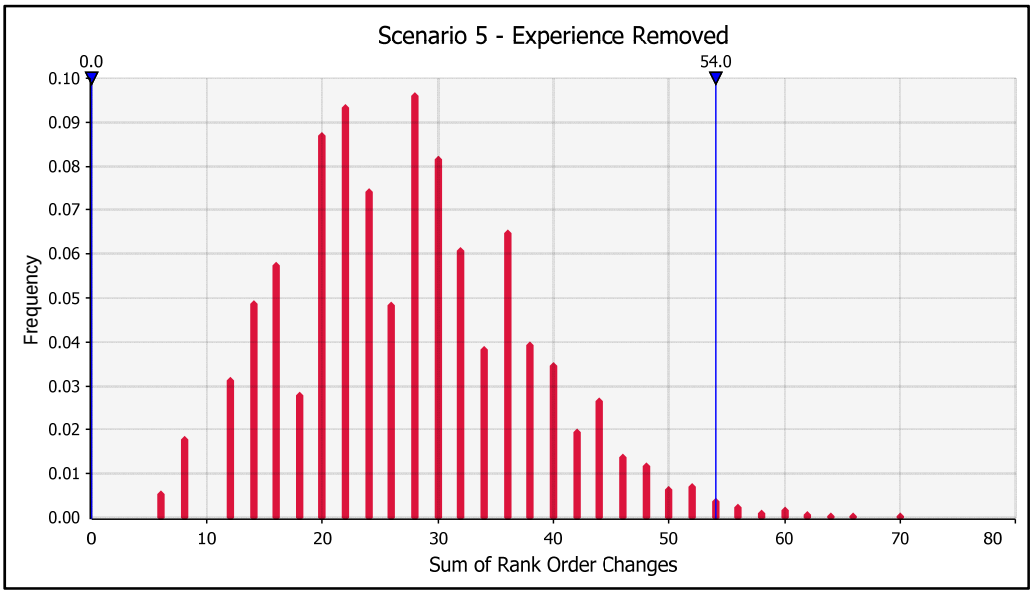


Figure 81. Scenario 5 with Experienced Personnel Removed

	SCENARIO 5 TOTALS					
	Written			Graphic Deciphered		
	1st	2nd	3rd	1st	2nd	3rd
A	6	16	7	12	9	8
B	17	6	6	4	13	12
C	6	7	16	13	7	9

SCENARIO 5 CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	6	-7	1	14
B	-13	7	6	26
C	7	0	-7	14
	26	14	14	54

Figure 82. Scenario 5 Choices and Change with Experienced Personnel Removed

3. Scenario 5 with Inexperienced Personnel Removed

Analysis with inexperienced personnel removed produced a test statistic with a p-value less than .0018; indicating strong evidence against the null hypothesis and certain rejection is using the traditional 95% confidence region. This scenario analysis continues to promote the unintended consequence of the proposed framework is an effective tool for personnel with national level experience. When inexperienced personnel are removed and the results are examined, this analysis attains a 97.4% confidence level as illuminated in Figure 83. Figure 84 illustrates the choices and changes for the experienced personnel. As with the last analysis, these participants, the personnel with national level experience, shifted completely away from the written CoA recommendation, shifting it to second place for the recommended CoA.

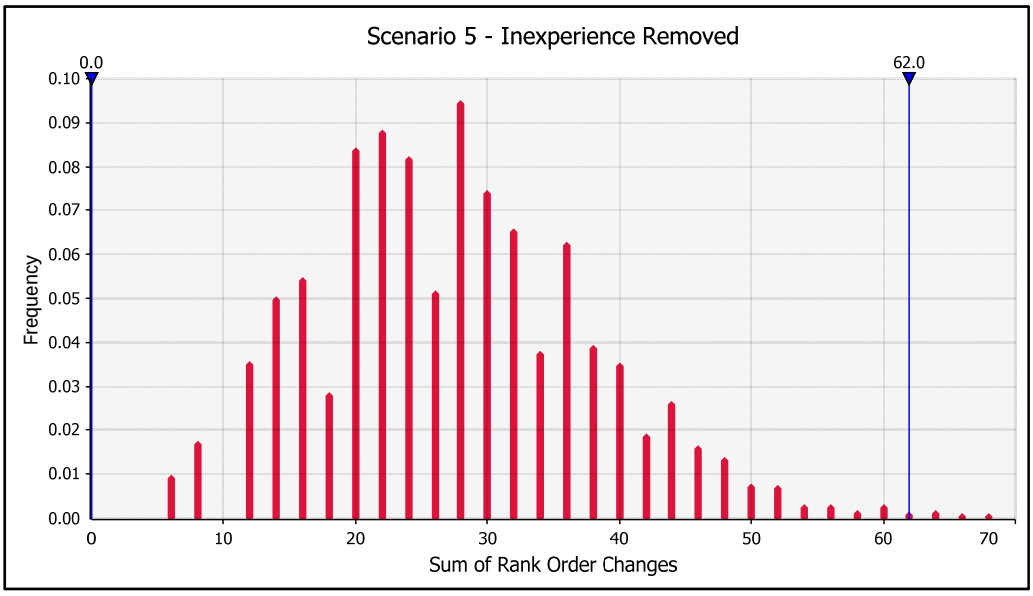


Figure 83. Scenario 5 with Inexperienced Personnel Removed

	SCENARIO 5 TOTALS					
	Written			Graphic Deciphered		
	1st	2nd	3rd	1st	2nd	3rd
A	4	18	9	18	11	2
B	18	9	4	3	15	13
C	9	4	18	10	5	16

	SCENARIO 5 CHANGE			
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	14	-7	-7	28
B	-15	6	9	30
C	1	1	-2	4
	30	14	18	62

Figure 84. Scenario 5 Choices and Change with Inexperienced Personnel Removed

4. Scenario 5 with USCYBERCOM Personnel Only

The last analysis resulted in a test statistic with a p-value of .506, constituting little or no evidence against the null hypothesis. For this level of analysis, Scenario 5 attained a 49.5% confidence level as depicted by the blue line in Figure 85. Analysis does

not suggest that the USCYBERCOM participants evaluated CoAs the same as the personnel in the other analyses, based on the percentage of simulation outputs in Region 1. In fact, no significant change of choice within ranks occurred. Changes made by the USCYBERCOM personnel reflected between rank changes of the same quantities, hence the lower amount of change. See Figure 86 for the choices and amount of change for this sample in Scenario 5. As with the previous two analyses in this scenario, the USCYBERCOM planners shifted CoA B from the written recommended CoA to the graphic second choice. This suggests that all there groups, the inexperienced, the experienced as a whole, and the USCYBERCOM planners all agree on CoA B should not be the recommended CoA for decision and action. This suggests that the outputs of this framework do not require national level experience and that both experienced and inexperienced personnel may benefit from it.

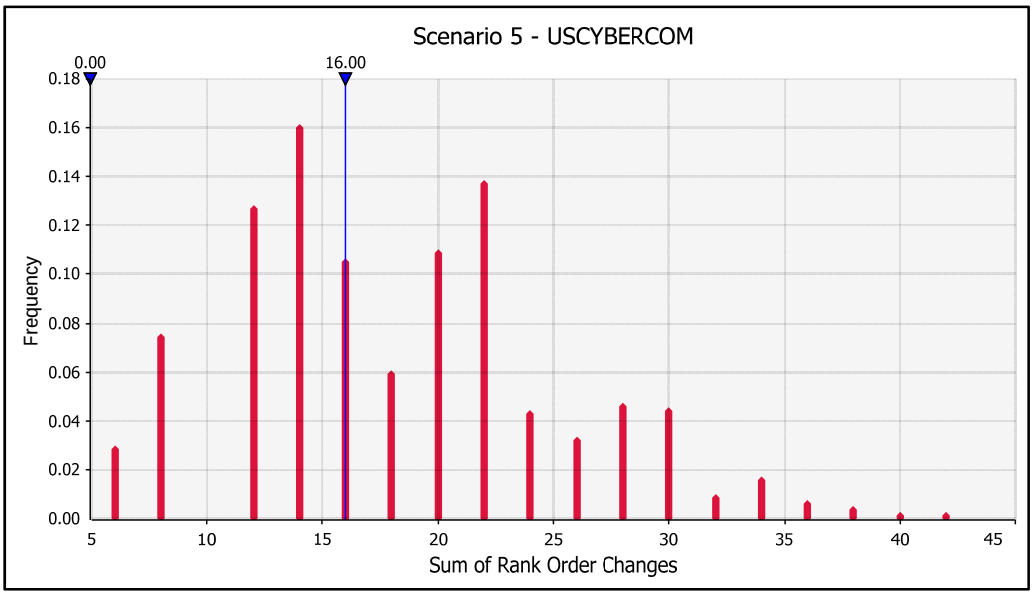


Figure 85. Scenario 5 with USCYBERCOM Personnel Only

	SCENARIO 5 TOTALS					
	Written			Graphic Deciphered		
	1st	2nd	3rd	1st	2nd	3rd
A	3	7	4	6	6	2
B	6	6	2	2	7	5
C	5	1	8	6	1	7

SCENARIO 5 CHANGE				
	Graphic Deciphered			
CHOICE	1st	2nd	3rd	
A	3	-1	-2	6
B	-4	1	3	8
C	1	0	-1	2
	8	2	6	16

Figure 86. Scenario 5 Choices and Change with USCYBERCOM Personnel Only

5. Scenario 5 Conclusions

This scenario suggests that participants use Region 1 and Region 2 of the graphics as a tool for assessing preference as observed in Scenario 1A. This method in which decision makers prioritize data for decision merits further research. In the graphic CoAs, 44% of the inexperienced personnel chose the same first preferred CoA. This is lower than the 58% of the overall national level experienced planners. Since the USCYBERCOM only planner analysis was not statistically significant and will not be compared. This result further suggests that the hypothesis is supported.

Please see Figure 87 for a consolidated account of analysis by levels of p-values for all scenarios. Individual analyses were grouped into one of four categories based on the p-value.

1. Strong rejection of the null hypothesis: p-values less than or equal to 0.05.
2. Possible rejection of the null hypothesis: p-values between 0.05 and 0.10.
3. Inconclusive evidence for the rejection of the null hypothesis: p-values between 0.10 and 0.15.
4. No evidence for the rejection of the null hypothesis: p-values in excess of 0.20.

	All Personnel	EXP Held Constant	INEX Held Constant	EXP Removed	INEX Removed	USCYBERCOM Planners Only
Scenario 1A	4	4	4	3	4	2
Scenario 1B	1	1	1	1	1	1
Scenario 2	1	1	1	1	1	1
Scenario 3	1	1	1	1	1	4
Scenario 4	4	4	4	4	4	4
Scenario 5	1	1	1	1	1	4
Number of analysis in Group 1:			22			
Number of analysis in Group 2:			1			
Number of analysis in Group 3:			1			
Number of analysis in Group 4:			12			

Figure 87. Consolidated Account of Analysis by p-value

THIS PAGE INTENTIONALLY LEFT BLANK

IX. ANALYSIS OF RESULTS

This research effort determined that 22 of the 36 analyses undertaken met or exceeded statistical significance, suggesting that this research supported the advanced hypothesis. This research succeeded in creating a tailor-made expression of risk based on the decision maker's preferences and desires.

A. TRENDS

The analysis uncovered three trends from the data. First, inexperienced personnel actually overcame their lack of national level experience and made decisions on par with experienced personnel. Next, using the framework, experienced personnel more often agreed on what CoA to recommend for decision and subsequent action. Third, the data suggests that Region 1 in the graphics was the primary determining factor for decision.

1. Inexperienced Personnel Overcome a Lack of Experience

The first trend identified was the goal of the research, namely to mitigate the lack of national level experience at organizations below the national level for OCO. Inexperienced personnel lack a thorough understanding of the environment, along with second and third order effects of operations. For this analysis, inexperienced offensive cyber planners made decisions on par with experienced offensive cyber planners as a whole, in addition to offensive planners currently working at USCYBERCOM.

Inexperienced personnel were more likely to agree on a recommended CoA in graphical form vice written form in four of six scenarios. The increase in aggregated agreement ranged from 18% in Scenario 4 to 47% in Scenario 2. Inexperienced personnel recorded a negative change in aggregated agreement, -11%, for the preferred CoA while the experienced group as a whole and the USCYBERCOM planners both recorded a 50% increase and 25% increase, respectively. Interestingly, the inexperienced personnel bested the experienced and USCYBERCOM personnel in Scenario 1B. In this scenario, the inexperienced personnel recorded a 33% increase in aggregated agreement on the

preferred CoA while the experienced personnel as a whole decreased by 28% and the USCYBERCOM planners decreased by an incredible 46%.

Scenario 5 was the other scenario in which the inexperienced personnel did not increase in aggregated agreement on the preferred CoA. In Scenario 5, the inexperienced personnel decreased in agreement by 23% and as a group, changed their preferred CoA selection from the written to the graphic. Conversely, the experienced personnel as a whole registered no change in the level of agreement but a change in CoA selection. The USCYBERCOM planners as a subset also had no change in their level of agreement but a change in CoA selection.

Additionally, data suggests that the graphics produced by this quantitative framework mitigate the lack of national level experience possessed by the inexperienced personnel. In the four scenarios that exceeded a 95% confidence interval, inexperienced personnel selected the same CoA in comparable numbers to the experienced personnel and the USCYBERCOM planners. For Scenario 1B, the inexperienced personnel chose CoA B at a rate of 55%, on par with 58% of the experienced personnel as a whole and 50% of the USCYBERCOM planners. Scenario 2 resulted in 86% of the inexperienced personnel choosing CoA A while 87% of the experienced personnel as a whole and 85% of the USCYBERCOM planners did also. Scenario 3 resulted in the USCYBERCOM planners not meeting or exceeding a 95% confidence interval; however, 62% of the inexperienced personnel selected CoA B while 74% of the experienced group did also. In Scenario 5, the USCYBERCOM planners again did not exceed a 95% confidence interval. However, 44% of the inexperienced personnel opted for CoA C as the primary choice while 58% of the experienced group chose CoA A. This analysis suggests that although the hypothesis is supported regarding mitigating the lack of national level expertise, the framework may also aid experienced personnel.

2. Value for Experienced Personnel

Experienced personnel exhibited greater aggregated agreement in selecting the first recommended CoA. As a whole, they increased in agreement in four scenarios. Most remarkably, in Scenario 2, they increased in aggregated agreement by 80% and in

Scenario 3 by 53%. Additionally, the USCYBERCOM planners in increased in aggregated agreement in three scenarios. Most notably, the agreement for CoA recommendation in Scenario 2 doubled. In Scenario 1A, the agreement increased by 50%. Additionally, a quantified framework may be of use in USCYBERCOM if offensive planners continue to rotate out of the organization at the current rate of two to three years.

USCYBERCOM is a military organization working at the national level of cyber operations, employing both military and civilian personnel. As such, the average military planner leaves this assignment in three years, sometimes two. It is also not unusual for planners to come from diverse backgrounds into USCYBERCOM and have no experience in cyber operations. Given this, the mean USCYBERCOM experience at the national level is 3.78 years, less than the five years needed for an expert status by this research effort and by many other mainstream researchers (Ericsson, Krampe, & Tesch-Romer, 1993; Ericsson, Prietula, & Cokely, 2007; Macnamara, Hambrick, & Oswald, 2014; Prietula & Simon, 1989). In fact, only five of the 14 USCYBERCOM planners attained the minimum of five years' experience to meet this standard. Three of the five personnel meeting the five-year standard to be considered an expert are civilian. This unexpected utility suggests that the framework is useful for national level personnel as well.

3. Use of Region 1 for Decision Making

As mentioned in the previous chapter, the data suggests that participants, both with and without national level experience, typically relied on Region 1 of the graphic CoAs for a rank preference decision. Recall that Region 1 is the quadrant of the graph that satisfies both the effectiveness and cost requirements of the commander. This suggestion was further reinforced by examination of the CoA ranking choices participants made. The selections of inexperienced, experienced, and USCYBERCOM personnel aligned to the highest Region 1 value in the CoAs for Scenarios 1B, 2, and 4. Additionally, the second and third CoA ranking aligned to the second and third highest

percentages of predicted success in Region 1 of the CoAs. Furthermore, the USCYBERCOM planners' choices aligned to the highest Region 1 value in Scenario 5.

In two of the scenarios, participants combined the predicted success scores of Regions 1 and 2 to create their rank order preferences. Region 2 meets the minimum effectiveness of the commander but goes past the maximum time allowed. In Scenarios 1A and 5, with the exception of the USCYBERCOM planners in Scenario 5, participant rankings aligned with the combined scores of Regions 1 and 2. The first preferred CoA aligned with the highest combined score, the second with the next highest, and so on. This suggested technique would focus on the effectiveness of a capability without regard to the cost in time, therefore, the participant only thinks about the end state, not the cost.

B. INTEGRATION WITH THE EXISTING LITERATURE

This research effort is unique, as it is the first to bridge the gaps between the areas of Command and Control, Decision Making, and Risk for offensive cyber operations. Past research attempts for these operations were limited to descriptions of operations (Denning, 2015; P. Denning & Denning, 2010; Grant, Burke, & van Heerden, 2012) and the life cycle of an offensive cyber capability (Axelrod & Iliev, 2014). Other cyber operations research primarily focused on defensive operations (Buckshaw, 2005; NIST, 2014). The closest comparison to this current research effort is past work for offensive kinetic operations. However, this analogy is not good enough. Cyber is a warfighting domain now, just as is Land, Air, Sea, and Space (Department of Defense, 2011b, 2013; Department of the Navy, 2014). As with the other warfighting domains, the cyber domain has unique aspects that differentiate it. Most notably, these aspects are speed, covertness of power projection, and geographic limitations.

Speed in the cyber domain is unlike that of the other domains. At the slowest, a cyber-capability transits a network at 2^{10} meters per second or 2/3 the speed of light. Even the fastest missile or bullet cannot compare to this speed. Covertness of power projection on a target also differentiates the cyber domain. Consider a kinetic attack. A network of early warning sensors encircle the globe. Air traffic controllers monitor the sky for anomalous aircraft. Satellites and other sensors recognize the seismic activity

from an intercontinental or orbital rocket. Cyber effects, however, do not appear until the appointed time or condition. Even then, the effect may not be detected or understood by the adversary, as shown by Stuxnet in Chapter 3. The only potential counterargument for cyber operations being analogous to kinetic operations is stealth technology. However, only a relatively small group of nations has the ability to launch a kinetic attack with a stealth platform. As such, these effects are geographically limited by operating range and the quantity of attack platforms. OCO, on the other hand, potentially has a wider reach across multiple attack vectors and targets simultaneously.

C. GENERALIZABILITY

The applicability of this research goes beyond military operations. This framework is applicable for any organization undertaking a novel operation and lacking the requisite in-house expertise to assess its risks. Organizations attempting to modify this framework would need information from multiple sources regarding past endeavors of the operation in question. Information would be attained from sources such as, in order of preference, actuarial data, historical data from similar ventures that will require analysis, or SMEs. Furthermore, an objective hierarchy would be required reflecting the concerns of the decision maker.

D. LIMITATIONS

The primary limitation of this research is the scenario construction of the survey packets. This research was limited to one opportunity to attain SME elicitations at each location. As such, scenarios were constructed, vetted, and adjusted at this university without validation from the SMEs. This led to two significant issues. First, Scenario 1A was found to have statistically similar choices when modeled with the SME elicitations, leading to no clear choice for recommendation within the graphic choices. Second, Scenario 4's language in the written CoAs correlated with the graphics modeled with the SME elicitations. Participant annotations suggest that key phrases regarding the probability of detection correlated with the probability of success measurements in Region 1 of the graphics.

E. FURTHER RESEARCH

Six areas of further research are recommended. First, researchers need to investigate how people view, rank, and incorporate data for decision making. Second, investigation is warranted in the use of piecewise linear models for eliciting decision maker values. Next, further research is needed in determining the most appropriate model for representing SME elicitations. Fourth, research is needed to better identify overconfidence in SME elicitations. Fifth, further investigation is needed in the descriptive model of decision maker choice behavior. Lastly, automation is needed to accelerate the process for implementation in cyberspace operations.

1. Information Ranking, Viewing, and Incorporating

Further research is needed to understand how participants rank order data sources and to determine under what conditions additional data should be incorporated into the participant decision analysis. Further research is also needed to understand how decision makers view the importance of the regions of the graphs, particularly Region 1 and Region 2. All six scenarios contained the following statement in the Commander's Intent, "If this deadline cannot be met, the staff must inform the commander as soon as possible and provide a timeline of events." Routinely Region 1 was the determining factor, the portion of the graph that met both the cost and effectiveness constraints immediately. This occurred even when a later execution date would provide greater effectiveness and thus change the order. Only two scenarios indicated participant use of Region 2.

Further research is also needed to understand what information is important to decision makers in cyberspace operations as the information used in the above scenarios is indicated by roughly half of the participants, both in annotation in the surveys or in the CoA choices. However, as previously mentioned, participants incorporated the data from Region 2 for two scenarios. This use of Region 2 illuminates a need for greater understanding of the decision makers' limits before more data is acquired.

Future research will need to understand how each region of the scatter diagram is employed and, to what importance, to the decision maker. For this, researchers will need to conduct iterative trials in which Region 1 is maximized. The next trial would use the

same data set, however, both Regions 1 and 2 would be maximized in order to minimize simulation iterations from appearing in Regions 3 and 4. Lastly, simulation outputs would be structured as to minimize Region 3 occurrence. By using the same data set in multiple trials, researchers will be able to ascertain the importance of each region and be able to identify how each region aligns to importance in the decision maker's mind.

Furthermore, another area for future research is dynamic variables. Dynamic variables are considerations of the decision maker that could quickly change, such as political risk. Researchers need to investigate the impact of these variables, the lifespan of the information, and the incorporation of these variables into the framework.

2. Piecewise Linear Model

Many commanders of cyber forces have limited availability to undertake the exercise of mid-value splitting as this dissertation advances. Following this constraint, research is needed on how a more expedited format of eliciting decision maker values would affect the simulation outputs. Following the research conducted by the RAND Corporation (Dreyer & Davis, 2005) an expedited method of seeking decision maker values exists—piecewise linear.

In this elicitation, two key questions are asked of the decision maker in lieu of the multiple iterations of questions used in mid-value splitting until indifference is attained. For situation in which "more is better" objective values are sought, the questions would be: "At what level, above which there is little or no additional value to you?" and "At what level, below which, is there little or no value for you. The first question seeks to determine what is "high enough" while the latter question determines what is "not enough." Once these two points are determined, a linear interpretation connects the two value assessments as shown in Figure 88.

Similarly, in situations for a "less is better" objective values are sought, the converses of the questions are used. The first question, "At what level, below which, is there little or no additional value?" seeks to assign a value to what the decision maker considers "low enough." The next question, "At what level, above which, there is no value for you?" seeks to assign the value for what the decision maker considers "too

much" or "too high." Again, these two points connect by linear interpretation as depicted in Figure 89.

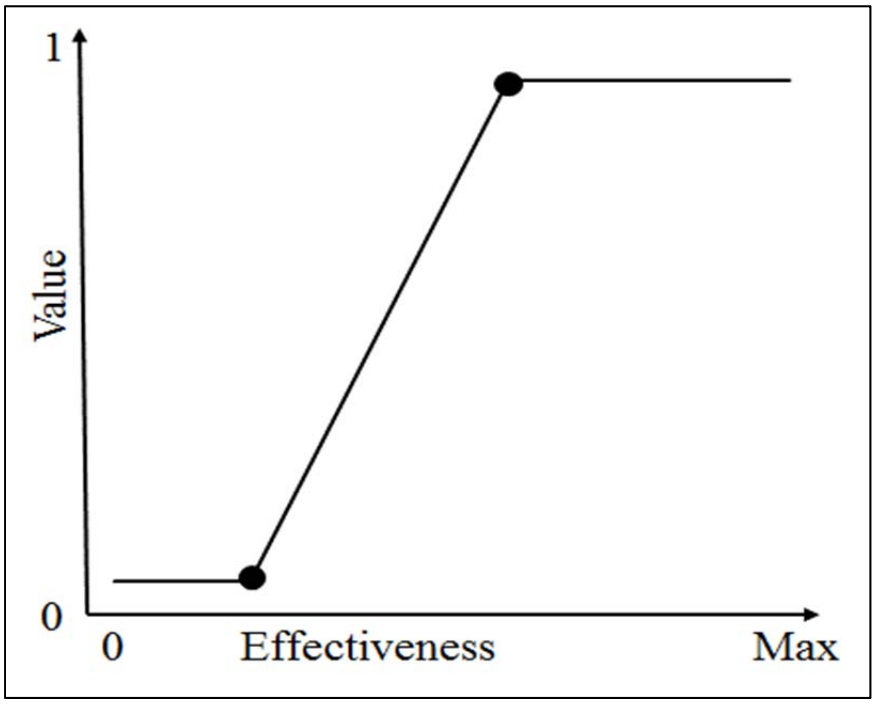


Figure 88. Example Piecewise Linear Elicitation of Decision Maker Values for a Maximization Objective

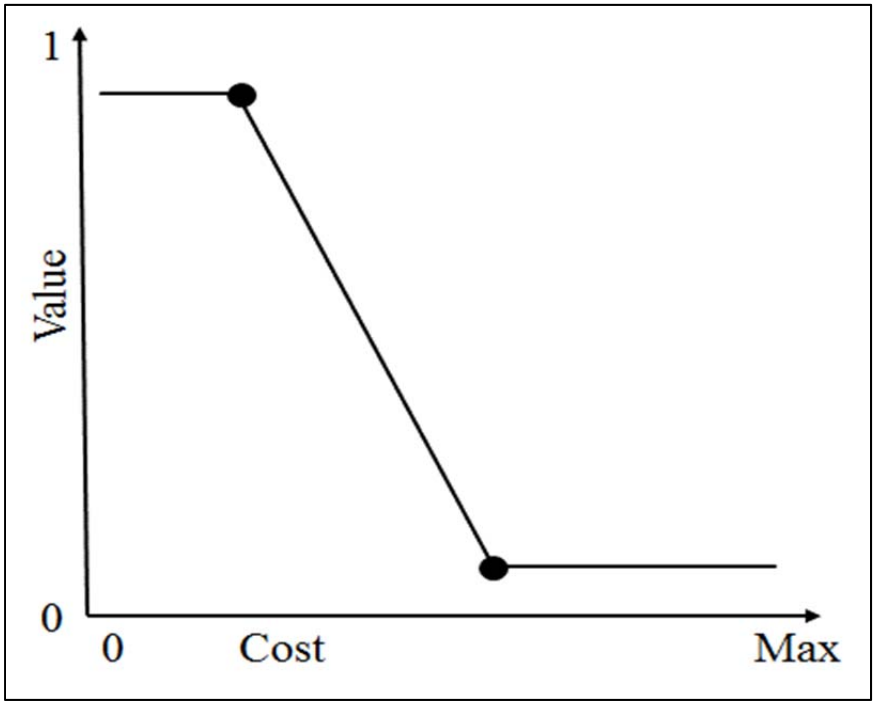


Figure 89. Example Piecewise Linear Elicitation of Decision Maker Values for a Minimization Objective

3. Potential Use of Other Models for Representing SME Assessments

This research effort used triangular distributions to model the upper value, most likely value, and the lower value to construct a 90% confidence interval in SME estimations. However, further research is needed to identify what is the optimal model for SME assessments. Future researchers may investigate the fit and utility of the beta, chi-squared, PERT, and the relative distributions. The latter two distributions have been used in the past to model expert opinions. However, the closeness of fit of these distributions in comparison to the truncated triangular, used in this dissertation, is unknown.

4. Overconfidence in SME Values

Multiple SME elicitations contained assessments extremely close together. For example, in Scenario 1A, one SME provided the assessment of .330, .420, and .500 to represent the lower value, the most likely value, and the upper value for their 90% confidence interval. Although precise, this begs the question of overconfidence on the

part of the SME when assessing the probability a fictitious cyberspace tool will achieve the required intelligence. Past research has alluded to experts being overconfident and further research is needed to investigate the potential of overconfidence in elicitations and how to calibrate SMEs for increased value to decision makers (Keren, 1987).

5. Descriptive Models of Decision Maker Choice Behavior

Evidence in the data collected for this research suggests that decision makers relied on the percentage of simulation iterations in Regions 1 and 2 to base the rank ordering of their answers. However, further research is needed to illuminate and understand a more descriptive model of decision maker choice behavior. Suggested research would involve using synthetic SME elicitations to create simulations. These simulations would be designed to present the decision maker with forced trade-offs. One potential simulation output would force the decision maker to evaluate CoAs that increase in effectiveness at the ramification of overrunning cost. In short, will the decision maker accept a higher than the maximum stated cost for an increase in effectiveness, even though the minimum effectiveness has already been achieved?

6. Framework Automation

The framework produced by this research still has manual components, namely decision maker preference value elicitation and modeling, along with SME elicitation and modeling. Decision maker preference elicitation could and would be as simple as an interactive webpage that asks iterative questions of the decision maker or their designated representative. Each response would be scored and recorded to determine the next question asked. This scoring and recording would provide the data points for the sigmoid functions used to model each objective of the hierarchy. Additionally, these sigmoid functions could then facilitate modeling of the decision maker values.

Intelligence personnel would characterize the adversary. This characterization would then be validated both by SMEs and by the operations planners. SMEs in this use are experts for the area or adversary that is the focus of the operation. SMEs should not be consulted if they lack expertise for the target of the operation in order to attain data

that are more relevant. Operations planners, in consultation with operators who would conduct the missions, would nominate capabilities for the operation.

SMEs would be sent an alert, most likely by email, with a historical account of events leading to the current situation, the commander's intent and endstate of the operation, and a no later than time for response. Complementing this automation effort would be another interactive webpage, the link for which would be in the alert that SMEs would use for elicitations. Again, questions of SMEs regarding attainment of specific objectives would be scored and recorded, using the three values, allowing for the creation of each SME's probability distribution. Additionally, the collective SMEs probability distributions and values would automatically update simulation models in a quick manner, allowing for rapid recommendations.

Upon reaching the desired amount of SME elicitations or at the end of the elicitation period, the simulation is ran to provide the planners graphical outputs for the decision maker to consider. Upon receiving the briefing on CoAs, the decision maker may refine guidance or their value models if none of the CoA are satisfactory. This process would then repeat until the decision maker is satisfied.

F. CONCLUSIONS

This research effort began with the assertion that current risk methodologies were ineffective for assessing risks in offensive cyber operations. That the current risk methods used subjective qualitative measures of risk that rely on an individual's knowledge and expertise to interpret risk levels and severity of impacts. However, these interpretations of risk levels are inconsistent across individuals due to cognitive frames of reference such as biases and heuristics. The problem of consensus for interpreting levels of risk intensifies when groups attempt to make a decision. Overconfidence or overestimation of the risks by the decision makers compounds the situation. In totality, decision makers in cyber operations are ill equipped to assess the risks of the operations they command.

This research effort set out to test the hypothesis that a quantifiable framework could mitigate the lack of national level expertise for offensive cyber operations at the CCMDs. The outcome is a highly effective framework that considers the operational

desires, risk tolerances, and personal values for individual decision makers. This framework uses insights of SME expertise to give a more complete and unbiased view of the probability of success in terms of mission effectiveness and the predicted costs. Not only did this research support the hypothesis, but it also has its own utility for experienced personnel in organizations below the national level and the current USCYBERCOM planners.

APPENDIX A. NSA PREPUBLICATION EVALUATION

From: Kappes, Paul D.
To: "Mike Klipstein"
Subject: RE: Dissertation Prepublication Review
Date: Thursday, January 5, 2017 6:36:56 AM

Good Morning MAJ Klipstein:

The standard statement refers to your non-disclosure agreement's lifelong obligation to submit for prepublication review that applies only to NSA- or IC-related information that has been gained solely through your NSA affiliation. Most publicly available information, and all information that has nothing to do with NSA or the IC in general, or your specific duties at NSA, is not subject to prepublication review. Please note that official NSA-related information appearing in the public domain should not be automatically considered UNCLASSIFIED and approved for public release unless an authorized disclosure of the information has been made (e.g. NSA-related information appearing on the NSA.gov or "IC on the Record" websites). Please refer to NSA/CSS Policy 1-30 for additional guidance or direct email to "DL pre_pub (ALIAS) DC3."

Based on our telephone conversation and the text below, a prepublication is not required as the information "has nothing to do with NSA or the IC in general."

Regards,
Paul

Paul Kappes
Information Security Policy Office
Office: (443) 654-4596
Fax: (240) 373-9275
E-mail addresses: pdkappe@nsa.gov

The information in this E-mail message including any attachments is intended only for the use of the individual(s) named above. If you, the reader of this message, are not the intended recipient, you are hereby notified that you should not further disseminate, distribute, or forward this E-mail message. If you have received this E-mail message in error, please notify the sender.

-----Original Message-----
From: Mike Klipstein [mailto:mklipste@nps.edu]
Sent: Wednesday, January 04, 2017 4:03 PM
To: Kappes, Paul D. <pdkappe@nsa.gov>
Subject: Dissertation Prepublication Review

Hello sir. My name is MAJ Michael Klipstein and I am the person with whom you recently today had a telephone conversation with. As a reminder, my dissertation is a method of quantifying risk for offensive cyber operations. I use open source information from the fields of Command and Control, Cognitive Psychology, Cyber Operations, and Multi-Criteria Decision Making. I have no content in my dissertation that reveals NSA information, proprietary or not. I did survey military members who currently work in NSA spaces. However, the identities of these people have been abstracted away and the information is now anonymous. Do I need to pass my dissertation to you for prepublication review?

Thank you for your time in this matter.

MAJ Mike Klipstein

Doctoral Candidate

Naval Postgraduate School

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. SME DEMOGRAPHICS

SME NUMBER	AGE	MIL/ CIV	YRS MIL?	ED LEVEL	WORK NATL CYBER?	NATL EXP YRS	JNAC	JCAC	BCNOPC	JACWC	CYBER 200	CYBER 300	SNIP	CNODP
SM001	38	MIL	18	MS	YES	3	NO	YES	YES	NO	NO	NO	NO	NO
SM002	33	MIL	15	HS	YES	10	NO	NO	NO	NO	NO	NO	NO	NO
SM003	38	MIL	19	MS	YES	10	NO	NO	NO	NO	NO	NO	NO	NO
SM004	33	MIL	14	AA	YES	14	YES	YES	NO	NO	NO	NO	NO	NO
SM007	33	MIL	13	BS	YES	7	NO	NO	NO	NO	NO	NO	NO	NO
SM009	39	CIV	20	MS	YES	5	NO	NO	YES	NO	NO	NO	NO	NO
SM010	43	CIV	20	BS	YES	7	NO	NO	NO	NO	NO	NO	NO	NO
SM011	40	MIL	20	MS	YES	7	NO	NO	YES	YES	NO	NO	NO	NO
SM012	37	MIL	17	MS	YES	16	YES	YES	NO	NO	NO	NO	NO	NO
SM013	33	CIV	14	MS	YES	6	NO	NO	NO	NO	NO	NO	NO	NO
SM014	35	MIL	13	MS	YES	5	NO	NO	NO	NO	NO	NO	NO	NO
SM016	35	CIV	11	BS	YES	7	NO	NO	NO	NO	NO	NO	NO	NO
SM017	42	MIL	23	MS	YES	6	NO	NO	NO	NO	NO	NO	NO	NO
SM018	48	MIL	28	BS	YES	14	YES	NO	NO	NO	NO	NO	NO	NO
SM019	35	MIL	10	MS	YES	8	NO	NO	NO	NO	NO	NO	NO	NO
SM020	37	MIL	18	BA	YES	8	NO	NO	NO	NO	NO	NO	NO	NO
SM022	37	MIL	18	BA	YES	13	NO	YES	NO	NO	YES	NO	NO	NO
SM024	38	MIL	18	MS	YES	18	NO	YES	NO	NO	NO	NO	NO	NO
SM026	48	MIL	31	MS	YES	5	NO	NO	NO	NO	NO	NO	NO	NO
SM028	37	MIL	18	BS	YES	12	NO	YES	YES	NO	NO	NO	NO	NO
SM029	44	MIL	22	MS	YES	5	YES	NO	YES	NO	NO	NO	NO	NO
SM030	35	MIL	13	AA	YES	5	NO	NO	NO	YES	NO	NO	NO	NO
SM032	33	MIL	15	BA	YES	15	NO	YES	YES	NO	NO	NO	NO	NO
SM033	42	MIL	19	BS	YES	5	NO	NO	NO	YES	NO	NO	NO	NO
SM035	37	MIL	16	HS	YES	15	NO	NO	NO	YES	NO	NO	NO	NO
SM036	49	MIL	19	BA	YES	6	YES	YES	NO	YES	NO	NO	NO	YES
SM037	33	MIL	15	AA	YES	5	NO	YES	NO	NO	NO	NO	NO	NO
SM038	35	MIL	14	BS	YES	5	NO	NO	NO	NO	NO	NO	NO	NO
SM040	42	MIL	6	HS	YES	5	NO	YES	NO	NO	NO	NO	NO	NO
SM042	36	MIL	16	AA	YES	5	NO	NO	NO	NO	YES	YES	NO	NO
	AVG AGE	COUNT MIL	AVG MIL YRS	COUNT HS	COUNT NATL EXP	AVG NATL EXP	COUNT JNAC	COUNT JCAC	COUNT BCNOPC	COUNT JACWC	COUNT CYBER 200	COUNT CYBER 300	COUNT SNIP	COUNT CNODP
	38.1667	26	17.1	3	30	8.4	5	10	6	5	2	1	0	1

COUNT CIV	COUNT BS	COUNT BA	COUNT MA	COUNT MS	COUNT MBA	COUNT JD	COUNT PhD
4	7	4	0	10	0	0	0

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. SCENARIO DISTRIBUTION MATRIX

Scenario 1 (State Actor - CNE)

DM TRADEOFF	DM VALUES	ADVERSARY	UNCERTAINTY
Intelligence		Peer Nation w = 1	P(Destruction)
			P(Intelligence)
			P(Detection)
			P(Attribution|Detection)
			P(Compromise|Detection)
Destruction	More is Better		
Detection w = .6	Less is Better	Developed Nation	P(Destruction)
			P(Intelligence)
			P(Detection)
			P(Attribution|Detection)
			P(Compromise|Detection)
Attribution|Detection		3rd World Nation	P(Destruction)
			P(Intelligence)
			P(Detection)
			P(Attribution|Detection)
			P(Compromise|Detection)
Compromise|Detection			

Scenario 2 (Non-State Actor - CNE)

DM TRADEOFF	DM VALUES	ADVERSARY	UNCERTAINTY
Intelligence w = .5	More is Better	Peer Nation	P(Destruction)
			P(Intelligence)
			P(Detection)
			P(Attribution|Detection)
			P(Compromise|Detection)
Destruction			
Detection w = .5	Less is Better	Developed Nation	P(Destruction)
			P(Intelligence)
			P(Detection)
			P(Attribution|Detection)
			P(Compromise|Detection)
Attribution|Detection		3rd World Nation w = 1	P(Destruction)
			P(Intelligence)
			P(Detection)
			P(Attribution|Detection)
			P(Compromise|Detection)
Compromise|Detection			

Scenario 3 (Non-State Actor (State-Sponsored) - CNE)

DM TRADEOFF	DM VALUES	ADVERSARY	UNCERTAINTY
Intelligence w = .4	More is Better	Peer Nation w = 1	P(Destruction)
			P(Intelligence)
			P(Detection)
			P(Attribution|Detection)
			P(Compromise|Detection)
Destruction			
Detection w = .6	Less is Better	Developed Nation	P(Destruction)
			P(Intelligence)
			P(Detection)
			P(Attribution|Detection)
			P(Compromise|Detection)
Attribution|Detection		3rd World Nation	P(Destruction)
			P(Intelligence)
			P(Detection)
			P(Attribution|Detection)
			P(Compromise|Detection)
Compromise|Detection			

Scenario 4 (Non-State Actor - CNA)

DM TRADEOFF	DM VALUES	ADVERSARY	UNCERTAINTY
Intelligence		Peer Nation	P(Destruction)
			P(Intelligence)
			P(Detection)
			P(Attribution|Detection)
			P(Compromise|Detection)
Destruction w = .4	More is Better		
Detection		Developed Nation	P(Destruction)
			P(Intelligence)
			P(Detection)
			P(Attribution|Detection)
			P(Compromise|Detection)
Attribution|Detection w = .3	Less is Better	3rd World Nation w = 1	P(Destruction)
			P(Intelligence)
			P(Detection)
			P(Attribution|Detection)
			P(Compromise|Detection)
Compromise|Detection w = .3	Less is Better		

Scenario 5 (Non-State Actor (State-Sponsored) - CNA)

DM TRADEOFF	DM VALUES	ADVERSARY	UNCERTAINTY
Intelligence		Peer Nation	P(Destruction)
			P(Intelligence)
			P(Detection)
			P(Attribution|Detection)
			P(Compromise|Detection)
Destruction w = .5	More is Better		
Detection		Developed Nation w = 1	P(Destruction)
			P(Intelligence)
			P(Detection)
			P(Attribution|Detection)
			P(Compromise|Detection)
Attribution|Detection w = .2	Less is Better	3rd World Nation	P(Destruction)
			P(Intelligence)
			P(Detection)
			P(Attribution|Detection)
			P(Compromise|Detection)
Compromise|Detection			

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. SME ELICITATION SCORES

SCENARIO 1A																				
	COA 1						COA 2						COA 3							
	INTELLIGENCE			DETECTED			INTELLIGENCE			DETECTED			INTELLIGENCE			DETECTED				
SME NUMBER	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV		
SM001	0.200	0.500	0.700	0.600	0.700	0.800	0.200	0.300	0.400	0.400	0.500	0.800	0.700	0.800	0.900	0.600	0.800	0.900		
SM002	0.000	0.250	0.300	0.500	0.800	0.900	0.350	0.660	0.850	0.250	0.330	0.850	0.000	0.050	0.200	0.750	0.920	1.000		
SM003	0.410	0.540	0.700	0.500	0.600	0.700	0.400	0.500	0.650	0.350	0.530	0.700	0.300	0.430	0.600	0.300	0.440	0.630		
SM004	0.300	0.400	0.500	0.420	0.500	0.700	0.200	0.300	0.400	0.300	0.400	0.500	0.420	0.500	0.620	0.200	0.300	0.400		
SM007	0.700	0.900	1.000	0.500	0.730	1.000	0.700	0.900	1.000	0.100	0.200	0.300	0.700	0.900	1.000	0.850	0.900	1.000		
SM009	0.230	0.530	0.730	0.480	0.580	0.680	0.350	0.650	0.725	0.250	0.380	0.450	0.350	0.450	0.560	0.550	0.680	0.720		
SM010	0.750	0.800	0.850	0.400	0.500	0.700	0.670	0.700	0.730	0.050	0.100	0.200	0.760	0.800	0.900	0.650	0.750	0.860		
SM011	0.250	0.300	0.500	0.500	0.750	0.900	0.500	0.600	0.900	0.100	0.200	0.400	0.000	0.250	0.500	0.500	0.750	1.000		
SM012	0.500	0.900	1.000	0.500	0.550	0.700	0.300	0.400	0.450	0.500	0.600	0.700	0.600	0.700	0.800	0.200	0.300	0.350		
SM013	0.100	0.600	0.800	0.200	0.400	0.900	0.100	0.300	0.500	0.100	0.400	0.600	0.100	0.400	0.700	0.100	0.400	0.700		
SM014	0.500	0.750	0.850	0.400	0.500	0.750	0.300	0.400	0.700	0.050	0.200	0.250	0.700	0.800	0.950	0.500	0.800	0.950		
SM016	0.700	0.750	0.950	0.500	0.700	0.750	0.700	0.750	0.950	0.100	0.200	0.210	0.700	0.750	0.950	0.700	0.750	0.990		
SM017	0.750	0.800	0.900	0.250	0.350	0.400	0.800	0.850	0.950	0.000	0.150	0.200	0.800	0.850	0.950	0.150	0.400	0.410		
SM018	0.000	0.200	0.500	0.400	0.600	1.000	0.400	0.600	1.000	0.000	0.200	0.400	0.300	0.500	1.000	0.400	0.700	1.000		
SM019	0.000	0.250	0.500	0.650	0.820	1.000	0.750	0.000	1.000	0.010	0.050	0.250	0.000	0.250	0.400	0.650	0.800	0.900		
SM020	0.250	0.500	0.750	0.300	0.500	0.850	0.500	0.700	0.800	0.100	0.200	0.300	0.800	0.850	0.900	0.800	0.900	1.000		
SM022	0.300	0.400	0.550	0.500	0.700	0.800	0.600	0.700	0.800	0.200	0.300	0.500	0.600	0.700	0.850	0.750	0.800	0.850		
SM024	0.300	0.500	0.600	0.300	0.500	0.600	0.200	0.300	0.400	0.350	0.400	0.450	0.600	0.700	0.900	0.400	0.500	0.600		
SM026	0.250	0.350	0.480	0.700	0.800	0.900	0.600	0.700	0.800	0.300	0.400	0.500	0.800	0.900	0.950	0.100	0.200	0.300		
SM028	0.600	0.700	0.900	0.400	0.500	0.600	0.700	0.800	1.000	0.200	0.300	0.500	0.500	0.700	0.800	0.600	0.800	0.900		
SM029	0.450	0.650	0.850	0.200	0.600	0.900	0.250	0.500	0.700	0.150	0.400	0.550	0.500	0.800	0.950	0.550	0.750	0.950		
SM030	0.330	0.420	0.500	0.620	0.700	0.750	0.230	0.300	0.320	0.400	0.510	0.600	0.540	0.620	0.650	0.310	0.330	0.400		
SM032	0.700	0.800	0.900	0.400	0.500	0.600	0.800	0.900	1.000	0.200	0.300	0.400	0.800	0.900	1.000	0.400	0.500	0.600		
SM033	0.400	0.500	0.800	0.300	0.500	0.700	0.200	0.300	0.500	0.000	0.100	0.200	0.600	0.750	0.900	0.700	0.900	1.000		
SM035	0.800	0.900	1.000	0.300	0.400	0.600	0.300	0.500	0.700	0.300	0.500	0.700	0.700	0.800	1.000	0.500	0.700	0.900		
SM036	0.400	0.700	0.800	0.520	0.550	0.570	0.600	0.700	0.800	0.100	0.300	0.500	0.700	0.800	0.900	0.600	0.700	0.800		
SM037	0.300	0.400	0.700	0.600	0.800	0.900	0.600	0.700	0.800	0.200	0.300	0.500	0.500	0.700	0.800	0.600	0.700	0.800		
SM038	0.500	0.700	0.800	0.500	0.650	0.800	0.400	0.500	0.600	0.200	0.340	0.430	0.600	0.700	0.800	0.700	0.800	0.900		
SM040	0.100	0.250	0.300	0.750	0.850	1.000	0.750	0.850	0.950	0.000	0.200	0.500	0.000	0.250	0.300	0.750	0.900	1.000		
SM042	0.500	0.620	0.780	0.400	0.800	0.850	0.200	0.500	0.800	0.150	0.500	0.600	0.500	0.620	0.900	0.100	0.600	0.900		

	SCENARIO 1B																	
	COA 1						COA 2						COA 3					
	DAMAGE			ATTRIBUTION			DAMAGE			ATTRIBUTION			DAMAGE			ATTRIBUTION		
SME NUMBER	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV
SM001	0.500	0.600	0.700	0.700	0.800	0.900	0.700	0.800	0.900	0.700	0.800	0.900	0.200	0.300	0.400	0.700	0.800	0.900
SM002	0.000	0.300	0.550	0.000	0.400	0.500	0.700	0.900	0.950	0.000	0.100	0.250	0.660	0.900	0.950	0.400	0.660	0.950
SM003	0.200	0.310	0.350	0.600	0.740	0.830	0.630	0.750	0.840	0.200	0.300	0.400	0.510	0.630	0.720	0.350	0.450	0.550
SM004	0.540	0.680	0.800	0.300	0.400	0.500	0.500	0.600	0.700	0.600	0.700	0.800	0.600	0.700	0.800	0.700	0.800	0.900
SM007	0.400	0.500	0.600	0.400	0.500	0.600	0.700	0.920	0.990	0.000	0.100	0.200	0.150	0.250	0.990	0.100	0.250	0.400
SM009	0.325	0.430	0.560	0.610	0.730	0.820	0.670	0.750	0.850	0.340	0.440	0.520	0.640	0.770	0.860	0.460	0.540	0.630
SM010	0.450	0.500	0.600	0.200	0.250	0.300	0.600	0.700	0.800	0.070	0.100	0.150	0.830	0.850	0.870	0.200	0.300	0.400
SM011	0.000	0.500	0.750	0.750	0.900	0.990	0.700	0.900	0.950	0.100	0.250	0.400	0.200	0.330	0.400	0.800	0.900	0.950
SM012	0.800	0.900	1.000	0.600	0.700	1.000	0.800	0.900	1.000	0.500	0.600	0.700	0.800	0.900	1.000	0.600	0.700	0.900
SM013	0.100	0.600	0.700	0.300	0.500	0.800	0.100	0.600	0.700	0.300	0.500	0.800	0.100	0.500	0.700	0.500	0.700	0.900
SM014	0.250	0.500	0.650	0.250	0.350	0.550	0.750	0.800	0.950	0.200	0.300	0.500	0.700	0.750	0.850	0.150	0.250	0.350
SM016	0.997	0.998	0.999	0.300	0.750	0.990	0.997	0.998	0.999	0.001	0.200	0.400	0.997	0.998	0.999	0.300	0.450	0.600
SM017	0.250	0.300	0.350	0.400	0.600	0.700	0.750	0.850	0.900	0.700	0.750	0.900	0.200	0.250	0.300	0.800	0.850	0.950
SM018	0.500	0.800	1.000	0.200	0.500	0.800	0.500	0.700	1.000	0.400	0.700	0.900	0.300	0.600	0.900	0.200	0.500	0.800
SM019	0.000	0.100	0.250	0.800	0.950	1.000	0.800	0.900	1.000	0.750	0.900	1.000	0.000	0.250	0.500	0.600	0.750	1.000
SM020	0.500	0.600	0.800	0.500	0.600	0.700	0.850	0.920	1.000	0.650	0.750	0.900	0.900	0.950	1.000	0.100	0.150	0.200
SM022	0.200	0.300	0.400	0.200	0.400	0.600	0.700	0.800	0.900	0.500	0.600	0.750	0.700	0.800	0.900	0.300	0.500	0.700
SM024	0.400	0.700	0.900	0.100	0.200	0.500	0.700	0.800	0.900	0.080	0.100	0.140	0.700	0.800	0.900	0.100	0.200	0.600
SM026	0.400	0.500	0.600	0.500	0.600	0.700	0.500	0.600	0.700	0.750	0.850	0.950	0.770	0.870	0.970	0.400	0.500	0.600
SM028	0.600	0.700	1.000	0.300	0.400	0.500	0.800	0.900	1.000	0.000	0.100	0.300	0.800	0.900	1.000	0.600	0.700	0.900
SM029	0.500	0.600	0.800	0.300	0.500	0.750	0.600	0.750	0.950	0.050	0.400	0.600	0.350	0.500	0.650	0.650	0.850	0.950
SM030	0.200	0.220	0.240	0.330	0.400	0.450	0.630	0.700	0.720	0.400	0.500	0.600	0.530	0.550	0.620	0.440	0.520	0.550
SM032	0.500	0.600	0.700	0.500	0.600	0.700	0.800	0.900	1.000	0.000	0.100	0.200	0.800	0.900	1.000	0.700	0.800	0.900
SM033	0.100	0.400	0.600	0.500	0.800	1.000	0.600	0.800	0.900	0.100	0.200	0.400	0.500	0.800	1.000	0.400	0.700	0.900
SM035	0.400	0.700	0.800	0.400	0.500	0.700	0.700	0.800	1.000	0.600	0.700	0.800	0.600	0.700	0.800	0.600	0.700	0.800
SM036	0.400	0.600	0.800	0.600	0.700	0.800	0.700	0.800	0.900	0.100	0.300	0.500	0.500	0.700	0.900	0.400	0.500	0.600
SM037	0.300	0.400	0.600	0.200	0.300	0.400	0.600	0.700	0.800	0.400	0.500	0.600	0.500	0.600	0.700	0.500	0.600	0.700
SM038	0.700	0.800	0.900	0.600	0.700	0.800	0.600	0.700	0.800	0.700	0.800	0.900	0.700	0.800	0.900	0.500	0.600	0.700
SM040	0.100	0.200	0.350	0.000	0.050	0.200	0.100	0.300	0.500	0.700	0.950	1.000	0.050	0.150	0.200	0.000	0.200	0.300
SM042	0.500	0.740	0.880	0.400	0.500	0.700	0.550	0.600	0.800	0.300	0.400	0.500	0.600	0.800	0.900	0.740	0.800	0.860

	SCENARIO 2																	
	COA 1						COA 2						COA 3					
	INTELLIGENCE			DETECTED			INTELLIGENCE			DETECTED			INTELLIGENCE			DETECTED		
SME NUMBER	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV
SM001	0.400	0.600	0.700	0.200	0.300	0.400	0.400	0.600	0.700	0.600	0.700	0.800	0.300	0.400	0.500	0.400	0.500	0.600
SM002	0.000	0.050	0.100	0.000	0.050	0.150	0.000	0.200	0.600	0.400	0.660	0.950	0.000	0.250	0.800	0.250	0.300	0.400
SM003	0.320	0.440	0.530	0.200	0.330	0.430	0.340	0.520	0.630	0.340	0.520	0.600	0.540	0.650	0.750	0.240	0.350	0.450
SM004	0.600	0.700	0.800	0.300	0.400	0.500	0.500	0.600	0.700	0.700	0.800	0.900	0.600	0.700	0.800	0.400	0.500	0.600
SM007	0.100	0.300	0.400	0.100	0.240	0.350	0.200	0.400	0.500	0.500	0.600	0.700	0.700	0.850	0.900	0.350	0.450	0.650
SM009	0.670	0.760	0.840	0.270	0.370	0.460	0.580	0.660	0.740	0.370	0.470	0.540	0.580	0.680	0.780	0.260	0.380	0.470
SM010	0.500	0.600	0.650	0.075	0.100	0.150	0.700	0.750	0.800	0.400	0.600	0.700	0.760	0.800	0.900	0.250	0.300	0.400
SM011	0.600	0.750	0.900	0.100	0.250	0.350	0.400	0.500	0.650	0.400	0.500	0.600	0.700	0.800	0.900	0.000	0.200	0.400
SM012	0.800	0.900	1.000	0.300	0.400	0.450	0.500	0.900	1.000	0.300	0.400	0.500	0.600	0.700	0.800	0.200	0.500	0.600
SM013	0.300	0.600	0.900	0.100	0.300	0.500	0.300	0.600	0.800	0.400	0.700	0.800	0.200	0.500	0.900	0.500	0.700	0.900
SM014	0.350	0.500	0.600	0.250	0.350	0.600	0.400	0.500	0.650	0.350	0.450	0.650	0.500	0.650	0.800	0.150	0.250	0.400
SM016	0.500	0.501	1.000	0.100	0.101	0.109	0.500	0.600	0.750	0.200	0.400	0.600	0.997	0.998	0.999	0.200	0.500	0.550
SM017	0.100	0.300	0.500	0.000	0.050	0.150	0.000	0.150	0.200	0.400	0.500	0.750	0.650	0.800	0.900	0.000	0.050	0.100
SM018	0.300	0.500	0.800	0.000	0.300	0.600	0.400	0.600	0.900	0.600	0.700	0.800	0.500	0.800	0.900	0.000	0.200	0.400
SM019	0.250	0.600	0.750	0.000	0.100	0.330	0.000	0.250	0.400	0.300	0.500	0.600	0.200	0.450	0.700	0.200	0.350	0.500
SM020	0.600	0.700	0.850	0.100	0.150	0.200	0.350	0.500	0.600	0.400	0.500	0.700	0.500	0.670	0.850	0.200	0.250	0.400
SM022	0.250	0.400	0.550	0.550	0.650	0.750	0.300	0.400	0.500	0.650	0.750	0.850	0.500	0.600	0.800	0.400	0.600	0.800
SM024	0.000	0.100	0.300	0.210	0.300	0.400	0.700	0.800	1.000	0.300	0.500	0.700	0.500	0.600	0.700	0.000	0.100	0.200
SM026	0.550	0.650	0.750	0.400	0.500	0.600	0.700	0.800	0.900	0.300	0.400	0.500	0.550	0.650	0.750	0.250	0.350	0.450
SM028	0.800	0.900	1.000	0.000	0.100	0.200	0.200	0.300	0.500	0.700	0.800	1.000	0.700	0.800	1.000	0.200	0.300	0.500
SM029	0.330	0.550	0.780	0.050	0.300	0.600	0.150	0.450	0.650	0.200	0.500	0.800	0.450	0.680	0.930	0.200	0.430	0.650
SM030	0.500	0.530	0.600	0.120	0.150	0.220	0.340	0.420	0.500	0.350	0.400	0.420	0.430	0.510	0.540	0.250	0.300	0.420
SM032	0.800	0.900	1.000	0.000	0.100	0.200	0.500	0.600	0.700	0.300	0.400	0.500	0.400	0.500	0.600	0.200	0.300	0.400
SM033	0.300	0.500	0.700	0.000	0.100	0.300	0.700	0.800	0.900	0.300	0.400	0.500	0.700	0.800	0.900	0.100	0.250	0.400
SM035	0.700	0.800	0.900	0.600	0.700	0.800	0.300	0.600	0.800	0.600	0.700	0.900	0.500	0.600	0.800	0.600	0.700	0.900
SM036	0.300	0.400	0.500	0.200	0.300	0.400	0.400	0.500	0.600	3.000	0.400	0.500	0.400	0.600	0.800	0.200	0.300	0.400
SM037	0.400	0.500	0.600	0.100	0.200	0.300	0.500	0.700	0.800	0.500	0.600	0.700	0.500	0.700	0.800	0.400	0.500	0.600
SM038	0.400	0.600	0.800	0.300	0.600	0.800	0.600	0.700	0.800	0.100	0.800	0.900	0.600	0.700	0.800	0.700	0.800	0.900
SM040	0.000	0.050	0.200	0.000	0.050	0.300	0.000	0.250	0.400	0.750	0.800	1.000	0.400	0.650	0.800	0.250	0.400	0.500
SM042	0.500	0.600	0.630	0.050	0.300	0.350	0.550	0.700	0.800	0.400	0.500	0.800	0.600	0.700	0.800	0.300	0.500	0.880

	SCENARIO 3																	
	COA 1						COA 2						COA 3					
	INTELLIGENCE			ATTRIBUTION			INTELLIGENCE			ATTRIBUTION			INTELLIGENCE			ATTRIBUTION		
SME NUMBER	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV
SM001	0.600	0.700	0.800	0.200	0.300	0.400	0.600	0.700	0.800	0.100	0.200	0.300	0.600	0.700	0.800	0.200	0.300	0.400
SM002	0.500	0.660	0.750	0.000	0.100	0.150	0.500	0.660	0.750	0.000	0.100	0.150	0.000	0.010	0.100	0.000	0.200	0.250
SM003	0.430	0.640	0.700	0.320	0.430	0.510	0.440	0.550	0.650	0.340	0.440	0.530	0.340	0.520	0.620	0.420	0.520	0.640
SM004	0.600	0.700	0.800	0.200	0.300	0.400	0.600	0.700	0.800	0.200	0.300	0.400	0.500	0.600	0.700	0.700	0.800	0.900
SM007	0.700	0.900	0.950	0.100	0.200	0.300	0.200	0.330	0.450	0.200	0.300	0.400	0.200	0.330	0.460	0.250	0.360	0.460
SM009	0.580	0.680	0.740	0.320	0.420	0.520	0.580	0.680	0.740	0.270	0.360	0.450	0.480	0.580	0.620	0.620	0.680	0.740
SM010	0.700	0.800	0.850	0.100	0.130	0.200	0.650	0.700	0.800	0.150	0.200	0.250	0.600	0.650	0.700	0.150	0.200	0.250
SM011	0.000	0.500	0.600	0.500	0.700	0.800	0.000	0.300	0.400	0.700	0.800	1.000	0.500	0.600	0.700	0.700	0.800	1.000
SM012	0.600	0.700	0.800	0.100	0.500	0.550	0.600	0.700	0.900	0.200	0.300	0.350	0.400	0.500	0.600	0.400	0.500	0.600
SM013	0.500	0.700	0.900	0.500	0.600	0.700	0.400	0.500	0.800	0.200	0.300	0.400	0.500	0.600	0.800	0.400	0.600	0.900
SM014	0.350	0.500	0.700	0.100	0.200	0.250	0.250	0.350	0.500	0.100	0.150	0.200	0.400	0.500	0.600	0.200	0.300	0.450
SM016	0.997	0.998	0.999	0.010	0.200	0.400	0.997	0.998	0.999	0.010	0.200	0.400	0.997	0.998	0.999	0.010	0.200	0.400
SM017	0.650	0.800	0.900	0.750	0.800	0.850	0.150	0.300	0.350	0.750	0.800	0.850	0.700	0.750	0.800	0.750	0.800	0.850
SM018	0.500	0.700	1.000	0.000	0.300	0.800	0.300	0.700	0.900	0.200	0.300	0.700	0.300	0.500	0.700	0.200	0.400	0.700
SM019	0.300	0.500	0.700	0.000	0.150	0.250	0.400	0.600	0.750	0.000	0.200	0.330	0.010	0.020	0.030	0.010	0.020	0.030
SM020	0.500	0.700	0.900	0.100	0.300	0.600	0.800	0.950	1.000	0.100	0.200	0.250	0.800	0.950	1.000	0.375	0.475	0.575
SM022	0.500	0.700	0.750	0.350	0.500	0.650	0.400	0.600	0.700	0.600	0.700	0.800	0.400	0.600	0.800	0.600	0.700	0.850
SM024	0.700	0.800	0.900	0.100	0.300	0.400	0.500	0.800	1.000	0.500	0.600	0.800	0.800	0.900	1.000	0.500	0.600	0.800
SM026	0.200	0.300	0.400	0.700	0.800	0.900	0.750	0.850	0.950	0.200	0.300	0.400	0.350	0.450	0.550	0.600	0.700	0.800
SM028	0.800	0.900	1.000	0.100	0.200	0.300	0.800	0.900	1.000	0.000	0.100	0.200	0.400	0.500	0.800	0.200	0.400	0.600
SM029	0.550	0.750	0.950	0.250	0.450	0.650	0.580	0.800	0.960	0.250	0.450	0.680	0.150	0.400	0.700	0.500	0.650	0.900
SM030	0.540	0.700	0.720	0.150	0.200	0.230	0.550	0.620	0.720	0.220	0.240	0.330	0.340	0.420	0.520	0.320	0.350	0.460
SM032	0.800	0.900	1.000	0.050	0.150	0.250	0.400	0.500	0.600	0.100	0.200	0.300	0.600	0.700	0.800	0.150	0.250	0.350
SM033	0.600	0.800	1.000	0.050	0.150	0.300	0.750	0.850	0.950	0.050	0.100	0.200	0.100	0.200	0.400	0.100	0.250	0.500
SM035	0.500	0.700	0.900	0.600	0.800	1.000	0.500	0.700	0.900	0.800	0.900	1.000	0.400	0.600	0.900	0.600	0.800	1.000
SM036	0.500	0.600	0.700	0.400	0.500	0.600	0.600	0.700	0.800	0.300	0.400	0.500	0.500	0.600	0.700	0.600	0.700	0.800
SM037	0.500	0.600	0.700	0.200	0.300	0.400	0.600	0.700	0.800	0.100	0.200	0.300	0.500	0.600	0.700	0.300	0.400	0.500
SM038	0.700	0.800	0.900	0.600	0.700	0.800	0.700	0.800	0.900	0.200	0.300	0.400	0.400	0.600	0.800	0.200	0.400	0.600
SM040	0.700	0.800	1.000	0.000	0.100	0.250	0.750	0.950	1.000	0.050	0.100	0.300	0.000	0.050	0.250	0.500	0.900	1.000
SM042	0.300	0.600	0.660	0.200	0.400	0.500	0.500	0.600	0.900	0.100	0.200	0.280	0.250	0.600	0.840	0.550	0.650	0.900

	SCENARIO 4																										
	COA 1									COA 2									COA 3								
	DAMAGE			ATTRIBUTION			COMPROMISE			DAMAGE			ATTRIBUTION			COMPROMISE			DAMAGE			ATTRIBUTION			COMPROMISE		
SME NUMBER	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV
SM001	0.600	0.700	0.800	0.300	0.400	0.500	0.200	0.300	0.400	0.600	0.700	0.800	0.400	0.500	0.600	0.500	0.600	0.700	0.300	0.400	0.500	0.500	0.600	0.700	0.500	0.600	0.700
SM002	0.250	0.500	0.600	0.000	0.100	0.200	0.000	0.100	0.200	0.660	0.850	1.000	0.000	0.050	0.200	0.000	0.050	0.150	0.250	0.330	0.600	0.400	0.750	0.900	0.400	0.750	0.900
SM003	0.540	0.720	0.820	0.340	0.430	0.530	0.320	0.420	0.520	0.320	0.350	0.440	0.410	0.510	0.610	0.340	0.440	0.520	0.320	0.410	0.530	0.330	0.510	0.610	0.340	0.440	0.550
SM004	0.300	0.400	0.500	0.200	0.300	0.400	0.500	0.600	0.700	0.500	0.600	0.700	0.400	0.500	0.600	0.600	0.700	0.800	0.300	0.400	0.500	0.700	0.800	0.900	0.600	0.700	0.800
SM007	0.300	0.480	0.500	0.250	0.380	0.400	0.100	0.200	0.300	0.400	0.620	0.700	0.100	0.120	0.200	0.100	0.120	0.200	0.700	0.850	0.900	0.500	0.600	0.700	0.600	0.740	0.900
SM009	0.520	0.660	0.730	0.380	0.460	0.550	0.370	0.460	0.580	0.540	0.620	0.760	0.240	0.360	0.480	0.180	0.260	0.360	0.580	0.680	0.760	0.580	0.660	0.760	0.620	0.680	0.780
SM010	0.500	0.700	0.800	0.050	0.100	0.150	0.150	0.200	0.250	0.700	0.750	0.850	0.050	0.100	0.150	0.050	0.100	0.130	0.550	0.600	0.650	0.400	0.500	0.820	0.500	0.600	0.800
SM011	0.700	0.800	0.900	0.000	0.200	0.300	0.000	0.200	0.300	0.700	0.800	0.900	0.000	0.200	0.300	0.000	0.200	0.300	0.400	0.500	0.600	0.400	0.500	0.600	0.600	0.700	0.800
SM012	0.700	0.800	0.900	0.400	0.500	0.670	0.300	0.500	0.600	0.100	0.200	0.250	0.400	0.500	0.600	0.300	0.500	0.550	0.200	0.300	0.350	0.850	0.900	1.000	0.800	0.900	1.000
SM013	0.400	0.600	0.800	0.100	0.300	0.400	0.100	0.200	0.300	0.500	0.600	0.800	0.300	0.400	0.500	0.300	0.600	0.700	0.600	0.800	0.900	0.600	0.800	1.000	0.800	0.900	1.000
SM014	0.400	0.600	0.700	0.700	0.750	0.850	0.500	0.600	0.800	0.500	0.750	0.850	0.200	0.300	0.400	0.400	0.500	0.600	0.600	0.800	0.850	0.300	0.400	0.500	0.350	0.450	0.550
SM016	0.000	0.300	1.000	0.010	0.200	0.400	0.130	0.151	0.159	0.997	0.998	0.999	0.010	0.200	0.400	0.010	0.100	0.200	0.997	0.998	0.999	0.010	0.200	0.400	0.450	0.500	0.550
SM017	0.800	0.850	0.950	0.050	0.200	0.250	0.000	0.100	0.200	0.050	0.350	0.500	0.000	0.100	0.150	0.000	0.050	0.070	0.300	0.400	0.750	0.000	0.200	0.250	0.000	0.050	0.100
SM018	0.200	0.500	0.800	0.300	0.600	0.900	0.500	0.600	0.900	0.300	0.700	1.000	0.300	0.500	0.700	0.300	0.600	0.900	0.400	0.700	0.900	0.300	0.400	0.700	0.300	0.600	0.900
SM019	0.100	0.400	0.600	0.000	0.100	0.200	0.000	0.100	0.200	0.500	0.700	0.800	0.000	0.050	0.100	0.000	0.050	0.100	0.010	0.020	0.030	0.010	0.020	0.030	0.010	0.020	0.030
SM020	0.700	0.800	0.900	0.150	0.200	0.300	0.150	0.300	0.450	0.600	0.700	0.900	0.500	0.600	0.800	0.000	0.050	0.100	0.700	0.800	0.900	0.000	0.050	0.100	0.150	0.400	0.800
SM022	0.700	0.800	0.950	0.450	0.600	0.750	0.600	0.700	0.900	0.300	0.500	0.750	0.300	0.500	0.700	0.250	0.400	0.500	0.700	0.800	0.900	0.600	0.700	0.850	0.750	0.900	1.000
SM024	0.300	0.600	0.700	0.000	0.100	0.200	0.100	0.200	0.300	0.100	0.300	0.340	0.000	0.100	0.200	0.000	0.020	0.100	0.600	0.800	0.900	0.500	0.800	1.000	0.700	0.800	0.900
SM026	0.550	0.650	0.750	0.300	0.400	0.500	0.400	0.500	0.600	0.600	0.700	0.800	0.300	0.400	0.500	0.300	0.400	0.500	0.600	0.700	0.800	0.700	0.800	0.900	0.650	0.750	0.850
SM028	0.600	0.700	1.000	0.100	0.400	0.600	0.200	0.300	0.400	0.400	0.500	0.600	0.000	0.200	0.400	0.100	0.300	0.500	0.700	0.800	0.900	0.500	0.600	0.800	0.200	0.400	0.600
SM029	0.550	0.750	0.950	0.250	0.350	0.550	0.150	0.300	0.500	0.230	0.450	0.600	0.200	0.450	0.750	0.300	0.480	0.700	0.450	0.630	0.880	0.400	0.620	0.830	0.530	0.700	0.950
SM030	0.430	0.500	0.550	0.150	0.200	0.250	0.230	0.300	0.330	0.650	0.730	0.800	0.100	0.130	0.210	0.200	0.230	0.320	0.530	0.630	0.700	0.550	0.600	0.700	0.570	0.610	0.720
SM032	0.800	0.900	1.000	0.000	0.150	0.300	0.000	0.100	0.200	0.800	0.900	1.000	0.100	0.200	0.300	0.000	0.100	0.200	0.400	0.500	0.600	0.000	0.100	0.200	0.300	0.450	0.600
SM033	0.700	0.800	0.900	0.100	0.150	0.200	0.000	0.250	0.050	0.600	0.700	0.800	0.100	0.200	0.300	0.100	0.200	0.300	0.300	0.500	0.600	0.500	0.600	0.800	0.500	0.600	0.800
SM035	0.600	0.700	0.800	0.600	0.700	0.800	0.500	0.600	0.700	0.600	0.700	0.900	0.300	0.600	0.800	0.200	0.500	0.900	0.400	0.600	0.800	0.200	0.400	0.700	0.200	0.500	0.800
SM036	0.600	0.700	0.800	0.400	0.500	0.600	0.400	0.500	0.600	0.600	0.700	0.800	0.600	0.700	0.800	0.500	0.600	0.700	0.600	0.700	0.800	0.700	0.800	0.900	0.700	0.800	0.900
SM037	0.600	0.700	0.800	0.100	0.200	0.300	0.200	0.300	0.400	0.600	0.800	0.900	0.200	0.300	0.400	0.300	0.400	0.500	0.500	0.600	0.700	0.300	0.400	0.500	0.300	0.400	0.500
SM038	0.500	0.700	0.800	0.100	0.300	0.500	0.300	0.500	0.700	0.500	0.600	1.000	0.200	0.500	0.800	0.200	0.500	0.800	0.100	0.800	0.900	0.100	0.600	0.800	0.100	0.600	0.800
SM040	0.050	0.300	0.400	0.000	0.250	0.400	0.050	0.150	0.400	0.600	0.750	0.950	0.050	0.200	0.250	0.000	0.100	0.300	0.600	0.750	0.900	0.100	0.200	0.300	0.000	0.100	0.250
SM042	0.400	0.500	0.680	0.300	0.500	0.700	0.400	0.500	0.600	0.500	0.600	0.700	0.500	0.600	0.800	0.400	0.600	0.800	0.300	0.500	0.600	0.400	0.550	0.900	0.600	0.700	0.900

	SCENARIO 5																										
	COA 1									COA 2									COA 3								
	DAMAGE			DETECTION			ATTRIBUTION			DAMAGE			DETECTION			ATTRIBUTION			DAMAGE			DETECTION			ATTRIBUTION		
SME NUMBER	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV	LV	ML	UV
SM001	0.600	0.700	0.800	0.600	0.700	0.800	0.200	0.300	0.400	0.600	0.700	0.800	0.200	0.300	0.400	0.400	0.500	0.600	0.600	0.700	0.800	0.700	0.800	0.900	0.200	0.300	0.400
SM002	0.000	0.050	0.100	0.400	0.900	1.000	0.400	0.900	1.000	0.000	0.050	0.100	0.200	0.250	0.300	0.000	0.200	0.300	0.000	0.050	0.100	0.800	0.900	1.000	0.850	0.950	1.000
SM003	0.520	0.630	0.730	0.400	0.440	0.530	0.400	0.600	0.730	0.540	0.720	0.820	0.340	0.430	0.520	0.340	0.430	0.540	0.410	0.530	0.640	0.340	0.430	0.530	0.400	0.600	0.730
SM004	0.600	0.700	0.800	0.600	0.700	0.800	0.500	0.600	0.700	0.500	0.600	0.700	0.600	0.700	0.800	0.200	0.300	0.400	0.700	0.800	0.900	0.400	0.500	0.600	0.400	0.500	0.600
SM007	0.700	0.870	0.900	0.300	0.400	0.500	0.200	0.230	0.300	0.800	0.900	0.990	0.150	0.200	0.250	0.100	0.220	0.400	0.800	0.910	0.990	0.200	0.500	0.600	0.500	0.600	0.750
SM009	0.320	0.620	0.760	0.580	0.700	0.900	0.200	0.400	0.600	0.560	0.700	0.860	0.100	0.220	0.300	0.100	0.200	0.300	0.100	0.200	0.300	0.600	0.700	0.800	0.600	0.700	0.800
SM010	0.700	0.750	0.800	0.350	0.400	0.500	0.400	0.450	0.500	0.650	0.700	0.750	0.200	0.250	0.300	0.300	0.400	0.550	0.550	0.650	0.750	0.200	0.300	0.400	0.350	0.400	0.450
SM011	0.600	0.800	1.000	0.300	0.400	0.500	0.000	0.600	1.000	0.600	0.800	1.000	0.000	0.200	0.500	0.200	0.600	0.800	0.000	0.200	0.400	0.000	0.200	0.300	0.300	0.500	0.700
SM012	0.400	0.500	0.600	0.400	0.450	0.500	0.450	0.500	0.600	0.500	0.600	0.700	0.400	0.800	0.900	0.350	0.700	0.800	0.600	0.700	0.800	0.560	0.800	0.860	0.400	0.800	0.900
SM013	0.400	0.600	0.900	0.100	0.600	0.700	0.400	0.600	0.800	0.500	0.700	1.000	0.700	0.800	1.000	0.400	0.500	0.700	0.700	0.800	1.000	0.400	0.500	1.000	0.300	0.600	0.800
SM014	0.050	0.100	0.150	0.600	0.900	0.950	0.050	0.200	0.250	0.750	0.800	0.900	0.100	0.150	0.250	0.100	0.150	0.250	0.500	0.700	0.800	0.200	0.300	0.400	0.100	0.200	0.250
SM016	0.997	0.998	0.999	0.400	0.405	0.409	0.010	0.200	0.400	0.997	0.998	0.999	0.200	0.205	0.209	0.400	0.405	0.409	0.997	0.998	0.999	0.200	0.201	0.999	0.010	0.200	0.400
SM017	0.500	0.800	0.900	0.800	0.900	1.000	0.850	0.900	1.000	0.200	0.750	0.850	0.850	0.900	1.000	0.870	0.900	1.000	0.850	0.950	1.000	0.850	0.900	1.000	0.900	0.950	1.000
SM018	0.400	0.700	0.900	0.200	0.700	0.900	0.300	0.400	0.700	0.400	0.700	0.900	0.300	0.700	0.800	0.100	0.400	0.500	0.400	0.600	0.900	0.300	0.500	0.800	0.100	0.300	0.600
SM019	0.300	0.500	0.700	0.300	0.400	0.500	0.400	0.600	0.800	0.400	0.550	0.700	0.300	0.400	0.550	0.600	0.750	0.900	0.400	0.600	0.800	0.200	0.400	0.550	0.600	0.800	1.000
SM020	0.900	0.950	1.000	0.350	0.400	0.550	0.000	0.050	0.100	0.900	0.950	1.000	0.200	0.250	0.300	0.400	0.450	0.500	0.900	0.950	1.000	0.000	0.050	0.100	0.000	0.050	0.100
SM022	0.450	0.600	0.750	0.700	0.800	0.950	0.500	0.600	0.700	0.700	0.800	0.850	0.400	0.600	0.750	0.600	0.700	0.800	0.800	0.900	1.000	0.600	0.750	0.850	0.600	0.700	0.850
SM024	0.800	0.900	1.000	0.200	0.300	0.400	0.000	0.100	0.200	0.300	0.400	0.700	0.400	0.500	0.600	0.700	0.800	0.900	0.600	0.700	0.800	0.700	0.800	0.900	0.700	0.800	0.900
SM026	0.400	0.500	0.600	0.300	0.400	0.500	0.150	0.250	0.350	0.750	0.850	0.950	0.100	0.200	0.300	0.300	0.400	0.500	0.350	0.450	0.550	0.500	0.600	0.700	0.300	0.400	0.500
SM028	0.600	0.800	1.000	0.300	0.400	0.500	0.200	0.400	0.600	0.800	0.900	1.000	0.300	0.500	0.800	0.400	0.500	0.700	0.500	0.600	0.800	0.000	0.100	0.200	0.000	0.100	0.200
SM029	0.430	0.600	0.830	0.350	0.520	0.730	0.450	0.650	0.830	0.300	0.620	0.890	0.150	0.350	0.520	0.350	0.550	0.730	0.650	0.750	0.950	0.330	0.550	0.650	0.330	0.550	0.730
SM030	0.500	0.600	0.620	0.300	0.400	0.500	0.520	0.600	0.630	0.600	0.720	0.740	0.140	0.200	0.230	0.130	0.140	0.200	0.700	0.730	0.800	0.320	0.400	0.530	0.420	0.500	0.630
SM032	0.800	0.900	1.000	0.300	0.400	0.500	0.000	0.100	0.200	0.700	0.800	0.900	0.100	0.200	0.300	0.300	0.400	0.500	0.800	0.900	1.000	0.000	0.100	0.200	0.200	0.300	0.400
SM033	0.100	0.200	0.300	0.300	0.400	0.500	0.400	0.500	0.600	0.600	0.800	0.900	0.100	0.200	0.300	0.100	0.400	0.500	0.700	0.800	0.900	0.500	0.600	0.800	0.500	0.600	0.800
SM035	0.500	0.700	0.900	0.800	0.900	1.000	0.200	0.500	0.800	0.500	0.700	0.900	0.500	0.600	0.800	0.600	0.700	0.900	0.700	0.800	0.900	0.100	0.500	0.900	0.100	0.500	0.900
SM036	0.500	0.600	0.700	0.600	0.700	0.800	0.500	0.600	0.700	0.500	0.700	0.800	0.500	0.600	0.700	0.400	0.500	0.600	0.500	0.600	0.700	0.400	0.500	0.600	0.600	0.700	0.800
SM037	0.500	0.600	0.700	0.300	0.400	0.500	0.200	0.300	0.400	0.600	0.700	0.800	0.100	0.200	0.300	0.100	0.200	0.250	0.600	0.700	0.800	0.200	0.300	0.400	0.100	0.200	0.300
SM038	0.100	0.800	0.900	0.600	0.700	0.800	0.000	0.300	0.600	0.700	0.800	0.900	0.100	0.200	0.300	0.100	0.500	0.600	0.500	0.600	0.800	0.300	0.500	0.700	0.300	0.500	0.700
SM040	0.050	0.100	0.300	0.750	0.900	1.000	0.000	0.150	0.250	0.400	0.850	1.000	0.750	0.950	1.000	0.250	0.400	0.750	0.000	0.150	0.250	0.000	0.100	0.150	0.000	0.100	0.250
SM042	0.500	0.600	0.760	0.300	0.500	0.700	0.200	0.400	0.460	0.200	0.900	0.950	0.500	0.600	0.880	0.600	0.700	0.800	0.400	0.700	0.800	0.400	0.600	0.700	0.400	0.600	0.750

APPENDIX E. SAMPLE DOSPERT QUESTIONNAIRE

Found at: https://www8.gsb.columbia.edu/decisionsciences/research/tools/dospert

Domain-Specific Risk-Taking (Adult) Scale—Risk Taking

For each of the following statements, please indicate the **likelihood** that you would engage in the described activity or behavior if you were to find yourself in that situation. Provide a rating from *Extremely Unlikely* to *Extremely Likely*, using the following scale:

1	2	3	4	5	6	7
Extremely Unlikely	Moderately Unlikely	Somewhat Unlikely	Not Sure	Somewhat Likely	Moderately Likely	Extremely Likely

1. Admitting that your tastes are different from those of a friend.
2. Going camping in the wilderness.
3. Betting a day's income at the horse races.
4. Investing 10% of your annual income in a moderate growth mutual fund.
5. Drinking heavily at a social function.
6. Taking some questionable deductions on your income tax return.
7. Disagreeing with an authority figure on a major issue.
8. Betting a day's income at a high-stake poker game.
9. Having an affair with a married man/woman.
10. Passing off somebody else's work as your own.
11. Going down a ski run that is beyond your ability.
12. Investing 5% of your annual income in a very speculative stock.
13. Going whitewater rafting at high water in the spring.
14. Betting a day's income on the outcome of a sporting event
15. Engaging in unprotected sex.
16. Revealing a friend's secret to someone else.
17. Driving a car without wearing a seat belt.
18. Investing 10% of your annual income in a new business venture.
19. Taking a skydiving class.
20. Riding a motorcycle without a helmet.
21. Choosing a career that you truly enjoy over a more prestigious one.
22. Speaking your mind about an unpopular issue in a meeting at work.
23. Sunbathing without sunscreen.
24. Bungee jumping off a tall bridge.
25. Piloting a small plane.
26. Walking home alone at night in an unsafe area of town.
27. Moving to a city far away from your extended family.
28. Starting a new career in your mid-thirties.
29. Leaving your young children alone at home while running an errand.
30. Not returning a wallet you found that contains $200.

Domain-Specific Risk-Taking (Adult) Scale—Risk Perceptions

People often see some risk in situations that contain uncertainty about what the outcome or consequences will be and for which there is the possibility of negative consequences. However, riskiness is a very personal and intuitive notion, and we are interested in **your gut level assessment of how risky** each situation or behavior is.

For each of the following statements, please indicate **how risky you perceive** each situation. Provide a rating from *Not at all Risky* to *Extremely Risky*, using the following scale:

1	2	3	4	5	6	7
Not at all Risky	Slightly Risky	Somewhat Risky	Moderately Risky	Risky	Very Risky	Extremely Risky

1. Admitting that your tastes are different from those of a friend.
2. Going camping in the wilderness.
3. Betting a day's income at the horse races.
4. Investing 10% of your annual income in a moderate growth mutual fund.
5. Drinking heavily at a social function.
6. Taking some questionable deductions on your income tax return.
7. Disagreeing with an authority figure on a major issue.
8. Betting a day's income at a high-stake poker game.
9. Having an affair with a married man/woman.
10. Passing off somebody else's work as your own.
11. Going down a ski run that is beyond your ability.
12. Investing 5% of your annual income in a very speculative stock.
13. Going whitewater rafting at high water in the spring.
14. Betting a day's income on the outcome of a sporting event
15. Engaging in unprotected sex.
16. Revealing a friend's secret to someone else.
17. Driving a car without wearing a seat belt.
18. Investing 10% of your annual income in a new business venture.
19. Taking a skydiving class.
20. Riding a motorcycle without a helmet.
21. Choosing a career that you truly enjoy over a more prestigious one.
22. Speaking your mind about an unpopular issue in a meeting at work.
23. Sunbathing without sunscreen.
24. Bungee jumping off a tall bridge.
25. Piloting a small plane.
26. Walking home alone at night in an unsafe area of town.
27. Moving to a city far away from your extended family.
28. Starting a new career in your mid-thirties.
29. Leaving your young children alone at home while running an errand.
30. Not returning a wallet you found that contains $200.

Domain-Specific Risk-Taking (Adult) Scale—Expected Benefits

For each of the following statements, please indicate **the benefits** you would obtain from each situation. Provide a rating from **1 to 7**, using the following scale:

1	2	3	4	5	6	7
No benefits At all			Moderate Benefits			Great Benefits

1. Admitting that your tastes are different from those of a friend.
2. Going camping in the wilderness.
3. Betting a day's income at the horse races.
4. Investing 10% of your annual income in a moderate growth mutual fund.
5. Drinking heavily at a social function.
6. Taking some questionable deductions on your income tax return.
7. Disagreeing with an authority figure on a major issue.
8. Betting a day's income at a high-stake poker game.
9. Having an affair with a married man/woman.
10. Passing off somebody else's work as your own.
11. Going down a ski run that is beyond your ability.
12. Investing 5% of your annual income in a very speculative stock.
13. Going whitewater rafting at high water in the spring.
14. Betting a day's income on the outcome of a sporting event
15. Engaging in unprotected sex.
16. Revealing a friend's secret to someone else.
17. Driving a car without wearing a seat belt.
18. Investing 10% of your annual income in a new business venture.
19. Taking a skydiving class.
20. Riding a motorcycle without a helmet.
21. Choosing a career that you truly enjoy over a more prestigious one.
22. Speaking your mind about an unpopular issue in a meeting at work.
23. Sunbathing without sunscreen.
24. Bungee jumping off a tall bridge.
25. Piloting a small plane.
26. Walking home alone at night in an unsafe area of town.
27. Moving to a city far away from your extended family.
28. Starting a new career in your mid-thirties.
29. Leaving your young children alone at home while running an errand.
30. Not returning a wallet you found that contains $200.

APPENDIX F. SME ELICITATION PACKET

Naval Postgraduate School
Consent to Participate in Research

Introduction. You are invited to participate in a research study entitled ***Quantifying Risk for Offensive Cyber Operations.*** The purpose of the research is to create a framework that allows for the analysis of risk for decision makers when undertaking new operations. The research use case for this framework is decision makers below the national level allocated to use Offensive Cyber Operations for intelligence gathering or augmenting direct action operations.

Procedures.

- You will be given two 30 question questionnaires to ascertain your risk tolerance profile. Both questionnaires ask the same 30 questions, but with different purposes.
- The first questionnaire asks your likelihood that you would engage in the described activity or behavior if you were to find yourself in that situation.
- The second questionnaire asks how risky you perceive each situation.
- You will be given a fictitious scenario and asked to assess the risks involved, at a 90% confidence interval, in one or more of the following categories:
  - Maximizing Attack Effects
  - Maximizing Intelligence Gained
  - Minimizing Detection or Compromise
- You will be asked to describe what mental protocols or frameworks were used to attain these answers
- The interview will likely take no more than two hours.
- Everyone will be given the same scenario and asked the same questions
- If you agree, audio recording of the interview may occur for the purposes of facilitating note taking. Notes will be kept on me until back at NPS. Notes will be scanned at NPS and kept on my computer. Hard copy of notes will be destroyed at the conclusion of the research. Data will be de-identified and given to the library for storage at the conclusion.
- You will be given a demographic information collection sheet to collect information that describes you, but does not identify you.

☐ I consent to be audio recorded for this research study.
☐ I do not consent to be audio recorded for this research study.

Location. The interview will take place at a place of the participant's choosing. The information collected for this study will be unclassified in nature and will be used in unclassified research.

Cost. There is no cost to participate in this research study.

Voluntary Nature of the Study. Your participation in this study is strictly voluntary. If you choose to participate you can change your mind at any time and withdraw from the study. You will not be penalized in any way or lose any benefits to which you would otherwise be entitled if you choose not to participate in this study or to withdraw. The alternative to participating in the research is to not participate in the research.

Potential Risks and Discomforts. The potential risks of participating in this study are: Minimal risk of breach of confidentiality. I will offer to anonymize the SMEs to prevent bias or undue influence from the SMEs.

Anticipated Benefits. Anticipated benefits from this study are Commanders below the national level of operations (COCOM and below) will have a framework for assessing the risks involved for Offensive Cyber Operations in the event this authority is decentralized. You will not directly benefit from your participation in this research.

Compensation for Participation. No tangible compensation will be given.

Confidentiality & Privacy Act. Any information that is obtained during this study will be kept confidential to the fullest extent permitted by law. All efforts, within reason, will be made to keep your personal information in your research record confidential but total confidentiality cannot be guaranteed. Names will be kept separate from the data; unanalyzed data will not be shared with persons outside the research team. Data will be de-identified and given to the library for storage at the conclusion. Data is defined as all scenarios, evaluations, and transcripts of interviews once the PII has been removed, all mathematical models, and all other data needed to replicate the experiment following the conclusion of this dissertation research.

If you consent to be identified by name in this study, any reference to or quote by you will be published in the final research finding only after your review and approval. If you do not agree, then you will be identified broadly by discipline and/or rank, (for example, "fire chief").

☐ I consent to be identified by name in this research study.

☐ I do not consent to be identified by name in this research study.

Points of Contact. If you have any questions or comments about the research, or you experience an injury or have questions about any discomforts that you experience while taking part in this study please contact the Principal Investigator, Dr. Dan Boger, (831) 656–3671, *dboger@nps.edu*. Questions about your rights as a research subject or any other concerns may be addressed to the Navy Postgraduate School IRB Chair, Dr. Larry Shattuck, 831–656-2473, lgshattu@nps.edu.

Statement of Consent. I have read the information provided above. I have been given the opportunity to ask questions and all the questions have been answered to my satisfaction. I have been provided a copy of this form for my records and I agree to participate in this study. I understand that by agreeing to participate in this research and signing this form, I do not waive any of my legal rights.

_____ _____

Participant's Signature Date

You are part of a planning team for Cyber Operations at a Geographic Combatant Command (GCC). The commander sees success in cyber operations following from the pursuit of two objectives: maximizing the effectiveness of operations while minimizing the costs. The commander defines effectiveness in terms of five objectives:

1.0 To Maximize Effectiveness
- 1.1 To Maximize Damage
- 1.2 To Maximize Intelligence Gained
- 1.3 To Minimize Detection
- 1.4 To Minimize Attribution given Detection
- 1.5 To Minimize Compromise given Detection

The commander defines cost in terms of three components so that minimizing cost implies minimizing three objectives:

2.0 To Minimize Costs
- 2.1 To Minimize Personnel Costs
- 2.2 To Minimize Equipment Costs
- 2.3 To Minimize Infrastructure Costs

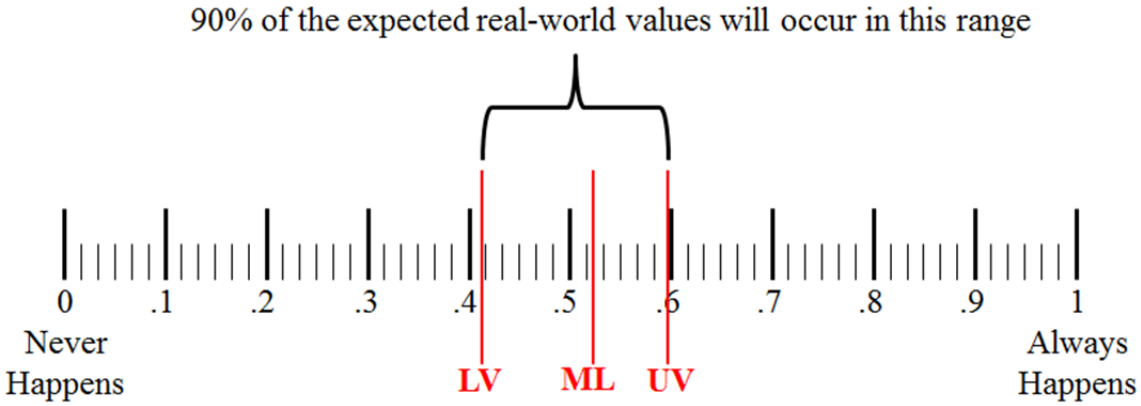
The cost considerations are the responsibility of another organization.
In this research, you will focus on scoring courses of action on the basis of the effectiveness measures all of which use a 0 to 1 interval scale. Some scales represent the percentage of a quantity to be attained. Other scales represent likelihood of the occurrence of a particular event.

For example, suppose the goal is to gather a specific amount intelligence. Then the commander's associated objective is to maximize intelligence gained. If you think there is no chance of gaining any of the required intelligence, then this course of action rates a value of 0.0 on the scale used for this objective. If you think there is a chance of gathering half of the required intelligence, then this course of action rates a value of 0.5. If you think it is certain that all the required intelligence is gained, the course of action is assigned a value of 1.0. Since the commander values gathering more intelligence to less intelligence, the commander places high decision value on 1.0 and extremely low value to 0.0. Thus, all possible outcomes for amount of intelligence gained are scaled between 0.0 and 1.0

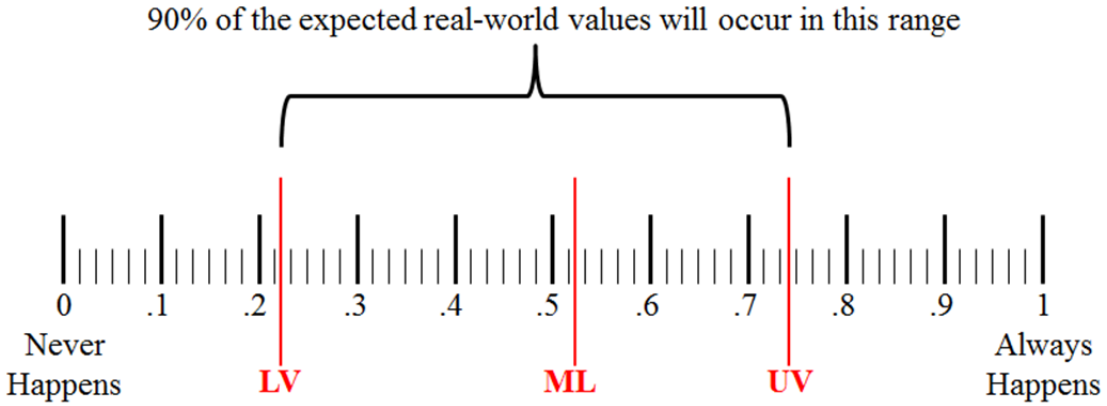
Conversely, suppose the goal is to avoid detection, then the commander's associated objective is to minimize detection. If you think there is no chance of being detected, the course of action rates a value of 0.0 in terms of this objective. If there is a 50–50 chance of detection, then this course of action rates a value of 0.5. If you think it is certain to be detected then this course of action rates a value of 1.0. Since the commander values avoiding detection, the commander places high decision value on 0.0 and extremely low value to 1.0. In this example, the rating used to evaluate a course of action is the probability of being detected so this objective uses a 0 -1 scale representing the detection probability; i.e., numbers between 0.0 and 1.0.

For this exercise, you will read each scenario and evaluate the associated courses of action.
Evaluation of a course of action requires you provide three numbers: a Lower Value (LV), an Upper Value (UV), and the Most Likely (ML) value. First specify ML. The Most Likely value will be your best estimate of the actual score value. The next two numbers, LV and UV, are very important. I want to know how certain you are of your ML value. Pick LV and UV such that you feel the actual or real value will be between LV and UV 90% of the time. **These values do not have to be symmetric around ML. There could be more variation to one side or the other.**

This example demonstrates much more confidence in the ML estimate because less uncertainty is involved:



This example demonstrates much less confidence in the ML estimate because more uncertainty is involved:



I am seeking your honest opinion of the uncertainty you recognize surrounding your best estimate of the ML.

1A BACKGROUND

It is five years from now and authority to conduct computer network exploitation (CNE) and computer network attack (CNA) has been partially delegated to COCOMs. CNE actions must be coordinated through USCYBERCOM, the Functional Combatant Command responsible for global cyber operations. USCYBERCOM supports Geographic Combatant Command (GCC) efforts with de-confliction, initial intelligence, assigned access points for operations, and capabilities. Primacy for all operations resides at USCYBERCOM to support de-confliction efforts. Command and control of cyber operations resides at the GCC once the operation is approved and commences. All computer network attack (CNA) actions taken by GCCs must have final approval from the national level authorities after review by the Joint Chiefs of Staff.

The Republic of Ameristan has long been an ally of the United States and has allowed forward basing of U.S. soldiers as part of theater security agreements and treaties. This is in conflict with Ameristan's neighbor, The Peoples' Democratic Republic of Koonistan, which is a technological peer to China, Russia, and Israel. Koonistan has long wanted U.S. forces to leave the region. Recently, tensions between Ameristan and Koonistan have risen and rhetoric from Koonistan has increased. This peaked last week with Koonistan shooting down an Ameristanian military helicopter resulting in no survivors. Koonistan claims that the helicopter violated the sovereign airspace and acted in self-defense.

Recent Human Intelligence (HUMINT) reports indicate a draft plan for a possible invasion of Ameristan has been created. The report indicated that a PowerPoint presentation of nearly 15MB in size along with a nearly 1MB Word document exists. Although the potential for an invasion of Ameristan by Koonistan is unlikely, the COCOM commander requires information from Koonistan's Ministry of Defense in order to ascertain Koonistan's intentions. This proposed action has been endorsed by USCYBERCOM. USCYBERCOM has identified only one viable access point in the targeted network. This access point resides in a Koonistan MoD user laptop that has been recently implanted by USCYBERCOM on behalf of the GCC. In the event that this access point is compromised access to this network will be lost and time consuming reconnaissance will be needed. This computer has local administrative credentials already but elevated privileges will be needed to traverse or execute capabilities. USCYBERCOM also has confirmed domain administrative credentials. USCYBERCOM has identified GCHQ as another friendly actor within the network; however, USCYBERCOM and the GCC have primacy.

1A COMMANDER'S INTENT

The GCC commander is interested in only two objectives: gaining more intelligence and decreasing the probability of detection of this operation. Success in this operation is the exfiltration of the Word document at a minimum. The commander prefers both the Word document and the PowerPoint however. The potential for attribution to the U.S. and inadvertently to GCHQ is a major concern. Additionally, with only one access point available, follow-on operations would be impossible for the foreseeable future.

The targeted machine is the Minister of Defense's laptop which is three hops away from the access point. It is a Lenovo laptop using Window 7, 64 bit with the bitlocker feature turned on. The operation is expected to occur during hours in which the laptop will be powered on and being used. This laptop is using a heuristics-based Kaspersky PSP with a local library of signatures that is updated by the admins weekly. The MoD network consists of Cisco routers and switches, Lenovo laptops all running the same operating system and PSP, and Microtik firewalls. Koonistan does not rely upon foreign ally support for network defense or analysis. Consequently, Koonistan has never detected friendly operations within their networks. However, non-routine Kaspersky support of Koonistan networks discovered a friendly capability 12 months ago.

USCYBERCOM has provided three potential CNE capability courses of action (COA) for consideration and choice by the COCOM Command and Staff. **As the GCC staff, you must order the COAs in precedence of most preferred to least preferred for consideration by the commander for a decision.**

1A COURSES OF ACTION

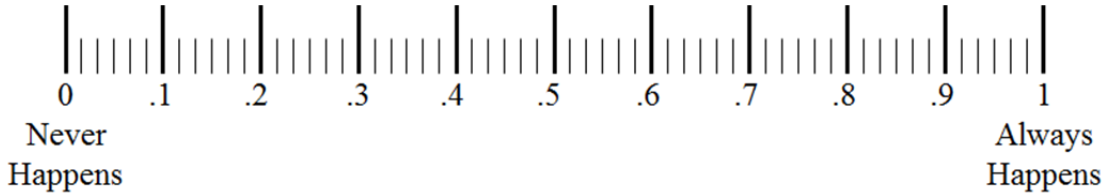
COA 1: STOLENCREDIT is an open-sourced tool that has been slightly modified and is available immediately. This tool hijacks an operating system function and will allow U.S. forces to monitor communications along with file creation/ modification/ deletion. This tool also has the capacity to accept a plug-in for monitoring room audio through the computer's microphone. However, the original open-sourced version of this tool is known in the computer security and hacker circles. This tool creates a process that is noticeable to system admins that is unique and tell-tale if detected. In virtualized testing, this tool has a 50/ 50 chance of being detected by Kaspersky.

COA 2: MONKEYSAURUSREX is a tool recently created by the USAF that claims to be able to be able to monitor communications along with file creation/ modification/ deletion. As a recently developed tool, this capability has no additional features or plug-ins for room audio monitoring or anything else. This capability has been tested in a virtualized environment and the capability was not detected by Kaspersky. However, this tool has not been used in a real operation. An experienced system administrator knowing

what to look for may be able to detect this capability as it shares the similar methodology for persistence within the network that the capability detected by the Chinese used 12 months ago. This capability can be configured and tested for this specific operation in between one and three weeks with a most likely completion at two weeks.

COA 3: COFFEEADDICT is a former NSA tool given to USCYBERCOM for operations. COFFEEADDICT was used globally by NSA for intelligence gathering until it was replaced with by another tool with more stealth and capability. This capability has been used in real operations last year where it was not detected by Kaspersky. Recent virtualized environment testing with the latest version of Kaspersky resulted in the capability being detected. It is unknown what change has occurred within Kaspersky to detect COFFEEADDICT. It is also unknown what version of Kapersky is being used on the target machine, only that library updates are completed weekly. If COFFEEADDICT is used, the capability to monitor communications along with file creation/ modification/ deletion exists along with room audio monitoring. Additionally, a plug-in to capture still photos using the laptop camera exists, but this plug-in has not been tested against this combination of hardware and software in virtualized or real environments. This capability can be configured and tested for this specific operation in between one and three weeks with a most likely completion at two and a half weeks.

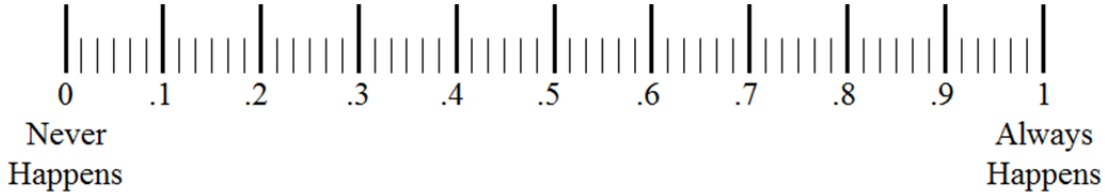
In **Scenario 1A**, COA 1, what do you feel is the percent of the required intelligence gained?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the percentage of required intelligence gained.
- Please draw a line on the above scale at the upper limit for percentage of required intelligence gained.
- Please draw a line on the above scale at the lower limit for the percentage of required intelligence gained.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

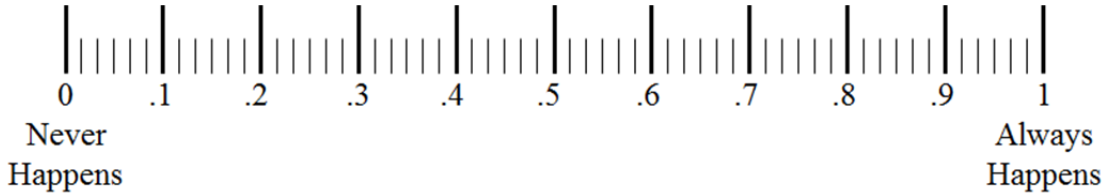
In **Scenario 1A**, COA 1, what do you feel is the probability of being detected?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being detected.
- Please draw a line on the above scale at the upper limit for the probability of being detected.
- Please draw a line on the above scale at the lower limit for the probability of being detected.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

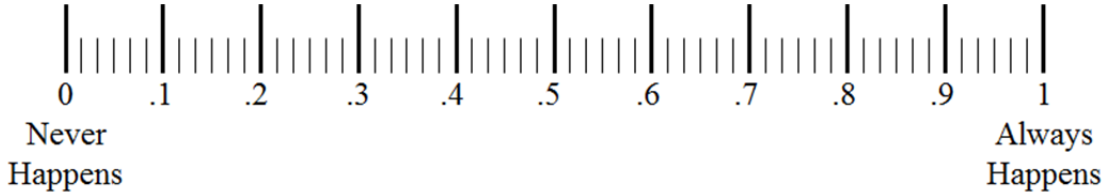
In **Scenario 1A**, COA 2, what do you feel is the percent of the required intelligence gained?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the percentage of required intelligence gained.
- Please draw a line on the above scale at the upper limit for percentage of required intelligence gained.
- Please draw a line on the above scale at the lower limit for the percentage of required intelligence gained.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

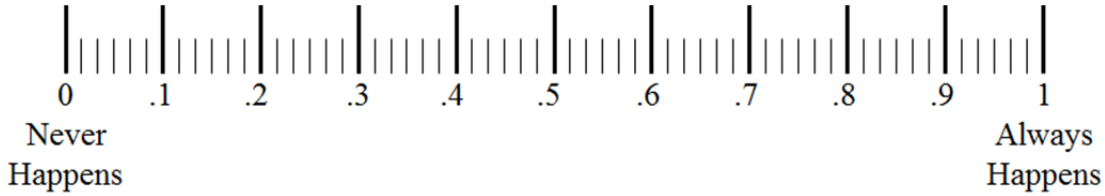
In **Scenario 1A**, COA 2, what do you feel is the probability of being detected?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being detected.
- Please draw a line on the above scale at the upper limit for the probability of being detected.
- Please draw a line on the above scale at the lower limit for the probability of being detected.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

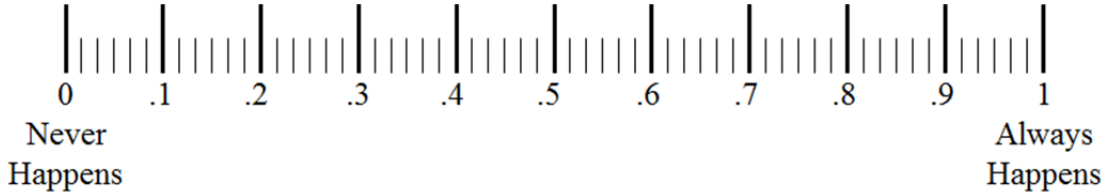
In **Scenario 1A**, COA 3, what do you feel is the percent of the required intelligence gained?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the percentage of required intelligence gained.
- Please draw a line on the above scale at the upper limit for percentage of required intelligence gained.
- Please draw a line on the above scale at the lower limit for the percentage of required intelligence gained.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

In **Scenario 1A**, COA 3, what do you feel is the probability of being detected?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being detected.
- Please draw a line on the above scale at the upper limit for the probability of being detected.
- Please draw a line on the above scale at the lower limit for the probability of being detected.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

1B BACKGROUND

The operation continues and the Minister of Defense's laptop has information exfiltrated without the operation being discovered. Analysis of the information points to Koonistan's plans to conduct small-scale guerilla attacks within Ameristan for the purpose of eroding trust and friendship between Ameristan and the U.S. Koonistan forces have escalated training, readiness, and forward deployment of forces near the Ameristan border as the rhetoric increases, particularly after the downing of the Ameristanian military helicopter.

The CCMD commander has requested and received authority to conduct a CNA operation within the MoD network. The desired endstate of this attack is two-fold: First, to disrupt the planning of the guerilla attacks in Ameristan and second, to demonstrate to the Koonistan leadership the vulnerabilities of their sensitive networks by our actions. This operation will be considered successful if all of the information on the targeted machine from the first phase of the operation is rendered inaccessible and unrecoverable. The targeted laptop has a 1TB SATA hard drive.

1B COMMANDER'S INTENT

Deterrence of Koonistan aggression is the goal of the COCOM commander. For this operation, the commander has two goals: destruction or denying access to the data and avoiding attribution. The COCOM commander wishes to demonstrate that a foreign actor is in Koonistan networks, however direct attribution to the U.S. is to be avoided. GCHQ has been informed of this potential operation and has exfiltrated all of their capabilities from the network.

Koonistan is assessed as a low risk for retaliation within U.S. critical infrastructure or key resources (CI/KR). Koonistan cyber actors has never been found within CI/KR, although they have claimed to infiltrated electrical power generation and distribution systems. Intelligence confirming this has not been conclusive. Koonistan has historically never allied with other nations to conduct cyber operations and the belief is that this will continue.

The Joint Chiefs of Staff and the President have approved this action. USCYBERCOM has expressed concern that the CNA effect may be detected by the Kapersky PSP if not executed immediately. This analysis is derived from virtualized modeling of the targeted environment. A delayed execution of the attack would likely result in the PSP detecting, quarantining, and passing the code to Kapersky for analysis. USCYBERCOM has provided three potential CNA capability courses of action (COA) for consideration and choice by the COCOM Command and Staff. **As the GCC staff, you must order the COAs in precedence of most preferred to least preferred for consideration by the commander for a decision.**

1B COURSES OF ACTION

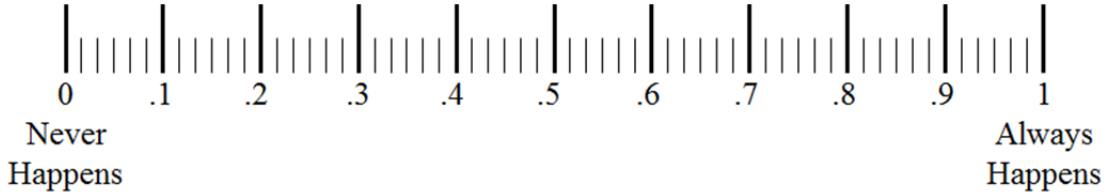
COA 1: ROADKILLDEER is a capability that encrypts the overwritten drive, then deletes the encryption key, and forces the computer to restart. It is predicted that this effect is irreversible if allowed to run completely. It is assessed that a 1TB drive will take approximately 10 minutes for the capability to completely take effect. This capability has a signature and may be traced to the U.S. due to its sophistication. This tool has not been used in real operations and only in a virtualized environment. Within the virtualized environment, Kaspersky quarantined this effect and prevented ROADKILLDEER from working 40% of the time. The software developers estimate that to configure and test this capability for the specific devices in this operation will most likely take three and a half weeks, but potentially can be completed in two weeks, but no more than five weeks. This capability can be configured and tested for this specific operation in between two and five weeks with a most likely completion at four weeks.

COA 2: FORGETFULHUSBAND is a capability that overwrites the hard drive with random characters over and over. This capability also destroys the file allocation table for the hard drive. In essence, this overwritten drive becomes one large file of gibberish. This capability has been used previously in a real-world operation. This previous operation was blamed on the US, but no forensic proof could be offered. The previous operation used a different hardware and software combination and the PSP did not detect the capability. This tool was not detected in virtualized testing for the hardware and software combination faced in this operation. This capability can be configured and tested for this specific operation in between one and three weeks with a most likely completion at one and a half weeks.

COA 3: DRUNKENFRATBOY is a capability that drags the read/ write head of the hard drive across the platters, rendering them unreadable. This capability increases the revolutions of the hard drive to the maximum of the hard drive and then applies the head to the metal oxide disk surfaces. This capability has not been used in real operations but has been tested on real machines. In testing on real machines, the capability commencing is immediate. This capability can be heard by the victim laptop user as the heads scrape across the platters. Additionally, because of what this capability is doing, the user will notice that no new information will be retrieved or saved once the capability commences. This capability has to run from a file written from the hard drive. This raises the potential for Kaspersky detecting this capability. In real-machine testing, Kaspersky detected the capability in a virus scan of the entire disk. Tradecraft used to write the file to disk enabled PSP evasion. The user of the laptop removing power to the machine could compromise the operation and bring attribution. Because of the sophistication of this capability, it is believed that if found, this capability will be attributed to the U.S. if the capability is

prevented from fully running. This capability can be configured and tested for this specific operation in between one and two weeks with a most likely completion at two weeks.

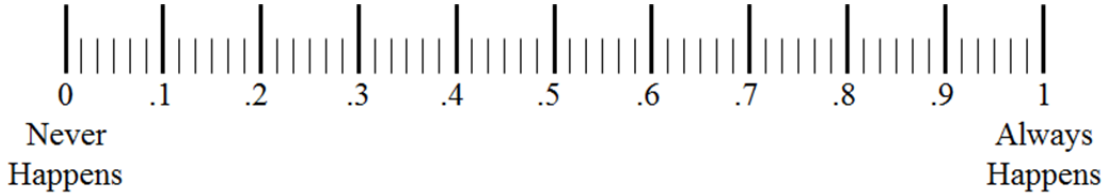
In **Scenario 1B**, COA 1, what do you feel is the percentage of the required damage inflicted?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the percentage of the required damage inflicted.
- Please draw a line on the above scale at the upper limit for the percentage of the required damage inflicted.
- Please draw a line on the above scale at the lower limit for the percentage of the required damage inflicted.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

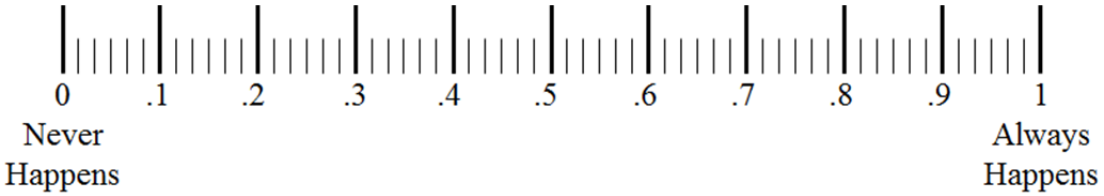
In **Scenario 1B**, COA 1, what do you feel is the probability of being attributed?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being attributed.
- Please draw a line on the above scale at the upper limit for the probability of being attributed.
- Please draw a line on the above scale at the lower limit for the probability of being attributed.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

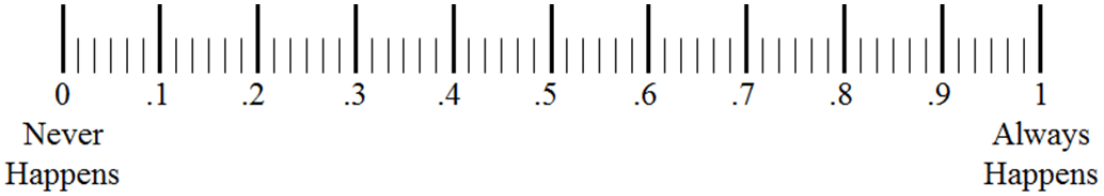
In **Scenario 1B**, COA 2, what do you feel is the percentage of the required damage inflicted?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the percentage of the required damage inflicted.
- Please draw a line on the above scale at the upper limit for the percentage of the required damage inflicted.
- Please draw a line on the above scale at the lower limit for the percentage of the required damage inflicted.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

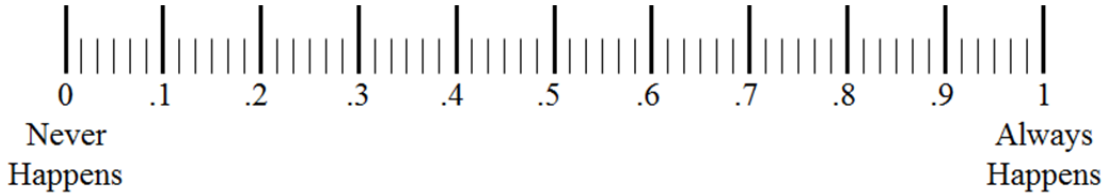
In **Scenario 1B**, COA 2, what do you feel is the probability of being attributed?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the lower limit for the probability of being attributed.
- Please draw a line on the above scale at the upper limit for the probability of being attributed.
- Please draw a line on the above scale at the most likely value for the probability of being attributed.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

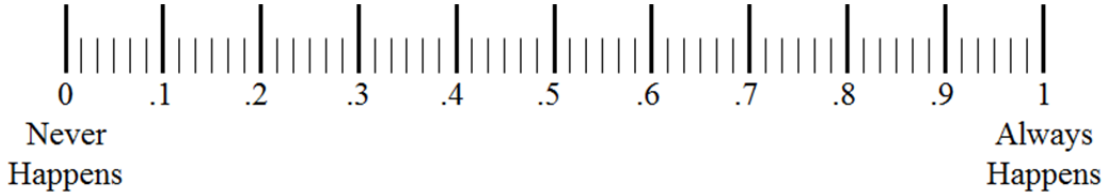
In **Scenario 1B**, COA 3, what do you feel is the percentage of the required damage inflicted?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the percentage of the required damage inflicted.
- Please draw a line on the above scale at the upper limit for the percentage of the required damage inflicted.
- Please draw a line on the above scale at the lower limit for the percentage of the required damage inflicted.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

In **Scenario 1B**, COA 3, what do you feel is the probability of being attributed?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being attributed.
- Please draw a line on the above scale at the upper limit for the probability of being attributed.
- Please draw a line on the above scale at the lower limit for the probability of being attributed.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

BACKGROUND

It is five years from now and authority to conduct computer network exploitation (CNE) and computer network attack (CNA) has been partially delegated to COCOMs. CNE actions must be coordinated through USCYBERCOM, the Functional Combatant Command responsible for global cyber operations. USCYBERCOM supports Geographic Combatant Command (GCC) with de-confliction, initial intelligence, assigned access points for operations, and capabilities. Primacy for all operations resides at USCYBERCOM to support de-confliction efforts. Command and control of cyber operations resides at the GCC once the operation is approved and commences. All computer network attack (CNA) actions taken by GCCs must have final approval from the national level authorities after review by the Joint Chiefs of Staff.

The Islamic State (IS) has continued to use the Internet to recruit, spread propaganda, and command and control decentralized operations over a wide swath of land in the Middle East. This online activity escalated with the video of a captured U.S. forces member being killed for propaganda purposes.

The GCC commander, in coordination with the Theater Special Operations Command (TSOC), has designated five IS personnel as high payoff targets (HPTs). These five people not only are instrumental in the operations and facilitation of IS operations, but are believed to be directed connected with the death of the above mentioned U.S. service member. The HPTs are believed to coordinate activities through instant messaging systems, shared email accounts, and file sharing sites. One of the instant messaging usernames has been identified and two others are suspected, but not confirmed. The shared email username and password has been identified along with one HPT's file sharing credentials. Initial intelligence indicates that the HPTs use Android phones of various manufacturers and Internet cafes providing Windows-based desktop computers with Internet access.

COMMANDER'S INTENT

The GCC commander has two goals: gathering intelligence and avoiding detection. The GCC requires that a CNE operation be undertaken to confirm the identity of the five HPTs by attaining a pictures of the targets using integrated cameras native to the devices. Additionally, the commander requires that geolocation of the targets must be attained and refreshed every fifteen minutes at a minimum in order to assist other intelligence assets in establishing patterns of life for the five HPTs. Once the patterns of life have been established, the TSOC will plan for coordinated capture/ kill operations of the five HPTs. This operation is to commence no later than five weeks from now.

The GCC commander places equal value on intelligence gathering for this operation and avoiding detection. The commander fears that if the operation is discovered or suspected

the HPTs will change their methods of communications. No other friendly actors have been identified working in the IS networks or their associated means of online communications such as the email account, file sharing, and instant messaging service. Due to their low maturity of tradecraft and frequent use of public Internet cafes this group is considered a low sophistication of threat.

USCYBERCOM has provided three potential CNE capability courses of action (COA) for consideration and choice by the COCOM Command and Staff. **As the GCC staff, you must order the COAs in precedence of most preferred to least preferred for consideration by the commander for a decision.**

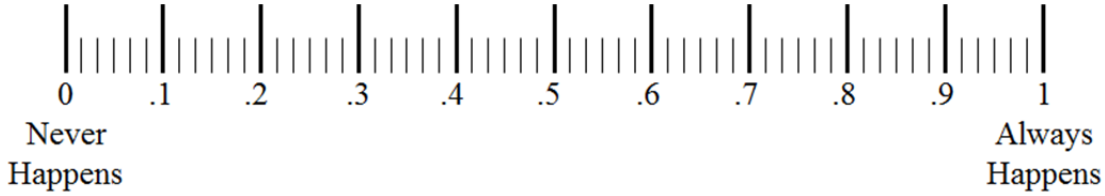
COURSES OF ACTION

COA 1: BOOTYCALL is a mobile device capability that monitors the HPTs' instant messaging application on Android devices. This capability is delivered over Wi-Fi or USB connections masquerading as an operating system update that must be accepted by the phone owner. The HPTs will both need to believe that the operating system update is needed and also be in a known Wi-Fi location. BOOTYCALL covertly monitors the instant messaging applications and simultaneously sends the GPS location of the phone to a collection sensor using Wi-Fi. An additional plug-in is available to access and control the camera. This plug-in may be delivered to the phone remotely over Wi-Fi once BOOTYCALL has installed. This capability only can transmit over Wi-Fi and not over the cellular provider. BOOTYCALL has not been used in a real operation and in a virtualized testing environment this capability demonstrated a 10% chance of causing the phone to repeatedly restart. Testing also leads to the indication of none of the prominent personal security products (PSPs) for mobile devices detecting BOOTYCALL. This capability can be configured and tested for this specific operation in between three and five weeks with a most likely completion at three weeks.

COA 2: OVERSTAYEDGUEST is a capability delivered by modified documents in an email. This capability infects Windows-based computers that open the document with an implant that will call back to a predetermined listening post. OVERSTAYEDGUEST has the capacity for plug-ins that can covertly turn on a camera, record files that have been read, written, or modified, and modify Wi-Fi emittances for a non-standard pattern may be used for geolocation. This capability has been used in real operations limitedly in the past due to the increasing sophistication of PSP vendors. Current virtualized testing indicates that OVERSTAYEDGUEST has a 40% chance of being detected by the top five PSPs being produced. The software developers responsible for virtualized testing expressed concern regarding the use of Internet cafes by the targets that may use one of the top five PSPs. This capability can be configured and tested for this specific operation in between one and three weeks with a most likely completion at two weeks.

COA 3: HOLIDAYREGIFT is a lightweight browser exploit that is compatible with Firefox and Chrome browsers in Android devices along with Windows laptops and desktops. This capability is delivered from downloading or opening an implanted file. The file sharing service will be the targeted mechanism of delivery. Once the implant is delivered and installed, HOLIDAYREGIFT will use the user agent string to download plug-ins as tasked. Plug-in capabilities include covertly operating the webcam (Windows only), gathering location information from the GPS to send periodic location updates through cellular transmission (Android only), USB proliferation to another device, and modifying the Wi-Fi modulation for potential geolocation (Windows and Android). This capability has not previously been used in real operations, but virtualized testing has determined that mobile devices have a 20% chance of browsers continually crashing if more than one browser is used. Windows devices using Kaspersky, Symantec, or Norton PSPs have a 20% chance of discovery. Each plug-in used in Windows devices increases the probability of detection by 5%. This capability can be configured and tested for this specific operation in between one and three weeks with a most likely completion at two weeks.

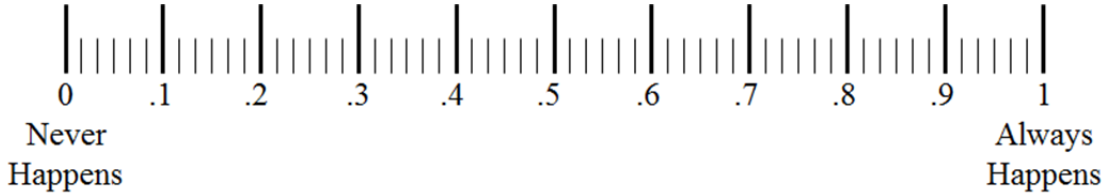
In COA 1, what do you feel is the percentage of required intelligence gained?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the percentage of required intelligence gained.
- Please draw a line on the above scale at the upper limit for percentage of required intelligence gained.
- Please draw a line on the above scale at the lower limit for the percentage of required intelligence gained.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

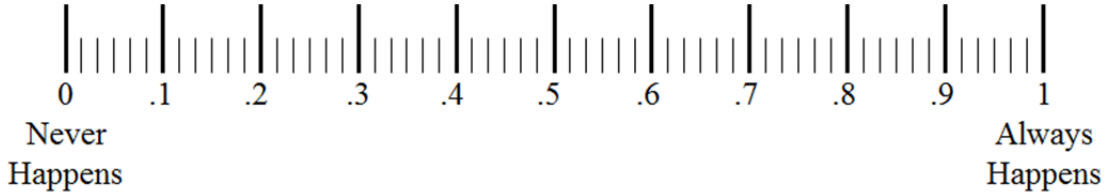
In COA 1, what do you feel is the probability of being detected?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being detected.
- Please draw a line on the above scale at the upper limit for the probability of being detected.
- Please draw a line on the above scale at the lower limit for the probability of being detected.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

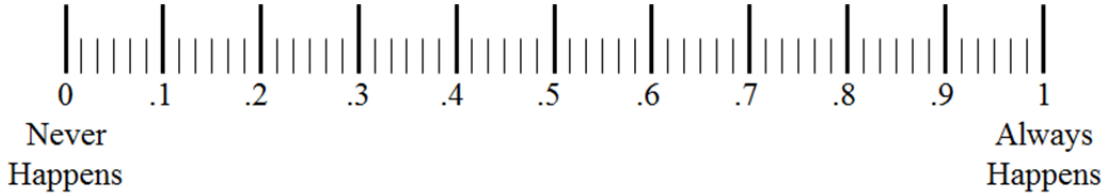
In COA 2, what do you feel is the percentage of required intelligence gained?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the percentage of required intelligence gained.
- Please draw a line on the above scale at the upper limit for percentage of required intelligence gained.
- Please draw a line on the above scale at the lower limit for the percentage of required intelligence gained.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

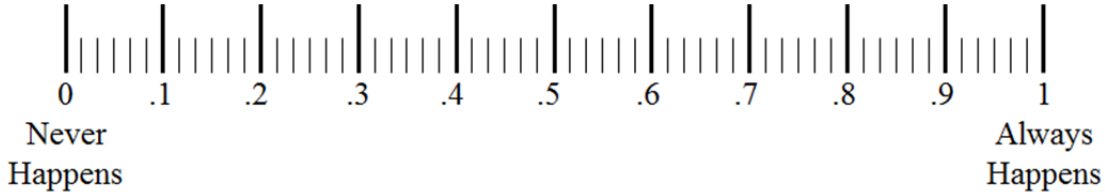
In COA 2, what do you feel is the probability of being detected?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being detected.
- Please draw a line on the above scale at the upper limit for the probability of being detected.
- Please draw a line on the above scale at the lower limit for the probability of being detected.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

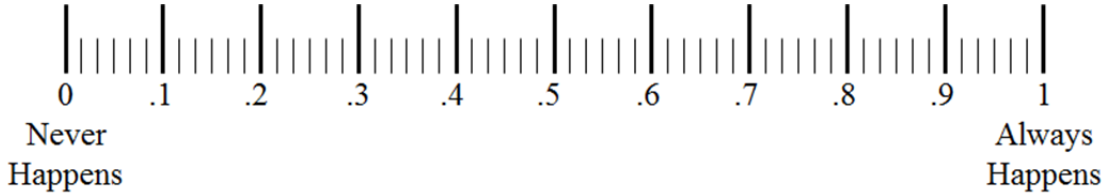
In COA 3, what do you feel is the percentage of required intelligence gained?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the percentage of required intelligence gained.
- Please draw a line on the above scale at the upper limit for percentage of required intelligence gained.
- Please draw a line on the above scale at the lower limit for the percentage of required intelligence gained.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

In COA 3, what do you feel is the probability of being detected?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being detected.
- Please draw a line on the above scale at the upper limit for the probability of being detected.
- Please draw a line on the above scale at the lower limit for the probability of being detected.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

BACKGROUND

It is five years from now and authority to conduct computer network exploitation (CNE) and computer network attack (CNA) has been partially delegated to COCOMs. CNE actions must be coordinated through USCYBERCOM, the Functional Combatant Command responsible for global cyber operations. USCYBERCOM supports Geographic Combatant Command (GCC) with de-confliction, initial intelligence, assigned access points for operations, and capabilities. Primacy for all operations resides at USCYBERCOM to support de-confliction efforts. Command and control of cyber operations resides at the GCC once the operation is approved and commences. All computer network attack (CNA) actions taken by GCCs must have final approval from the national level authorities after review by the Joint Chiefs of Staff.

The Republic of Ameristan has long been an ally of the United States and has allowed forward basing of U.S. soldiers as part of theater security agreements and treaties. This is in conflict with Ameristan's neighbor, The Peoples' Democratic Republic of Koonistan, which is a technological peer to China, Russia, and Israel. Koonistan has long wanted U.S. forces to leave the region. Recently, tensions between Ameristan and Koonistan have risen and rhetoric from Koonistan has increased. This peaked last week with Koonistan shooting down an Ameristanian military helicopter resulting in no survivors. Koonistan claims that the helicopter violated the sovereign airspace and acted in self-defense.

To prevent attribution of cyber activities, the Koonistan government relies upon state-sponsored contracted companies to conduct cyber operations to meet government operational goals. These companies are given financial support, intelligence, and resources for their operations, along with government-provided protection. Recent national level intelligence indicates that a Koonistan company, برق آساحمله (تک)ی (English: Lightning Attack; (LI)), has infiltrated the GCC networks and exfiltrated documents. The suspected documents included the recent updates to the Theater Security Cooperation Agreements with Ameristan that include personnel and equipment movement schedules and locations.

A portion of a document was exfiltrated from the LI network as proof, but proved inconclusive as the document was partially corrupted. USCYBERCOM has tasked the GCC to conduct a CNE operation to confirm or deny the presence of sensitive GCC document within the LI network, along with the amount of data taken. Confirmation is defined as the 400mb of non-public portion of the Theater Security Agreement that ranges in classification from SECRET to TOP SECRET/SI/NOFORN. This operation will be considered a success if all 400mb of the sensitive portion of the document is

identified, copied, and downloaded. CNA action is not authorized at this time. That will be a later effort pending the results of this operation.

Due to the sophistication of Koonistan, LI is considered to be the same level of sophistication. If attribution of GCC activities within the LI network is discovered and attributed, Koonistan may order a retaliatory attack within the GCC networks. Forensic analysis of the GCC networks continues, resulting in two LI entry points within the GCC network discovered with the fear that more exist.

COMMANDER'S INTENT

The commander has two equal goals: gathering intelligence and avoiding attribution due to the known activities by LI within the GCC networks.
USCYBERCOM has attained the target IP address where the document was discovered and a single entry point into the LI network. The target IP address is one hop away from the entry point. The entry point is a HP desktop with a Windows 7 with Service Pack 1 along with a Kaspersky personal security product (PSP). Access to this computer is through a misconfigured port. This machine rarely browses the Internet, so care must be taken not to draw attention to this computer and subsequently, to this operation. The target machine is a Dell PowerEdge server running a Windows Server 2012 R2 operating system. This machine is also using Kaspersky Security for Windows Server as a PSP.

A domain user credential has been provided for this operation. Additionally, USCYBERCOM has coordinated for all other friendly actors to be out of the LI network for the GCC operation. USCYBERCOM has provided three potential CNE capability courses of action (COA) for consideration and choice by the COCOM Command and Staff. **As the GCC staff, you must order the COAs in precedence of most preferred to least preferred for consideration by the commander for a decision.**

COURSES OF ACTION

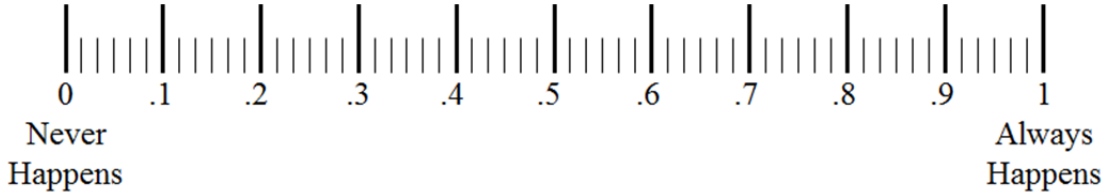
COA 1: SURREPTITIOUSCAMEL is a capability that scans and lists the directory of a device, creates executive summaries of chosen documents, and then will exfiltrate selected documents. This capability is a former NSA capability that has been replaced. This capability requires on-net operators to monitor and direct the capability. SURREPTITIOUSCAMEL has the ability to customize the rate of data exfiltration in the attempt to avoid detection in network traffic. On the lowest data transmission rate, SURREPTITIOUSCAMEL will at 6KB/ sec. Although used in real operations previously, this capability has not been used in over a year. Virtualized testing indicates a 10% chance of Kaspersky detecting the capability. It is estimated that for every KB/sec over 5KB/ sec in bandwidth leaving the access point computer, the potential for network administrator detecting the traffic increases by 5%. This capability can be configured and

tested for this specific operation in between one and three weeks with a most likely completion at two weeks.

COA 2: ANGRYPIRATE is an automated capability that inventories the directories of a device and sends selected files to a predetermined location. This capability requires several days to complete these tasks. Once activated, ANGRYPIRATE begins an inventory of all directories it can find. Once this is complete, it sends a small encrypted file using extremely low bandwidth to the predetermined sensor. The sensor will then notify the operator that information is waiting. Once the information is analyzed, an on-net operator tasks ANGRYPIRATE with a listing of files to encrypt and exfiltrate. It is estimated that a 1MB file will take an hour and a half to transmit. Additionally, ANGRYPIRATE is customizable to transmit only during predefined windows of time to prevent noticeable network traffic during time of network inactivity. This capability has not been used in real operations but virtualized testing indicated that Kaspersky will not detect ANGRYPIRATE. However, there is a 20% chance of a network administrator noticing traffic leaving a seldom used computer and identifying both the traffic leaving the network and the sensor used for communication with ANGRYPIRATE. This capability can be configured and tested for this specific operation in between one and two weeks with a most likely completion at two weeks.

COA 3: SKITTLEPARTY is a capability that exfiltrates all the contents of a hard drive. This capability has options for the exfiltration rate and windows of time to work that must be predefined. Once SKITTLEPARTY begins, it cannot stop to reconfigure without starting all over. On the lowest data transmission rate, SKITTLEPARTY will at 5KB/ sec. It is estimated that for every KB/sec over 5KB/ sec in bandwidth leaving the access point computer, the potential for detection increases by 5%. All files are encrypted and sent to a preconfigured location. The awaiting sensor must receive all the files on the hard drive before access to the files is possible. This capability has not been used in real operations however, in virtualized testing, Kaspersky detected SKITTLEPARTY only 17% of the time. However, with the amount of data that would be transmitted from this capability, it is estimated that there is a 20% chance that the system administrator will detect the traffic leaving the network and discover the sensor used with SKITTLEPARTY. This capability can be configured and tested for this specific operation in between one and two weeks with a most likely completion at one and a half weeks.

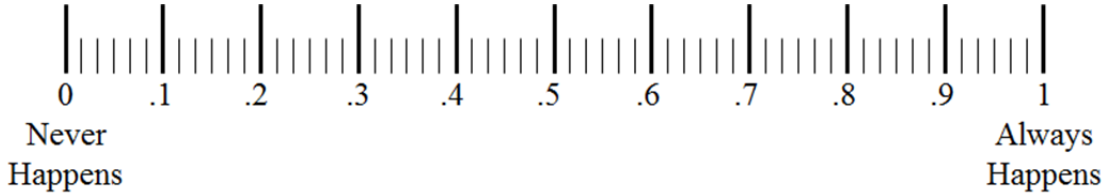
In COA 1, what do you feel is the percentage of required intelligence gained?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the percentage of required intelligence gained.
- Please draw a line on the above scale at the upper limit for percentage of required intelligence gained.
- Please draw a line on the above scale at the lower limit for the percentage of required intelligence gained.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

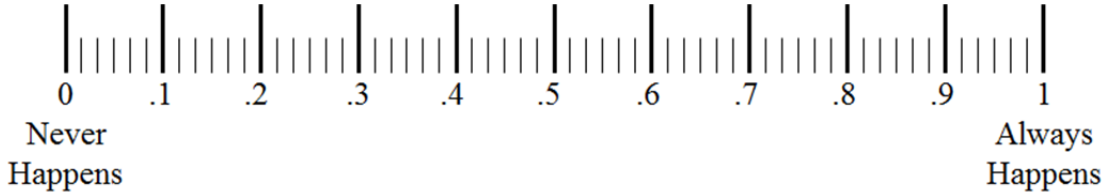
In COA 1, what do you feel is the probability of being attributed?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being attributed.
- Please draw a line on the above scale at the upper limit for the probability of being attributed.
- Please draw a line on the above scale at the lower limit for the probability of being attributed.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

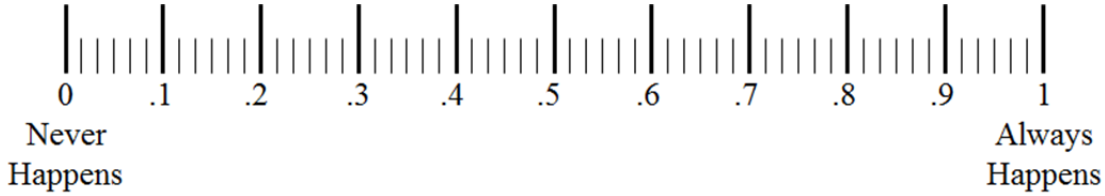
In COA 2, what do you feel is the percentage of required intelligence gained?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the percentage of required intelligence gained.
- Please draw a line on the above scale at the upper limit for percentage of required intelligence gained.
- Please draw a line on the above scale at the lower limit for the percentage of required intelligence gained.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

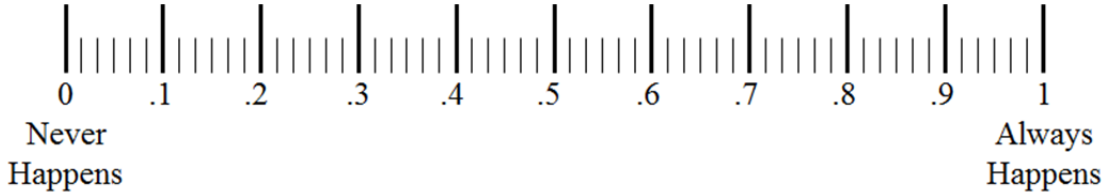
In COA 2, what do you feel is the probability of being attributed?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being attributed.
- Please draw a line on the above scale at the upper limit for the probability of being attributed.
- Please draw a line on the above scale at the lower limit for the probability of being attributed.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

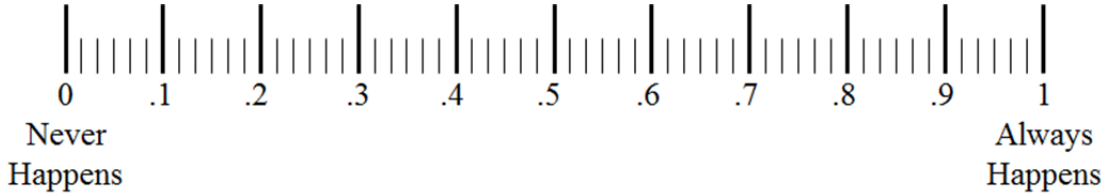
In COA 3, what do you feel is the percentage of required intelligence gained?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the percentage of required intelligence gained.
- Please draw a line on the above scale at the upper limit for percentage of required intelligence gained
- Please draw a line on the above scale at the lower limit for the percentage of required intelligence gained.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

In COA 3, what do you feel is the probability of being attributed?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being attributed.
- Please draw a line on the above scale at the upper limit for the probability of being attributed.
- Please draw a line on the above scale at the lower limit for the probability of being attributed.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

BACKGROUND

It is five years from now and authority to conduct computer network exploitation (CNE) and computer network attack (CNA) has been partially delegated to COCOMs. CNE actions must be coordinated through USCYBERCOM, the Functional Combatant Command responsible for global cyber operations. USCYBERCOM supports Geographic Combatant Command (GCC) with de-confliction, initial intelligence, assigned access points for operations, and capabilities. Primacy for all operations resides at USCYBERCOM to support de-confliction efforts. Command and control of cyber operations resides at the GCC once the operation is approved and commences. All computer network attack (CNA) actions taken by GCCs must have final approval from the national level authorities after review by the Joint Chiefs of Staff (JCS).

The Islamic State (IS) has continued to use the Internet to recruit, spread propaganda, and command and control decentralized operations over a wide swath of land in the Middle East. This online activity is escalating and after a video of a captured U.S. forces member being killed for propaganda purposes was released. The Central Intelligence Agency (CIA) has reported that the new edition of the jihadist magazine, Inspire, will be published online in two weeks. In this edition will be a call to arms for jihadists after the propaganda victory of the video of the American being killed. Additionally, this edition will have a new technique for bomb making.

COMMANDER'S INTENT

The GCC, in coordination with national level intelligence has decided that a CNA operation against Inspire magazine is warranted. The JCS and national level authorities have approved of the action. USCYBERCOM has tasked the GCC to conduct CNA upon the magazine file, which is an Adobe PDF. Specifically, the task for this is to prevent viewing of the file with two purposes; preventing dissemination of the bomb making information and to facilitate CIA identification of readers of the magazine. The target machine is an Apache web server using FreeBSD 10.3 and Panda Security antivirus protection.

One consideration is that the CIA monitors and participates within the web forum as a way of identifying persons of interest and high payoff targets (HPTs). The commander has been ordered to not bring attribution the U.S. or compromise the CIA efforts. As such, the commander has his goals as the denial of the video, avoiding attribution, and avoiding compromise.

USCYBERCOM has provided three potential CNA capability courses of action (COA) for consideration and choice by the COCOM Command and Staff. **As the GCC staff, you must order the COAs in precedence of most preferred to least preferred for consideration by the commander for a decision.**

COURSES OF ACTION

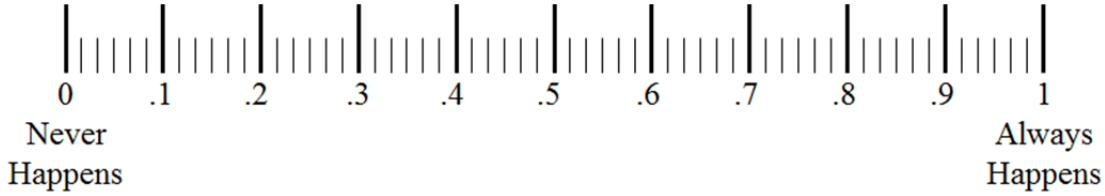
COA 1: BAMBOOSHIRT is a capability that is used to corrupt files and render them unreadable. This capability can accept plug-ins for disseminating implants and recording IP addresses of people attempting to access the file, providing a TCP reset to people attempting to access the file, redirecting the user to another predefined location (see concerns in COA 2), or disseminating malware to people attempting to access the file, such limited-scope as CNA capabilities. Only one implant may be used at a time or BAMBOOSHIRT becomes unstable and will cause the device to act erratically. This capability has not been used in real operations, but in virtualized testing it was not detected by personal security products (PSPs). However, if an implant or CNA capability is deployed from BAMBOOSHIRT, there is a 15% chance of those capabilities being detected. This capability can be configured and tested for this specific operation in between two and three weeks with a most likely completion at three weeks.

COA 2: DEPRESSEDCLOWN is a capability that would record the IP address and redirect users attempting to access a predetermined file to another predetermined location. When the user clicks the link to view or download the file, the user is automatically redirected to another location. That second location may or may not have a file for the user to see or download. When users are redirected, the computer being used is implanted. This implant then beacons back to a predefined sensor to wait for tasking. DEPRESSEDCLOWN has been used limitedly in real operations without being detected. This capability has the ability to filter what IP address blocks are redirected and implanted in the effort to prevent collection of information and the implant of computers belonging to U.S. persons. However, the concern is the collection of information and implanting of computers of U.S. persons and violating the Foreign Intelligence Surveillance Act. It is estimated that a 20% chance exists that information collection and implant of a computer belonging to a U.S. person will occur, based on analysis of the web forum. It is unknown if these are real U.S. persons or if they are foreign nationals using U.S. –based proxies. This capability can be configured and tested for this specific operation in between one and three weeks with a most likely completion at two weeks.

COA 3: OBESECATEPILLAR is a capability that allows the replacement of adobe PDF files while retaining the hash of the original. OBESECATEPILLAR further uses steganography to imbed an executable for an implant into the file. This implant will then beacon a sensor to await instructions. This capability has been used limitedly in real operations with success. Although OBESECATEPILLAR is not detected by Panda security, the risk also is with the end user device. There is a 15% chance of detection from Kaspersky, a 20% chance of protection by Symantec. It is unknown how OBESECATEPILLAR will perform with Qihoo 360. Estimates range from 40% likelihood of detection to 80% likelihood. The median consensus is a 45% chance of

detection. The concern is that if the file is detected by a PSP forensic examination will show that the file has been changed and the location of the sensor the implant beacons to. This would cause the terrorists to change tactics and move the web forum to another location, potentially causing the CIA to lose this source of intelligence. This capability can be configured and tested for this specific operation in between one and three weeks with a most likely completion at two weeks.

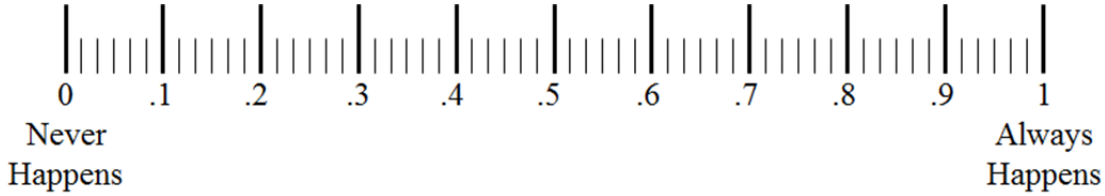
In COA 1, what do you feel is the percentage desired damage inflicted?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the percentage desired damage inflicted.
- Please draw a line on the above scale at the upper limit for the percentage desired damage inflicted.
- Please draw a line on the above scale at the lower limit for the percentage desired damage inflicted.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

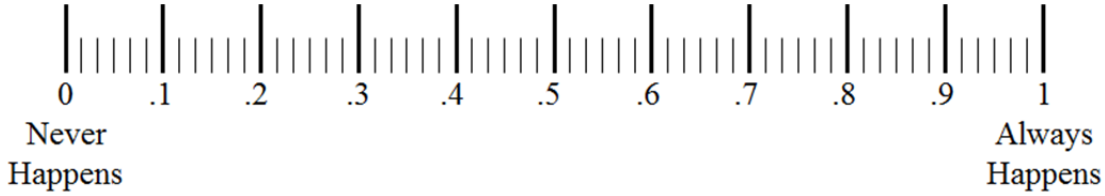
In COA 1 what do you feel is the probability of being attributed?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being attributed.
- Please draw a line on the above scale at the upper limit for the probability of being attributed.
- Please draw a line on the above scale at the lower limit for the probability of being attributed.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

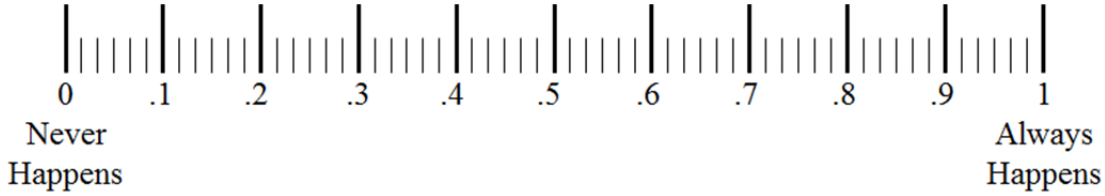
In COA 1, what do you feel is the probability of being compromised?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being compromised.
- Please draw a line on the above scale at the upper limit for the probability of being compromised.
- Please draw a line on the above scale at the lower limit for the probability of being compromised.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

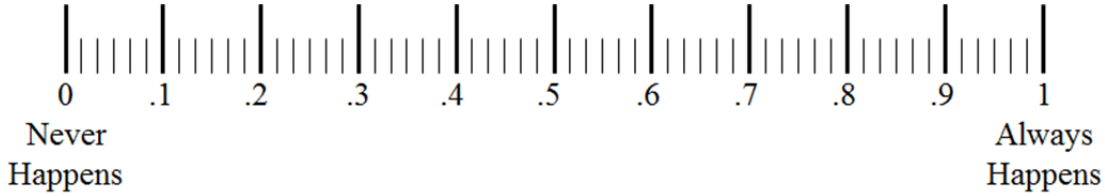
In COA 2, what do you feel is the percentage desired damage inflicted?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the percentage desired damage inflicted.
- Please draw a line on the above scale at the upper limit for the percentage desired damage inflicted.
- Please draw a line on the above scale at the lower limit for the percentage desired damage inflicted.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

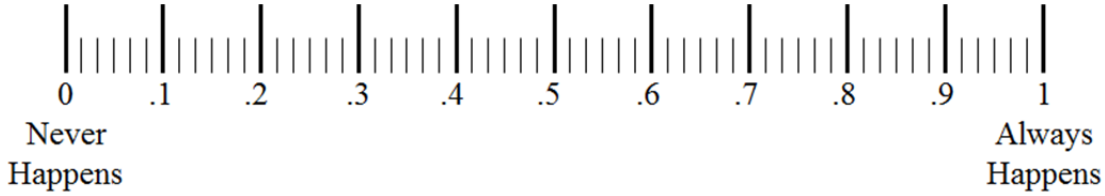
In COA 2, what do you feel is the probability of being attributed?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being attributed.
- Please draw a line on the above scale at the upper limit for the probability of being attributed.
- Please draw a line on the above scale at the lower limit for the probability of being attributed.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

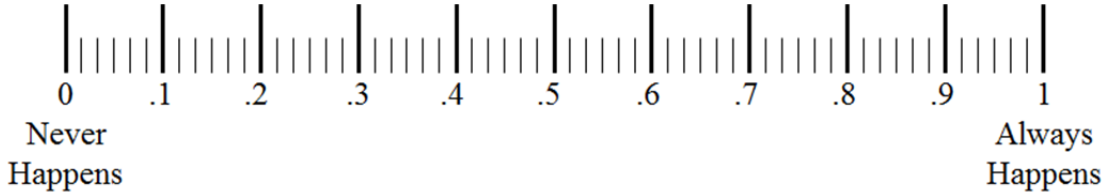
In COA 2, what do you feel is the probability of being compromised?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being compromised.
- Please draw a line on the above scale at the upper limit for the probability of being compromised.
- Please draw a line on the above scale at the lower limit for the probability of being compromised.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

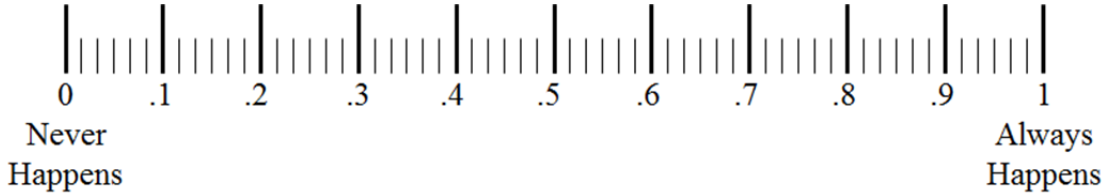
In COA 3, what do you feel is the percentage desired damage inflicted?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the percentage desired damage inflicted.
- Please draw a line on the above scale at the upper limit for the percentage desired damage inflicted.
- Please draw a line on the above scale at the lower limit for the percentage desired damage inflicted.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

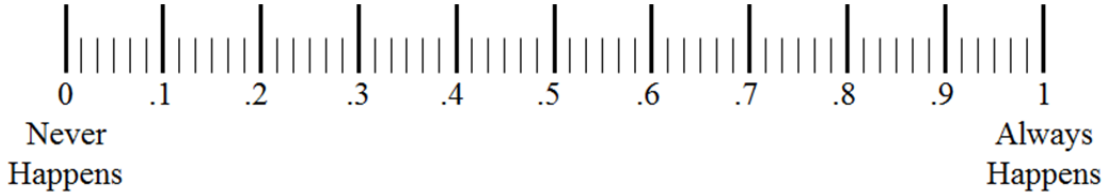
In COA 3, what do you feel is the probability of being attributed?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being attributed.
- Please draw a line on the above scale at the upper limit for the probability of being attributed.
- Please draw a line on the above scale at the lower limit for the probability of being attributed.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

In COA 3, what do you feel is the probability of being compromised?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being compromised.
- Please draw a line on the above scale at the upper limit for the probability of being compromised.
- Please draw a line on the above scale at the lower limit for the probability of being compromised.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

BACKGROUND

It is five years from now and authority to conduct computer network exploitation (CNE) and computer network attack (CNA) has been partially delegated to COCOMs. CNE actions must be coordinated through USCYBERCOM, the Functional Combatant Command responsible for global cyber operations. USCYBERCOM supports Geographic Combatant Command (GCC) with de-confliction, initial intelligence, assigned access points for operations, and capabilities. Primacy for all operations resides at USCYBERCOM to support de-confliction efforts. Command and control of cyber operations resides at the GCC once the operation is approved and commences. All computer network attack (CNA) actions taken by GCCs must have final approval from the national level authorities after review by the Joint Chiefs of Staff (JCS).

The Republic of Aragon has long been an ally of the United States and has allowed forward basing of U.S. soldiers as part of theater security agreements and treaties. This is in conflict with Aragon's neighbor, The Peoples' Democratic Republic of Krasnovia, which is a technological peer to Iran, South Korea, and India. Krasnovia has long wanted U.S. forces to leave the region. Recently, tensions between Aragon and Krasnovia have risen and rhetoric from Krasnovia has increased. This peaked last week with Krasnovia shooting down an Klondikian military helicopter resulting in no survivors. Krasnovia claims that the helicopter violated the sovereign airspace and acted in self-defense.

To prevent attribution of cyber activities, the Krasnovia government relies upon state-sponsored contracted companies to conduct cyber operations to meet government operational goals. These companies are given financial support, intelligence, and resources for their operations, along with government-provided protection. Recent national level intelligence indicates that a Krasnovia company, ممکن است خدا (English: Allah's Might; (AM)), has targeted U.S. and Aragon networks with malware. The application of malware differs from site to site. Both U.S. and Aragon networks have suffered from both intelligence gathering and denial of service attacks. None of the attacks within the U.S. have been within networks deemed to be critical infrastructure or key resources. However, the attacks have been highly publicized but not publicly attributed due to U.S. equities for intelligence gathering.

COMMANDER'S INTENT

AM infrastructure has been identified and national level authorities have ordered that a CNA operation be undertaken to stop the attacks. As AM is physically located within this GCC's area of operations, USCYBERCOM has tasked this GCC with this operation. USCYBERCOM has dictated that the attack will be demonstrative to both AM and Krasnovia that the U.S. knows they are responsible. However, attribution of the U.S. cyber operations infrastructure must be protected. Additionally, top prevent collateral

damage, the operational effects cannot expand beyond the AM networks. The commander has expressed his goals of this operation as attaining destruction, avoiding detection, and avoiding attribution.

The targeted machines are Lenovo laptops using Window 7, 64 bit with the bitlocker feature turned on. This network is also using a heuristics-based Qihoo 360 personal security product (PSP) with a cloud-based analytical engine. The network consists of Hauwei routers and switches, Lenovo laptops all running the same operating system and PSP, ZTE firewalls, and Dell Power Edge file servers implementing RAID 1. The total usable space of the servers is four terabytes. NSA estimates, from previous operations, that five gigabytes of malware projects are housed within the servers. Success of this operation is two-fold: First, the malware projects must be downloaded and analyzed for future signatures to protect DOD networks. This task will be undertaken by NSA. The GCC is responsible for the second task, destroying all information residing on the file servers by corrupting the information or by rendering the information inaccessible. In whatever method is used, the information must be unrecoverable.

USCYBERCOM has identified CIA and NSA as other friendly actors within the network. NSA has primacy within the network, however, has agreed to the COCOM actions. NSA has provided a known access point and they, along with the CIA, have withdrawn all their capabilities from the AM network. Additionally, NSA has provided a user credential. This credential is believed to have read/ write access to the file servers.
USCYBERCOM has provided three potential CNA capability courses of action (COA) for consideration and choice by the COCOM Command and Staff. **As the GCC staff, you must order the COAs in precedence of most preferred to least preferred for consideration by the commander for a decision.**

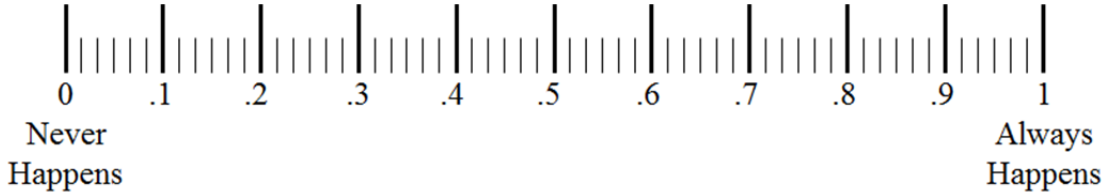
COURSES OF ACTION

COA 1: MONKEYSTOMP is a capability that removes all the file allocation pointers, overwrites the hard drives, and then encrypts the hard drive before deleting the key and restarting the device. This capability has the projected ability to overwrite and encrypt drives at a rate of 1GB every five minutes based on the file server specifications. MONKEYSTOMP has not been used in real operations but virtualized testing indicates host-based PSPs do not detect this capability. However, it is unknown if a cloud-based PSP will detect it due to the inability to create a virtualized environment that replicates the real PSP ability. Due to the past performance of Qihoo 360, is it estimated that a 40% chance of discovery and quarantine will occur prior to activation. This capability can be configured and tested for this specific operation in between one and two weeks with a most likely completion at two weeks.

COA 2: HYPEROPOSSUM is a capability that causes device hard drives to accelerate to maximum speed and then the read/ write heads of the server hard drives to drag the plates, rendering them unreadable. This capability has been used limitedly in the past for real operations but on smaller applications such as individual laptops and desktops. This incarnation of the capability performed as expected in virtualized testing but required an on-net operator to activate the capability on each server. Once activated, MONKEYSTOMP cannot be stopped; however, the risk elevates for detection and attribution for a manual activation of the capability. It is estimated that a 20% chance of detection exists and a 40% chance of attribution exists if detected. This capability can be configured and tested for this specific operation in between one and three weeks with a most likely completion at two weeks.

COA 3: ANGRYDRAGON is a capability that uses the properties of RAID to propagate and initiate. This capability monitors the RAID controllers to ensure it reaches all RAID participants. When the RAID update is complete, ANGRYDRAGON begins to overwrite all information on the drives. This capability has not been used in real operations. Virtualized testing indicates a 20% chance of propagation outside of the targeted servers if users have mapped a file server as a network drive on a laptop or desktop. If propagation outside of the server occurs, each device ANGRYDRAGON moves to is a possible vector for further propagation if that device is has other mapped network locations, peer to peer connections, USB connected devices or storage, or if the device is dual-homed on the networks. This capability can be configured and tested for this specific operation in between two and three weeks with a most likely completion at three weeks.

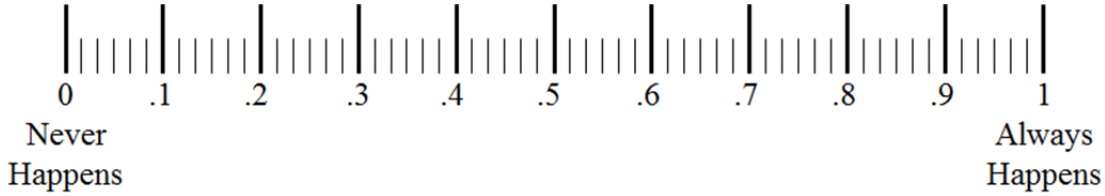
In COA 1, what do you feel is the percent of the required damage inflicted?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the percent of the required damage inflicted.
- Please draw a line on the above scale at the upper limit for the percent of the required damage inflicted.
- Please draw a line on the above scale at the lower limit for the percent of the required damage inflicted.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

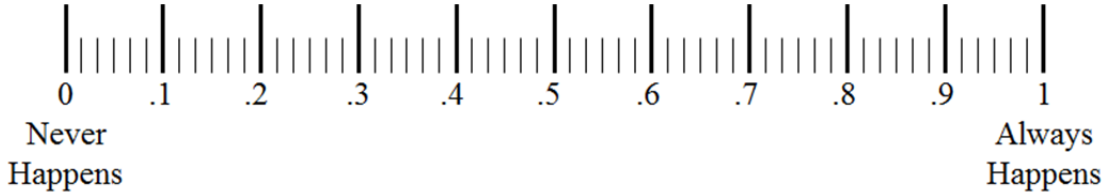
In COA 1, what do you feel is the probability of being detected?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being detected.
- Please draw a line on the above scale at the upper limit for the probability of being detected.
- Please draw a line on the above scale at the lower limit for the probability of being detected.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

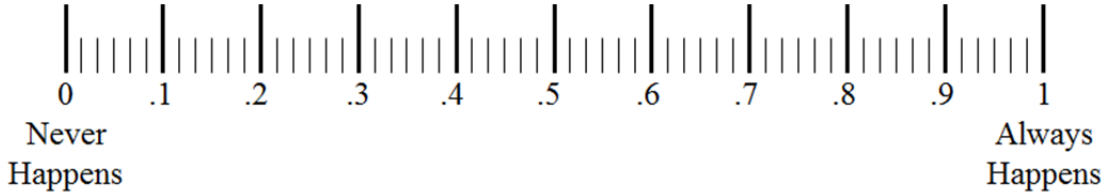
In COA 1, what do you feel is the probability of being attributed?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being attributed.
- Please draw a line on the above scale at the upper limit for the probability of being attributed.
- Please draw a line on the above scale at the lower limit for the probability of being attributed.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

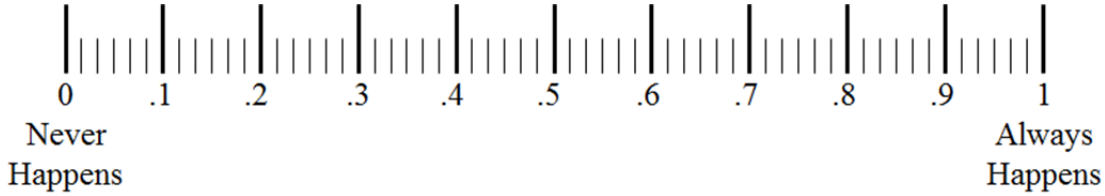
In COA 2, what do you feel is the percent of the required damage inflicted?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the percent of the required damage inflicted.
- Please draw a line on the above scale at the upper limit for the percent of the required damage inflicted.
- Please draw a line on the above scale at the lower limit for the percent of the required damage inflicted

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

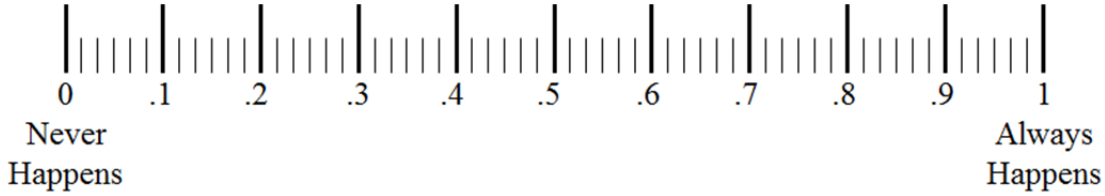
In COA 2, what do you feel is the probability of being detected?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for t the probability of being detected.
- Please draw a line on the above scale at the upper limit for the probability of being detected.
- Please draw a line on the above scale at the lower limit for the probability of being detected.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

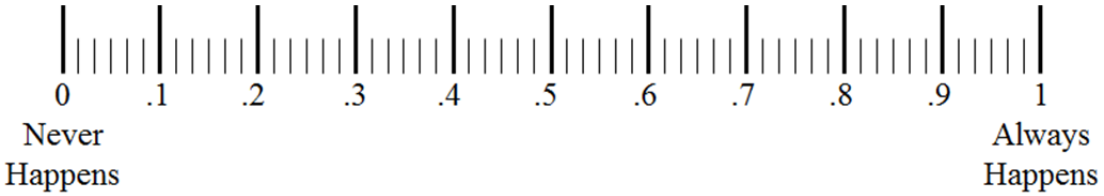
In COA 2, what do you feel is the probability of being attributed?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being attributed.
- Please draw a line on the above scale at the upper limit for the probability of being attributed.
- Please draw a line on the above scale at the lower limit for the probability of being attributed.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

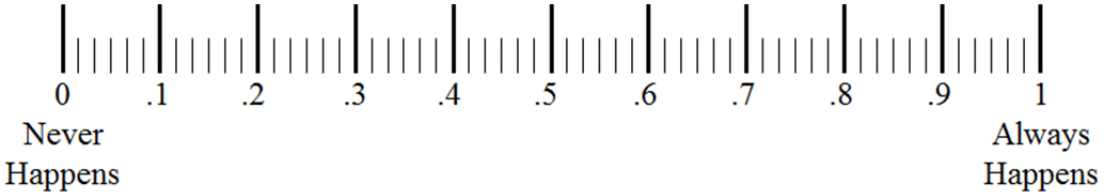
In COA 3, what do you feel is the percent of the required damage inflicted damage inflicted?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the percent of the required damage inflicted.
- Please draw a line on the above scale at the upper limit for the percent of the required damage inflicted.
- Please draw a line on the above scale at the lower limit for the percent of the required damage inflicted.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

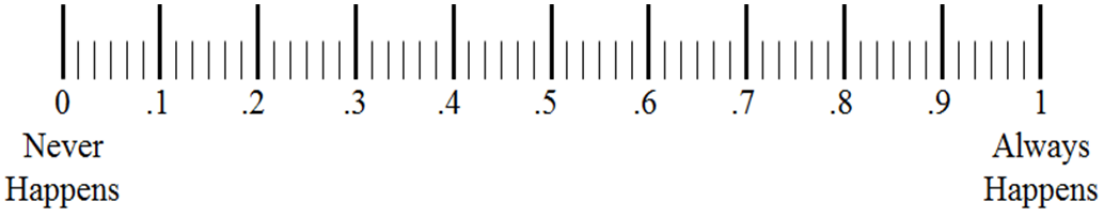
In COA 3, what do you feel is the probability of being detected?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being detected.
- Please draw a line on the above scale at the upper limit for the probability of being detected.
- Please draw a line on the above scale at the lower limit for the probability of being detected.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

In COA 3, what do you feel is the probability of being attributed?



- Remember that LV and UV define the interval that you are confident that will contain the REAL value "90% of the time."
- Please draw a line on the above scale at the most likely value for the probability of being attributed.
- Please draw a line on the above scale at the upper limit for the probability of being attributed.
- Please draw a line on the above scale at the lower limit for the probability of being attributed.

Most Likely Value =_____
Upper Limit Value = _____
Lower Limit Value =_____

Participant Demographic Information

What is your age?
What is your military service?
How long have you been in the military?
What is your rank?
What is your current position?
How long have you held this position?
What is your highest civilian education completed?
What IT/ IA certifications do you possess?

Have you ever worked within national level cyber activities (NSA, CIA, DIA, etc.)?

If so, how long and in what capacity?

Have you graduated from any of the following?

- JNAC
- JCAC
- BCNOPC
- JACWC
- Cyber 200
- Cyber 300
- SNIP
- CNODP

APPENDIX G. PARTICIPANT DEMOGRAPHICS

Participant	AGE	MIL/ CIV	YRS MIL?	ED LEVEL	WORK NATL CYBER?	NATL EXP YRS	JNAC	JCAC	BCNOPC	JACWC	CYBER 200	CYBER 300	SNIP	CNODP
P001	56	CIV	20	HS	YES	3	NO	NO	YES	NO	NO	NO	NO	NO
P002	40	MIL	20	BS	NO	0	NO	NO	NO	NO	NO	NO	NO	NO
P003	42	MIL	24	MS	YES	1	YES	NO	NO	YES	NO	NO	NO	NO
P004	50	CIV	8	MS	NO	0	NO	NO	NO	NO	NO	NO	NO	NO
P005	50	CIV	21	HS	YES	2.5	NO	NO	YES	NO	NO	NO	NO	NO
P006	42	CIV	8	MS	YES	6	NO	YES	NO	NO	NO	NO	NO	NO
P007	35	MIL	16	MS	YES	9	NO	NO	NO	NO	NO	NO	NO	NO
P008	53	CIV	0	MS	NO	0	NO	NO	NO	NO	NO	NO	NO	NO
P009	40	MIL	18	MS	NO	0	NO	NO	NO	NO	YES	YES	NO	NO
P010	42	MIL	19	PhD	NO	0	NO	NO	NO	NO	YES	YES	NO	NO
P011	40	MIL	17	MS	NO	0	NO	NO	NO	NO	NO	YES	NO	NO
P012	40	MIL	14	MBA	YES	2	NO	NO	NO	NO	YES	NO	NO	NO
P013	45	MIL	22	MS	NO	0	NO	NO	NO	NO	NO	NO	NO	NO
P014	32	MIL	11	MBA	NO	0	NO	NO	NO	NO	NO	NO	NO	NO
P015	46	MIL	21	PhD	YES	3	NO	NO	NO	NO	NO	NO	NO	NO
P016	43	CIV	20	MS	NO	0	YES	NO	NO	NO	NO	NO	NO	NO
P017	43	CIV	21	MS	YES	4	NO	YES	NO	NO	YES	YES	NO	NO
P018	57	CIV	33	MS	NO	0	NO	NO	NO	NO	NO	NO	NO	NO
P019	34	CIV	10	PhD	YES	12	NO	NO	NO	NO	NO	NO	NO	NO
P020	38	MIL	16	PhD	NO	0	NO	NO	NO	NO	NO	YES	NO	NO
P021	45	MIL	27	MS	NO	0	NO	NO	NO	NO	NO	NO	NO	NO
P022	53	CIV	0	MS	YES	9	NO	NO	YES	NO	NO	NO	NO	NO
P023	49	CIV	23	JD	YES	5	NO	NO	NO	NO	NO	NO	NO	NO
P024	35	MIL	15	MBA	NO	0	NO	NO	NO	NO	NO	NO	NO	NO
P025	50	CIV	20	MS	NO	0	YES	NO	YES	NO	NO	NO	NO	YES
P026	47	CIV	25	MS	NO	0	NO	NO	NO	YES	NO	NO	NO	NO
P027	40	CIV	21	BS	NO	0	NO	NO	NO	NO	YES	YES	NO	NO
P028	36	MIL	14	MS	NO	0	YES	NO	NO	NO	YES	YES	NO	NO
P029	31	CIV	9	MS	NO	0	NO	NO	NO	NO	NO	NO	NO	NO
P030	43	MIL	22	MS	YES	4	NO	NO	NO	NO	NO	YES	NO	NO
P031	35	CIV	13	JD	NO	0	YES	NO	YES	NO	YES	YES	NO	NO
P032	45	CIV	0	MS	NO	0	YES	NO	NO	YES	NO	YES	NO	NO
P033	54	CIV	24	MS	YES	35	NO	NO	NO	NO	NO	NO	NO	NO
P034	37	MIL	18	MS	YES	3	NO	NO	NO	NO	NO	NO	NO	NO
P035	44	CIV	20	MS	YES	6	NO	NO	NO	NO	NO	NO	NO	NO
P036	42	MIL	20	MS	NO	0	NO	NO	NO	NO	YES	YES	NO	NO
P037	51	CIV	29	MS	NO	0	NO	NO	NO	NO	NO	NO	NO	NO
P038	40	MIL	18	MS	YES	3	NO	NO	NO	NO	NO	YES	YES	YES
P039	45	MIL	25	MS	YES	4	NO	NO	NO	NO	NO	YES	NO	NO
P040	33	MIL	13	BS	NO	0	NO	NO	NO	NO	YES	NO	NO	NO
P041	53	CIV	20	MBA	NO	0	NO	NO	YES	NO	NO	NO	NO	NO
P042	37	MIL	13	MA	NO	0	NO	NO	NO	NO	NO	NO	NO	NO
P043	44	CIV	20	MS	NO	0	NO	NO	NO	NO	NO	NO	NO	NO
P044	27	MIL	5	BS	NO	0	NO	NO	NO	NO	NO	NO	NO	NO
P045	48	MIL	24	MS	NO	0	NO	NO	NO	YES	YES	YES	NO	NO
P046	43	MIL	25	MS	NO	0	NO	NO	NO	NO	YES	YES	NO	NO
P047	48	CIV	0	MA	YES	2	NO	NO	NO	NO	NO	NO	NO	NO
P048	46	CIV	0	AA	YES	5	NO	NO	NO	NO	NO	NO	NO	NO
P049	42	MIL	19	MS	YES	5	NO	NO	NO	YES	NO	NO	NO	NO
P050	39	CIV	15	MS	YES	1	NO	NO	NO	NO	NO	NO	NO	NO
P051	50	CIV	10	BS	YES	2	NO	NO	NO	NO	NO	NO	NO	NO
P052	56	CIV	17	PhD	YES	6	NO	NO	NO	NO	NO	NO	NO	NO
P053	41	MIL	19	MS	YES	4	NO	NO	NO	NO	NO	NO	NO	NO
P054	52	MIL	10	MS	YES	10	NO	NO	NO	NO	NO	NO	NO	NO
P055	46	MIL	26	MS	YES	1	YES	NO	NO	NO	NO	YES	NO	NO
P056	38	MIL	15	MS	YES	1	NO	NO	YES	NO	NO	NO	NO	NO
P057	44	CIV	27	MS	YES	1	NO	NO	NO	NO	NO	NO	NO	NO
P058	37	MIL	16	BS	YES	3	YES	NO	NO	NO	NO	NO	NO	NO
P059	43	MIL	24	BS	YES	1	NO	NO	NO	NO	NO	NO	NO	NO
P060	50	CIV	20	MA	YES	11	YES	NO	YES	NO	NO	NO	NO	NO

AVG AGE	COUNT MIL	AVG MIL YRS	COUNT HS	COUNT NATL EXP	AVG NATL EXP	COUNT JNAC	COUNT JCAC	COUNT BCNOPC	COUNT JACWC	COUNT CYBER 200	COUNT CYBER 300	COUNT SNIP	COUNT CNODP
43.45	31	17	2	31	2.741667	9	2	8	5	11	16	1	2

COUNT CIV	# MIL	COUNT BS	COUNT NATL INEX	AVG USCC EXP
29	60	7	27	3.785714

COUNT MS
36

COUNT MA
3

COUNT MBA
4

COUNT JD
3

COUNT PhD
5

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX H. PARTICIPANT SCENARIOS AND GRAPHICS

A. BACKGROUND

It is five years from now and authority to conduct surveillance and reconnaissance (SR), also known as computer network exploitation (CNE) and computer network attack (CNA) has been partially delegated to combatant commands (CCMD). SR/ CNE actions must be coordinated through USCYBERCOM, the Functional Combatant Command responsible for global cyber operations. USCYBERCOM supports Geographic Combatant Command efforts with de-confliction, initial intelligence, assigned access points for operations, and capabilities. Primacy for all operations resides at USCYBERCOM to support de-confliction efforts. Command and control of cyber operations resides at the CCMD once the operation is approved and commences. All CNA actions taken by CCMDs must have final approval from the national level authorities after review by the Joint Chiefs of Staff.

The Republic of Ameristan has long been an ally of the United States and has allowed forward basing of U.S. soldiers as part of theater security agreements and treaties. This is in conflict with Ameristan's neighbor, The Peoples' Democratic Republic of Koonistan, which is a technological peer to China, Russia, and Israel. Koonistan has long wanted U.S. forces to leave the region. Recently, tensions between Ameristan and Koonistan have risen and rhetoric from Koonistan has increased. This peaked last week with Koonistan shooting down an Ameristanian military helicopter resulting in no survivors. Koonistan claims that the helicopter violated the sovereign airspace and acted in self-defense.

Recent Human Intelligence (HUMINT) reports indicate a draft plan for a possible invasion of Ameristan has been created. The report indicated that a PowerPoint presentation of nearly 15MB in size along with a nearly 1MB Word document exists. Although the potential for an invasion of Ameristan by Koonistan is unlikely, the CCMD commander requires information from Koonistan's Ministry of Defense in order to ascertain Koonistan's intentions. This proposed action has been endorsed by

USCYBERCOM. USCYBERCOM has identified only one viable access point in the targeted network. This access point resides in a Koonistan MoD user laptop that has been recently implanted by USCYBERCOM on behalf of the CCMD. In the event that this access point is compromised access to this network will be lost and time consuming reconnaissance will be needed. This computer has local administrative credentials already but elevated privileges will be needed to traverse or execute capabilities. USCYBERCOM also has confirmed domain administrative credentials. USCYBERCOM has identified GCHQ as another friendly actor within the network; however, USCYBERCOM and the CCMD have primacy.

B. COMMANDER'S INTENT

The CCMD commander is interested in only two objectives: gaining more intelligence and decreasing the probability of detection of this operation. More in depth conversations reveal the commander's relative value between the two is 60% for avoiding detection versus 40% for gathering intelligence. Success in this operation is the exfiltration of the Word document at a minimum. The commander prefers both the Word document and the PowerPoint however. The potential for attribution to the U.S. and inadvertently to GCHQ is a major concern. Additionally, with only one access point available, follow-on operations would be impossible for the foreseeable future. Because of these considerations, this operation is considered to be a high risk operation. The commander's guidance is that this operation will commence within 10 days. This deadline is based off of the upcoming Theater Security Cooperation conference. If this deadline cannot be met, the staff must inform the commander as soon as possible and provide a timeline of events.

The targeted machine is the Minister of Defense's laptop which is three hops away from the access point. It is a Lenovo laptop using Window 7, 64 bit with the bitlocker feature turned on. The operation is expected to occur during hours in which the laptop will be powered on and being used. This laptop is using a heuristics-based Kapersky PSP with a local library of signatures that is updated by the admins weekly. The MoD network consists of Cisco routers and switches, Lenovo laptops all running the

same operating system and PSP, and Microtik firewalls. Koonistan does not rely upon foreign ally support for network defense or analysis. Consequently, Koonistan has never detected friendly operations within their networks. However, non-routine Kaspersky support of Koonistan networks discovered a friendly capability 12 months ago.

USCYBERCOM has provided three potential SR/ CNE capability courses of action (COA) for consideration and choice by the CCMD Command and Staff. As the CCMD staff, you must order the COAs within each of the two groups in precedence of most preferred to least preferred for consideration by the commander for a decision.

GROUP 1 COURSES OF ACTION

COA A: STOLENCREDIT is an open-sourced tool that has been slightly modified and is available immediately. This tool hijacks an operating system function and will allow U.S. forces to monitor communications along with file creation/ modification/ deletion. This tool also has the capacity to accept a plug-in for monitoring room audio through the computer's microphone. However, the original open-sourced version of this tool is known in the computer security and hacker circles. This tool creates a process that is noticeable to system admins that is unique and tell-tale if detected. In virtualized testing, this tool has a 50/ 50 chance of being detected by Kaspersky.

COA B: MONKEYSAURUSREX is a tool recently created by the USAF that claims to be able to be able to monitor communications along with file creation/ modification/ deletion. As a recently developed tool, this capability has no additional features or plug-ins for room audio monitoring or anything else. This capability has been tested in a virtualized environment and the capability was not detected by Kaspersky. However, this tool has not been used in a real operation. An experienced system administrator knowing what to look for may be able to detect this capability as it shares the similar methodology for persistence within the network that the capability detected by the Chinese used 12 months ago. This capability can be configured and tested for this specific operation in between one and three weeks with a most likely completion at two weeks.

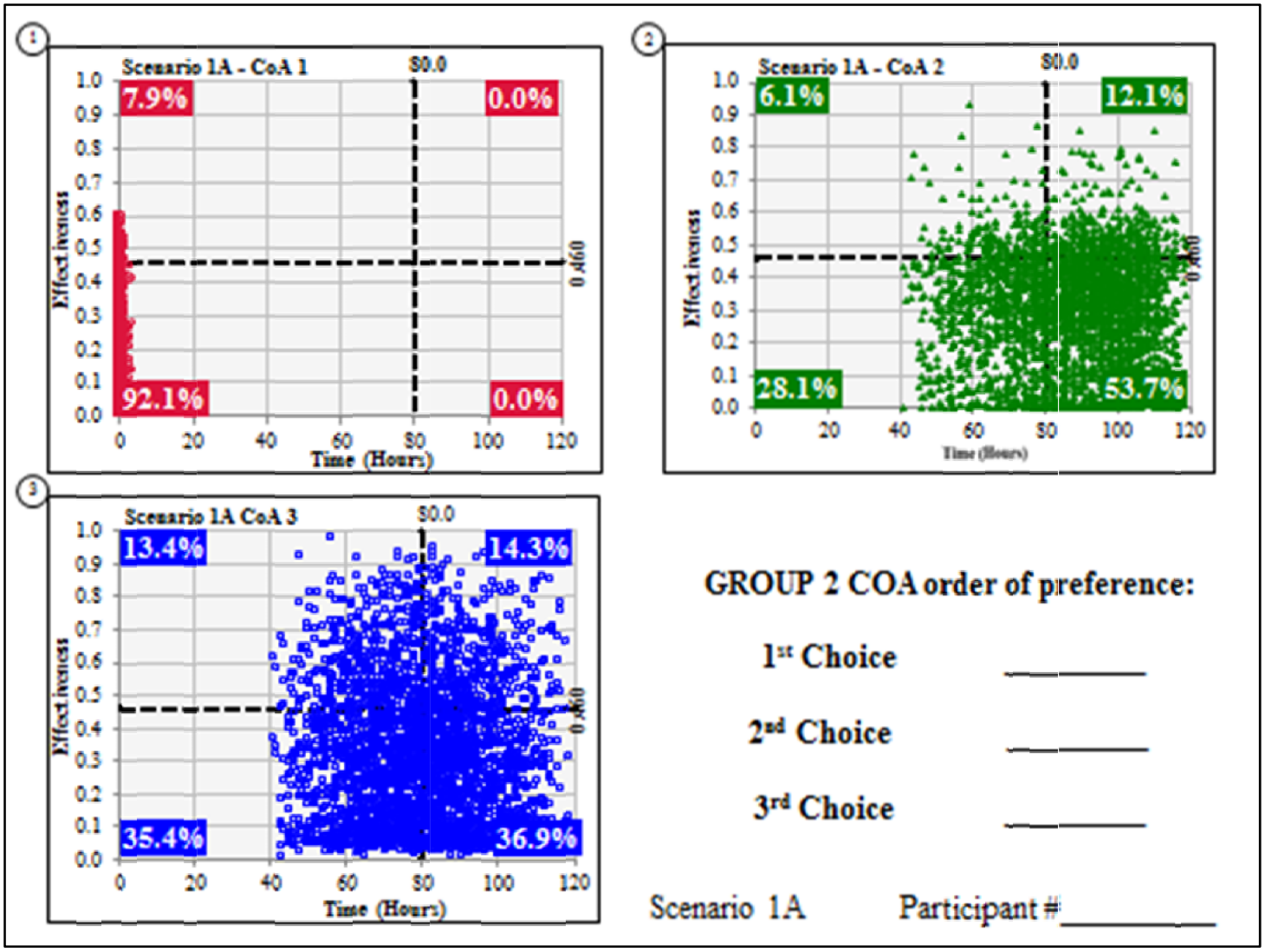
COA C: COFFEEADDICT is a former NSA tool given to USCYBERCOM for operations. COFFEEADDICT was used globally by NSA for intelligence gathering until it was replaced with by another tool with more stealth and capability. This capability has been used in real operations last year where it was not detected by Kaspersky. Recent virtualized environment testing with the latest version of Kaspersky resulted in the capability being detected. It is unknown what change has occurred within Kaspersky to detect COFFEEADDICT. It is also unknown what version of Kapersky is being used on the target machine, only that library updates are completed weekly. If COFFEEADDICT is used, the capability to monitor communications along with file creation/ modification/ deletion exists along with room audio monitoring. Additionally, a plug-in to capture still photos using the laptop camera exists, but this plug-in has not been tested against this combination of hardware and software in virtualized or real environments. This capability can be configured and tested for this specific operation in between one and three weeks with a most likely completion at two and a half weeks.

GROUP 1 COA order of preference:

1st Choice _____

2nd Choice _____

3rd Choice _____


1
Scenario 1A - CoA 1
$0.0
7.9%
0.0%
92.1%
0.0%
Effectiveness
Time (Hours)
2
Scenario 1A - CoA 2
$0.0
6.1%
12.1%
28.1%
53.7%
Effectiveness
Time (Hours)
3
Scenario 1A CoA 3
$0.0
13.4%
14.3%
35.4%
36.9%
Effectiveness
Time (Hours)
GROUP 2 COA order of preference:
1st Choice _____
2nd Choice _____
3rd Choice _____
Scenario 1A
Participant #_____

1B BACKGROUND

The operation continues and the Minister of Defense's laptop has information exfiltrated without the operation being discovered. Analysis of the information points to Koonistan's plans to conduct small-scale guerilla attacks within Ameristan for the purpose of eroding trust and friendship between Ameristan and the U.S. Koonistan forces have escalated training, readiness, and forward deployment of forces near the Ameristan border as the rhetoric increases, particularly after the downing of the Ameristanian military helicopter.

The CCMD commander has requested and received authority to conduct a CNA operation within the MoD network. The desired endstate of this attack is two-fold: First, to disrupt the planning of the guerilla attacks in Ameristan and second, to demonstrate to the Koonistan leadership the vulnerabilities of their sensitive networks by our actions. This operation will be considered successful if all of the information on the targeted machine from the first phase of the operation is rendered inaccessible and unrecoverable. The targeted laptop has a 1TB SATA hard drive.

1B COMMANDER'S INTENT

Deterrence of Koonistan aggression is the goal of the CCMD commander. For this operation, the commander values the outcome of this operation as 60% (Destruction; denying access to the data) versus 40% (avoiding attribution). The CCMD commander wishes to demonstrate that a foreign actor is in Koonistan networks, however direct attribution to the U.S. is to be avoided. GCHQ has been informed of this potential operation and has exfiltrated all of their capabilities from the network. Because of these considerations, this operation is considered to be a moderate risk operation. The commander's guidance is that this operation will commence within 10 days. This deadline is based off of the upcoming multi-national exercise. If this deadline cannot be met, the staff must inform the commander as soon as possible and provide a timeline of events.

Koonistan is assessed as a low risk for retaliation within U.S. critical infrastructure or key resources (CI/KR). Koonistan cyber actors has never been found within CI/KR, although they have claimed to infiltrated electrical power generation and distribution systems. Intelligence confirming this has not been conclusive. Koonistan has historically never allied with other nations to conduct cyber operations and the belief is that this will continue.

The Joint Chiefs of Staff and the President have approved this action. USCYBERCOM has expressed concern that the CNA effect may be detected by the Kapersky PSP if not executed immediately. This analysis is derived from virtualized modeling of the targeted environment. A delayed execution of the attack would likely result in the PSP detecting,

quarantining, and passing the code to Kapersky for analysis. USCYBERCOM has provided three potential CNA capability courses of action (COA) for consideration and choice by the CCMD Command and Staff. **As the CCMD staff, you must order the COAs within each of the two groups in precedence of most preferred to least preferred for consideration by the commander for a decision.**

GROUP 1 COURSES OF ACTION

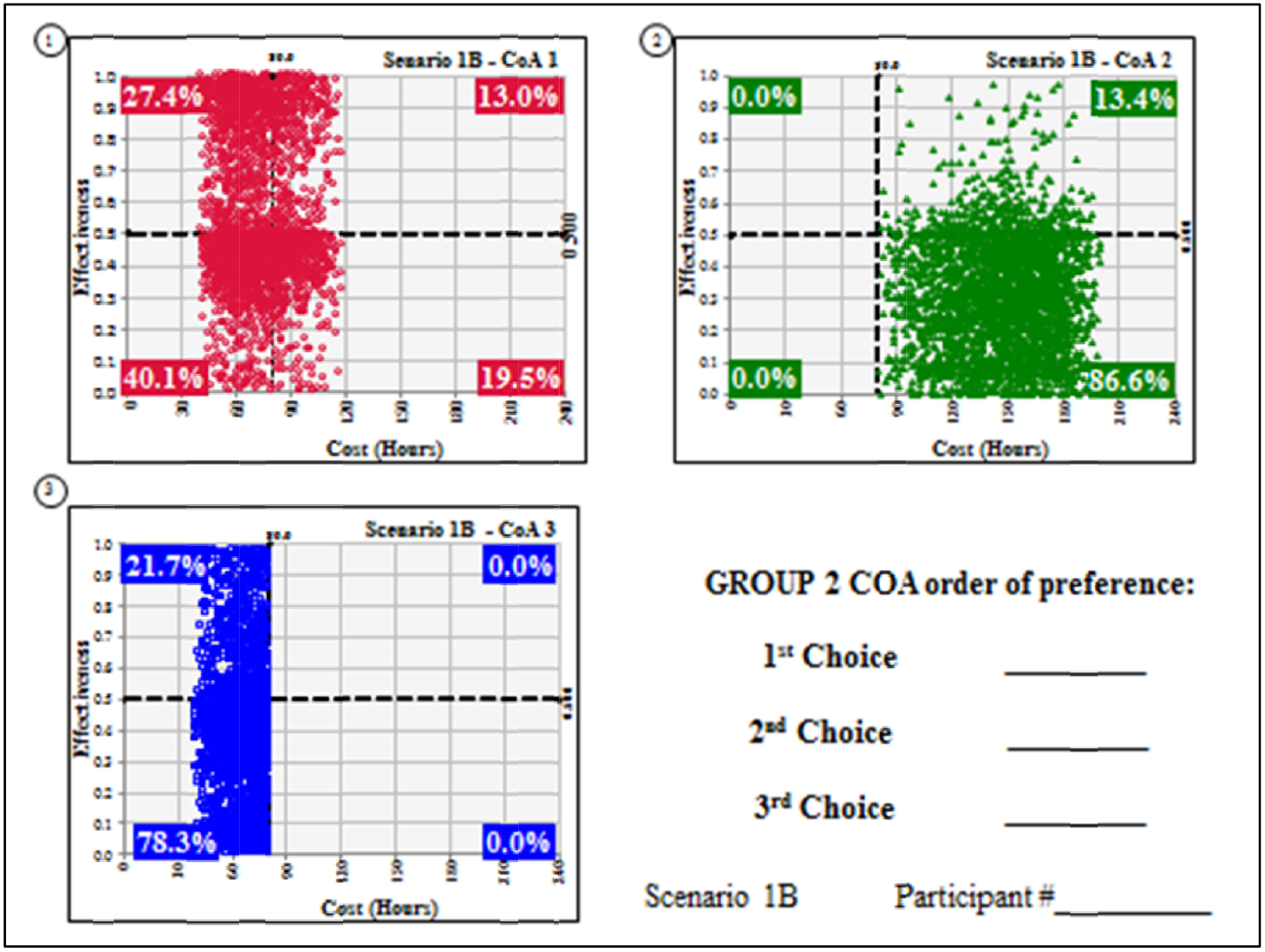
COA A: ROADKILLDEER is a capability that encrypts the overwritten drive, then deletes the encryption key, and forces the computer to restart. It is predicted that this effect is irreversible if allowed to run completely. It is assessed that a 1TB drive will take approximately 10 minutes for the capability to completely take effect. This capability has a signature and may be traced to the U.S. due to its sophistication. This tool has not been used in real operations and only in a virtualized environment. Within the virtualized environment, Kaspersky quarantined this effect and prevented ROADKILLDEER from working 40% of the time. The software developers estimate that to configure and test this capability for the specific devices in this operation will most likely take three and a half weeks, but potentially can be completed in two weeks, but no more than five weeks. This capability can be configured and tested for this specific operation in between two and five weeks with a most likely completion at four weeks.

COA B: FORGETFULHUSBAND is a capability that overwrites the hard drive with random characters over and over. This capability also destroys the file allocation table for the hard drive. In essence, this overwritten drive becomes one large file of gibberish. This capability has been used previously in a real-world operation. This previous operation was blamed on the US, but no forensic proof could be offered. The previous operation used a different hardware and software combination and the PSP did not detect the capability. This tool was not detected in virtualized testing for the hardware and software combination faced in this operation. This capability can be configured and tested for this specific operation in between one and three weeks with a most likely completion at one and a half weeks.

COA C: DRUNKENFRATBOY is a capability that drags the read/ write head of the hard drive across the platters, rendering them unreadable. This capability increases the revolutions of the hard drive to the maximum of the hard drive and then applies the head to the metal oxide disk surfaces. This capability has not been used in real operations but has been tested on real machines. In testing on real machines, the capability commencing is immediate. This capability can be heard by the victim laptop user as the heads scrape across the platters. Additionally, because of what this capability is doing, the user will notice that no new information will be retrieved or saved once the capability commences. This capability has to run from a file written from the hard drive. This raises the potential

for Kaspersky detecting this capability. In real-machine testing, Kaspersky detected the capability in a virus scan of the entire disk. Tradecraft used to write the file to disk enabled PSP evasion. The user of the laptop removing power to the machine could compromise the operation and bring attribution. Because of the sophistication of this capability, it is believed that if found, this capability will be attributed to the U.S. if the capability is prevented from fully running. This capability can be configured and tested for this specific operation in between one and two weeks with a most likely completion at two weeks.

GROUP 1 COA order of preference:
1st Choice _____
2nd Choice _____
3rd Choice _____


1
Scenario 1B - CoA 1
27.4%
13.0%
40.1%
19.5%
Effect Index
Cost (Hours)
2
Scenario 1B - CoA 2
0.0%
13.4%
0.0%
86.6%
Effect Index
Cost (Hours)
3
Scenario 1B - CoA 3
21.7%
0.0%
78.3%
0.0%
Effect Index
Cost (Hours)
GROUP 2 COA order of preference:
1st Choice _____
2nd Choice _____
3rd Choice _____
Scenario 1B
Participant # _____

BACKGROUND

It is five years from now and authority to conduct surveillance and reconnaissance (SR), also known as computer network exploitation (CNE) and computer network attack (CNA) has been partially delegated to combatant commands (CCMD). SR/ CNE actions must be coordinated through USCYBERCOM, the Functional Combatant Command responsible for global cyber operations. USCYBERCOM supports Geographic Combatant Command efforts with de-confliction, initial intelligence, assigned access points for operations, and capabilities. Primacy for all operations resides at USCYBERCOM to support de-confliction efforts. Command and control of cyber operations resides at the CCMD once the operation is approved and commences. All CNA actions taken by CCMDs must have final approval from the national level authorities after review by the Joint Chiefs of Staff.

The Islamic State (IS) has continued to use the Internet to recruit, spread propaganda, and command and control decentralized operations over a wide swath of land in the Middle East. This online activity escalated with the video of a captured U.S. forces member being killed for propaganda purposes.

The CCMD commander, in coordination with the Theater Special Operations Command (TSOC), has designated five IS personnel as high payoff targets (HPTs). These five people not only are instrumental in the operations and facilitation of IS operations, but are believed to be directed connected with the death of the above mentioned U.S. service member. The HPTs are believed to coordinate activities through instant messaging systems, shared email accounts, and file sharing sites. One of the instant messaging usernames has been identified and two others are suspected, but not confirmed. The shared email username and password has been identified along with one HPT's file sharing credentials. Initial intelligence indicates that the HPTs use Android phones of various manufacturers and Internet cafes providing Windows-based desktop computers with Internet access.

COMMANDER'S INTENT

The CCMD commander has two goals: gathering intelligence and avoiding detection. The CCMD requires that a SR/ CNE operation be undertaken to confirm the identity of the five HPTs by attaining a pictures of the targets using integrated cameras native to the devices. Additionally, the commander requires that geolocation of the targets must be attained and refreshed every fifteen minutes at a minimum in order to assist other intelligence assets in establishing patterns of life for the five HPTs. Once the patterns of life have been established, the TSOC will plan for coordinated capture/ kill operations of the five HPTs.

The CCMD commander places equal value on intelligence gathering for this operation and avoiding detection. The commander wishes to achieve an overall minimum effectiveness of .47. The commander fears that if the operation is discovered or suspected the HPTs will change their methods of communications. No other friendly actors have been identified working in the IS networks or their associated means of online communications such as the email account, file sharing, and instant messaging service. Due to their low maturity of tradecraft and frequent use of public Internet cafes this group is considered a low sophistication of threat. Because of these considerations, this operation is considered to be a low risk operation. The commander's guidance is that this operation will commence within 14 days. This deadline is based off of guidance from national command authority. If this deadline cannot be met, the staff must inform the commander as soon as possible and provide a timeline of events.

USCYBERCOM has provided three potential SR/ CNE capability courses of action (COA) for consideration and choice by the COCOM Command and Staff. **As the CCMD staff, you must order the COAs within each of the two groups in precedence of most preferred to least preferred for consideration by the commander for a decision.**

GROUP 1 COURSES OF ACTION

COA A: BOOTYCALL is a mobile device capability that monitors the HPTs' instant messaging application on Android devices. This capability is delivered over Wi-Fi or USB connections masquerading as an operating system update that must be accepted by the phone owner. The HPTs will both need to believe that the operating system update is needed and also be in a known Wi-Fi location. BOOTYCALL covertly monitors the instant messaging applications and simultaneously sends the GPS location of the phone to a collection sensor using Wi-Fi. An additional plug-in is available to access and control the camera. This plug-in may be delivered to the phone remotely over Wi-Fi once BOOTYCALL has installed. This capability only can transmit over Wi-Fi and not over the cellular provider. BOOTYCALL has not been used in a real operation and in a virtualized testing environment this capability demonstrated a 10% chance of causing the phone to repeatedly restart. Testing also leads to the indication of none of the prominent personal security products (PSPs) for mobile devices detecting BOOTYCALL. This capability can be configured and tested for this specific operation in between one and three weeks with a most likely completion at one and a half weeks.

COA B: OVERSTAYEDGUEST is a capability delivered by modified documents in an email. This capability infects Windows-based computers that open the document with an implant that will call back to a predetermined listening post. OVERSTAYEDGUEST has the capacity for plug-ins that can covertly turn on a camera, record files that have been read, written, or modified, and modify Wi-Fi emittances for a non-standard pattern may

be used for geolocation. This capability has been used in real operations limitedly in the past due to the increasing sophistication of PSP vendors. Current virtualized testing indicates that OVERSTAYEDGUEST has a 40% chance of being detected by the top five PSPs being produced. The software developers responsible for virtualized testing expressed concern regarding the use of Internet cafes by the targets that may use one of the top five PSPs. This capability can be configured and tested for this specific operation in between one and three weeks with a most likely completion at two weeks.

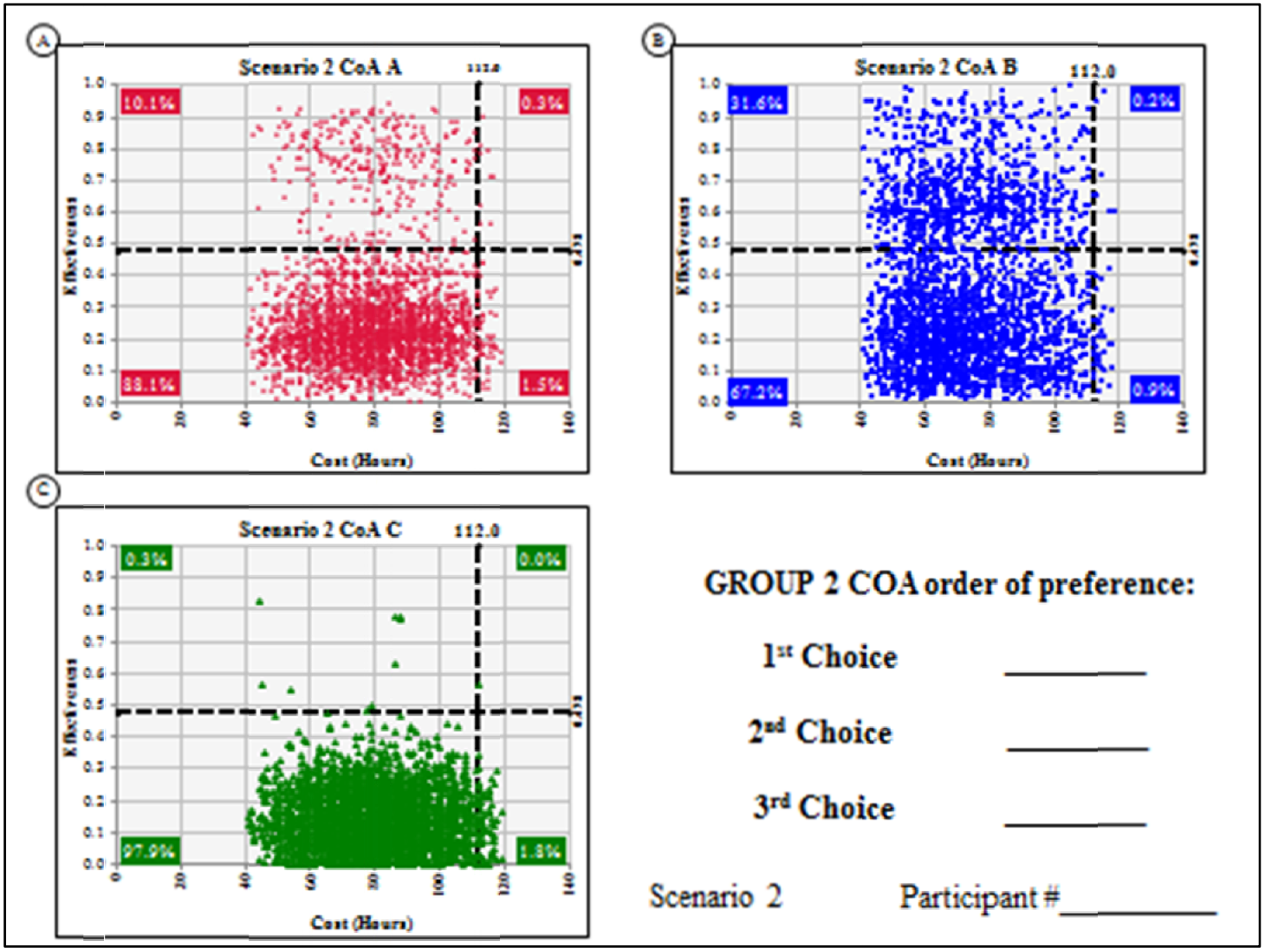
COA C: HOLIDAYREGIFT is a lightweight browser exploit that is compatible with Firefox and Chrome browsers in Android devices along with Windows laptops and desktops. This capability is delivered from downloading or opening an implanted file. The file sharing service will be the targeted mechanism of delivery. Once the implant is delivered and installed, HOLIDAYREGIFT will use the user agent string to download plug-ins as tasked. Plug-in capabilities include covertly operating the webcam (Windows only), gathering location information from the GPS to send periodic location updates through cellular transmission (Android only), USB proliferation to another device, and modifying the Wi-Fi modulation for potential geolocation (Windows and Android). This capability has not previously been used in real operations, but virtualized testing has determined that mobile devices have a 20% chance of browsers continually crashing if more than one browser is used. Windows devices using Kaspersky, Symantec, or Norton PSPs have a 20% chance of discovery. Each plug-in used in Windows devices increases the probability of detection by 5%. This capability can be configured and tested for this specific operation in between one and three weeks with a most likely completion at two weeks.

GROUP 1 COA order of preference:

1st Choice _____

2nd Choice _____

3rd Choice _____


A
Scenario 2 CoA A
112.0
10.1%
0.3%
88.1%
1.5%
Effectiveness
Cost (Hours)
B
Scenario 2 CoA B
112.0
31.6%
0.2%
67.2%
0.9%
Effectiveness
Cost (Hours)
C
Scenario 2 CoA C
112.0
0.3%
0.0%
97.9%
1.8%
Effectiveness
Cost (Hours)
GROUP 2 COA order of preference:
1st Choice _____
2nd Choice _____
3rd Choice _____
Scenario 2
Participant # _____

BACKGROUND

It is five years from now and authority to conduct surveillance and reconnaissance (SR), also known as computer network exploitation (CNE) and computer network attack (CNA) has been partially delegated to combatant commands (CCMD). SR/ CNE actions must be coordinated through USCYBERCOM, the Functional Combatant Command responsible for global cyber operations. USCYBERCOM supports Geographic Combatant Command efforts with de-confliction, initial intelligence, assigned access points for operations, and capabilities. Primacy for all operations resides at USCYBERCOM to support de-confliction efforts. Command and control of cyber operations resides at the CCMD once the operation is approved and commences. All CNA actions taken by CCMDs must have final approval from the national level authorities after review by the Joint Chiefs of Staff.

The Republic of Ameristan has long been an ally of the United States and has allowed forward basing of U.S. soldiers as part of theater security agreements and treaties. This is in conflict with Ameristan's neighbor, The Peoples' Democratic Republic of Koonistan, which is a technological peer to China, Russia, and Israel. Koonistan has long wanted U.S. forces to leave the region. Recently, tensions between Ameristan and Koonistan have risen and rhetoric from Koonistan has increased. This peaked last week with Koonistan shooting down an Ameristanian military helicopter resulting in no survivors. Koonistan claims that the helicopter violated the sovereign airspace and acted in self-defense.

To prevent attribution of cyber activities, the Koonistan government relies upon state-sponsored contracted companies to conduct cyber operations to meet government operational goals. These companies are given financial support, intelligence, and resources for their operations, along with government-provided protection. Recent national level intelligence indicates that a Koonistan company, آسا برق (تک)یحمله (English: Lightning Attack; (LI)), has infiltrated the CCMD networks and exfiltrated documents. The suspected documents included the recent updates to the Theater Security Cooperation Agreements with Ameristan that include personnel and equipment movement schedules and locations.

A portion of a document was exfiltrated from the LI network as proof, but proved inconclusive as the document was partially corrupted. USCYBERCOM has tasked the CCMD to conduct a SR/ CNE operation to confirm or deny the presence of sensitive CCMD document within the LI network, along with the amount of data taken. Confirmation is defined as the 400mb of non-public portion of the Theater Security Agreement that ranges in classification from SECRET to TOP SECRET/SI/NOFORN. This operation will be considered a success if all 400mb of the sensitive portion of the

document is identified, copied, and downloaded. CNA action is not authorized at this time. That will be a later effort pending the results of this operation.

Due to the sophistication of Koonistan, LI is considered to be the same level of sophistication. If attribution of CCMD activities within the LI network is discovered and attributed, Koonistan may order a retaliatory attack within the CCMD networks. Forensic analysis of the CCMD networks continues, resulting in two LI entry points within the CCMD network discovered with the fear that more exist.

COMMANDER'S INTENT

The commander has two goals: gathering intelligence and avoiding attribution. He places a relative value of 60% on avoiding attribution and 40% on intelligence collected due to the known activities by LI within the CCMD networks. The commander wishes to achieve an overall minimum effectiveness of .73. Because of these risks and requirements, this operation is considered to be a high risk operation. The commander's guidance is that this operation will commence within 9 days. This deadline is based off of the upcoming Theater Security Cooperation conference. If this deadline cannot be met, the staff must inform the commander as soon as possible and provide a timeline of events.

USCYBERCOM has attained the target IP address where the document was discovered and a single entry point into the LI network. The target IP address is one hop away from the entry point. The entry point is a HP desktop with a Windows 7 with Service Pack 1 along with a Kaspersky personal security product (PSP). Access to this computer is through a misconfigured port. This machine rarely browses the Internet, so care must be taken not to draw attention to this computer and subsequently, to this operation. The target machine is a Dell PowerEdge server running a Windows Server 2012 R2 operating system. This machine is also using Kaspersky Security for Windows Server as a PSP.

A domain user credential has been provided for this operation. Additionally, USCYBERCOM has coordinated for all other friendly actors to be out of the LI network for the CCMD operation. USCYBERCOM has provided three potential SR/ CNE capability courses of action (COA) for consideration and choice by the COCOM Command and Staff. **As the CCMD staff, you must order the COAs within each of the two groups in precedence of most preferred to least preferred for consideration by the commander for a decision.**

GROUP 1 COURSES OF ACTION

COA A: SURREPTITIOUSCAMEL is a capability that scans and lists the directory of a device, creates executive summaries of chosen documents, and then will exfiltrate

selected documents. This capability is a former NSA capability that has been replaced. This capability requires on-net operators to monitor and direct the capability. SURREPTITIOUSCAMEL has the ability to customize the rate of data exfiltration in the attempt to avoid detection in network traffic. On the lowest data transmission rate, SURREPTITIOUSCAMEL will at 6KB/ sec. Although used in real operations previously, this capability has not been used in over a year. Virtualized testing indicates a 10% chance of Kaspersky detecting the capability. It is estimated that for every KB/sec over 5KB/ sec in bandwidth leaving the access point computer, the potential for network administrator detecting the traffic increases by 5%. This capability can be configured and tested for this specific operation in between one and three weeks with a most likely completion at two weeks.

COA B: ANGRYPIRATE is an automated capability that inventories the directories of a device and sends selected files to a predetermined location. This capability requires several days to complete these tasks. Once activated, ANGRYPIRATE begins an inventory of all directories it can find. Once this is complete, it sends a small encrypted file using extremely low bandwidth to the predetermined sensor. The sensor will then notify the operator that information is waiting. Once the information is analyzed, an on-net operator tasks ANGRYPIRATE with a listing of files to encrypt and exfiltrate. It is estimated that a 1MB file will take an hour and a half to transmit. Additionally, ANGRYPIRATE is customizable to transmit only during predefined windows of time to prevent noticeable network traffic during time of network inactivity. This capability has not been used in real operations but virtualized testing indicated that Kaspersky will not detect ANGRYPIRATE. However, there is a 20% chance of a network administrator noticing traffic leaving a seldom used computer and identifying both the traffic leaving the network and the sensor used for communication with ANGRYPIRATE. This capability can be configured and tested for this specific operation in between one and two weeks with a most likely completion at two weeks.

COA C: SKITTLEPARTY is a capability that exfiltrates all the contents of a hard drive. This capability has options for the exfiltration rate and windows of time to work that must be predefined. Once SKITTLEPARTY begins, it cannot stop to reconfigure without starting all over. On the lowest data transmission rate, SKITTLEPARTY will at 5KB/ sec. It is estimated that for every KB/sec over 5KB/ sec in bandwidth leaving the access point computer, the potential for detection increases by 5%. All files are encrypted and sent to a preconfigured location. The awaiting sensor must receive all the files on the hard drive before access to the files is possible. This capability has not been used in real operations however, in virtualized testing, Kaspersky detected SKITTLEPARTY only 17% of the time. However, with the amount of data that would be transmitted from this capability, it is estimated that there is a 20% chance that the system administrator will

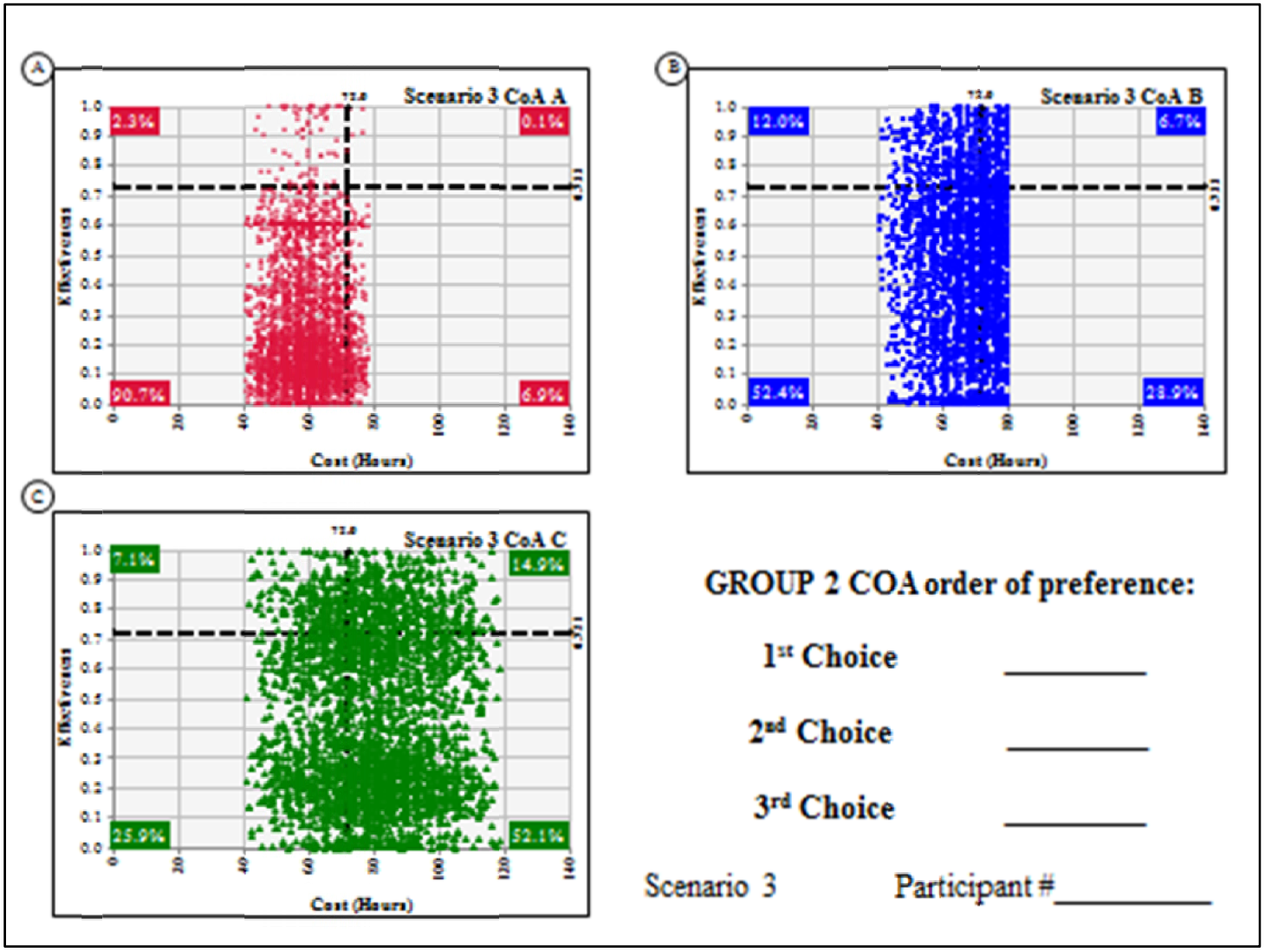
detect the traffic leaving the network and discover the sensor used with SKITTLEPARTY. This capability can be configured and tested for this specific operation in between one and two weeks with a most likely completion at one and a half weeks.

GROUP 1 COA order of preference:

1st Choice _____

2nd Choice _____

3rd Choice _____


A
Scenario 3 CoA A
2.3%
0.1%
90.7%
6.9%
Effectiveness
Cost (Hours)
B
Scenario 3 CoA B
12.0%
6.7%
52.4%
28.9%
Effectiveness
Cost (Hours)
C
Scenario 3 CoA C
7.1%
14.9%
25.9%
52.1%
Effectiveness
Cost (Hours)
GROUP 2 COA order of preference:
1st Choice _____
2nd Choice _____
3rd Choice _____
Scenario 3
Participant #_____

BACKGROUND

It is five years from now and authority to conduct surveillance and reconnaissance (SR), also known as computer network exploitation (CNE) and computer network attack (CNA) has been partially delegated to combatant commands (CCMD). SR/ CNE actions must be coordinated through USCYBERCOM, the Functional Combatant Command responsible for global cyber operations. USCYBERCOM supports Geographic Combatant Command efforts with de-confliction, initial intelligence, assigned access points for operations, and capabilities. Primacy for all operations resides at USCYBERCOM to support de-confliction efforts. Command and control of cyber operations resides at the CCMD once the operation is approved and commences. All CNA actions taken by CCMDs must have final approval from the national level authorities after review by the Joint Chiefs of Staff.

The Islamic State (IS) has continued to use the Internet to recruit, spread propaganda, and command and control decentralized operations over a wide swath of land in the Middle East. This online activity is escalating and after a video of a captured U.S. forces member being killed for propaganda purposes was released. The Central Intelligence Agency (CIA) has reported that the new edition of the jihadist magazine, Inspire, will be published online in two weeks. In this edition will be a call to arms for jihadists after the propaganda victory of the video of the American being killed. Additionally, this edition will have a new technique for bomb making.

COMMANDER'S INTENT

The CCMD, in coordination with national level intelligence has decided that a CNA operation against Inspire magazine is warranted. The JCS and national level authorities have approved of the action. USCYBERCOM has tasked the CCMD to conduct CNA upon the magazine file, which is an Adobe PDF. Specifically, the task for this is to prevent viewing of the file with two purposes; preventing dissemination of the bomb making information and to facilitate CIA identification of readers of the magazine. The target machine is an Apache web server using FreeBSD 10.3 and Panda Security antivirus protection.

One consideration is that the CIA monitors and participates within the web forum as a way of identifying persons of interest and high payoff targets (HPTs). The commander has been ordered to not bring attribution the U.S. or compromise the CIA efforts. As such, the commander has expressed that he places the values of the outcomes of this operation at 40% (Destruction; video denial), 30% (avoiding attribution), and 30% (avoiding compromise). The commander wishes to achieve an overall minimum effectiveness of .66. Because of these risks, this operation is considered to be a high risk operation. The commander's guidance is that this operation will commence within 14 days. This deadline is based off of the upcoming Theater Security Cooperation

conference. If this deadline cannot be met, the staff must inform the commander as soon as possible and provide a timeline of events.
USCYBERCOM has provided three potential CNA capability courses of action (COA) for consideration and choice by the COCOM Command and Staff. **As the CCMD staff, you must order the COAs within each of the two groups in precedence of most preferred to least preferred for consideration by the commander for a decision.**

GROUP 1 COURSES OF ACTION

COA A: BAMBOOSHIRT is a capability that is used to corrupt files and render them unreadable. This capability can accept plug-ins for disseminating implants and recording IP addresses of people attempting to access the file, providing a TCP reset to people attempting to access the file, redirecting the user to another predefined location (see concerns in COA 2), or disseminating malware to people attempting to access the file, such limited-scope as CNA capabilities. Only one implant may be used at a time or BAMBOOSHIRT becomes unstable and will cause the device to act erratically. This capability has not been used in real operations, but in virtualized testing it was not detected by personal security products (PSPs). However, if an implant or CNA capability is deployed from BAMBOOSHIRT, there is a 15% chance of those capabilities being detected. This capability can be configured and tested for this specific operation in between two and three weeks with a most likely completion at three weeks.

COA B: DEPRESSEDCLOWN is a capability that would record the IP address and redirect users attempting to access a predetermined file to another predetermined location. When the user clicks the link to view or download the file, the user is automatically redirected to another location. That second location may or may not have a file for the user to see or download. When users are redirected, the computer being used is implanted. This implant then beacons back to a predefined sensor to wait for tasking. DEPRESSEDCLOWN has been used limitedly in real operations without being detected. This capability has the ability to filter what IP address blocks are redirected and implanted in the effort to prevent collection of information and the implant of computers belonging to U.S. persons. However, the concern is the collection of information and implanting of computers of U.S. persons and violating the Foreign Intelligence Surveillance Act. It is estimated that a 20% chance exists that information collection and implant of a computer belonging to a U.S. person will occur, based on analysis of the web forum. It is unknown if these are real U.S. persons or if they are foreign nationals using U.S. –based proxies. This capability can be configured and tested for this specific operation in between one and three weeks with a most likely completion at two weeks.

COA C: OBESECATEPILLAR is a capability that allows the replacement of adobe PDF files while retaining the hash of the original. OBESECATEPILLAR further uses

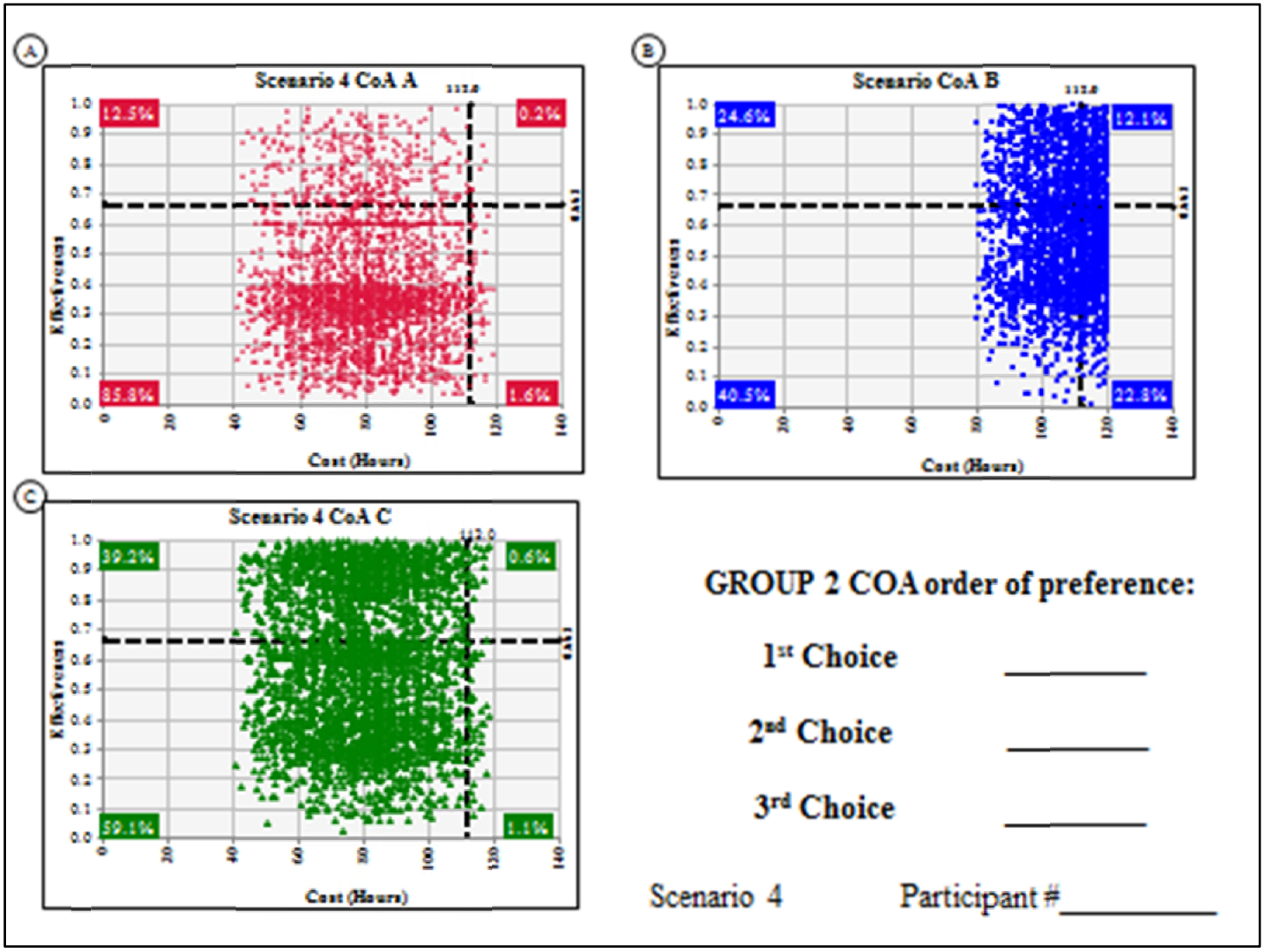
steganography to imbed an executable for an implant into the file. This implant will then beacon a sensor to await instructions. This capability has been used limitedly in real operations with success. Although OBESECATEPILLAR is not detected by Panda security, the risk also is with the end user device. There is a 15% chance of detection from Kaspersky, a 20% chance of protection by Symantec. It is unknown how OBESECATEPILLAR will perform with Qihoo 360. Estimates range from 40% likelihood of detection to 80% likelihood. The median consensus is a 45% chance of detection. The concern is that if the file is detected by a PSP forensic examination will show that the file has been changed and the location of the sensor the implant beacons to. This would cause the terrorists to change tactics and move the web forum to another location, potentially causing the CIA to lose this source of intelligence. This capability can be configured and tested for this specific operation in between one and three weeks with a most likely completion at two weeks.

GROUP 1 COA order of preference:

1st Choice _____

2nd Choice _____

3rd Choice _____


A
Scenario 4 CoA A
12.5%
0.2%
85.8%
1.6%
Cost (Hours)
B
Scenario CoA B
24.6%
12.1%
40.5%
22.8%
Cost (Hours)
C
Scenario 4 CoA C
39.2%
0.6%
59.1%
1.1%
Cost (Hours)
GROUP 2 COA order of preference:
1st Choice _____
2nd Choice _____
3rd Choice _____
Scenario 4
Participant #_____

BACKGROUND

It is five years from now and authority to conduct surveillance and reconnaissance (SR), also known as computer network exploitation (CNE) and computer network attack (CNA) has been partially delegated to combatant commands (CCMD). SR/ CNE actions must be coordinated through USCYBERCOM, the Functional Combatant Command responsible for global cyber operations. USCYBERCOM supports Geographic Combatant Command efforts with de-confliction, initial intelligence, assigned access points for operations, and capabilities. Primacy for all operations resides at USCYBERCOM to support de-confliction efforts. Command and control of cyber operations resides at the CCMD once the operation is approved and commences. All CNA actions taken by CCMDs must have final approval from the national level authorities after review by the Joint Chiefs of Staff.

The Republic of Aragon has long been an ally of the United States and has allowed forward basing of U.S. soldiers as part of theater security agreements and treaties. This is in conflict with Aragon's neighbor, The Peoples' Democratic Republic of Krasnovia, which is a technological peer to Iran, South Korea, and India. Krasnovia has long wanted U.S. forces to leave the region. Recently, tensions between Aragon and Krasnovia have risen and rhetoric from Krasnovia has increased. This peaked last week with Krasnovia shooting down an Klondikian military helicopter resulting in no survivors. Krasnovia claims that the helicopter violated the sovereign airspace and acted in self-defense.

To prevent attribution of cyber activities, the Krasnovia government relies upon state-sponsored contracted companies to conduct cyber operations to meet government operational goals. These companies are given financial support, intelligence, and resources for their operations, along with government-provided protection. Recent national level intelligence indicates that a Krasnovia company, خدا است ممکن (English: Allah's Might; (AM)), has targeted U.S. and Aragon networks with malware. The application of malware differs from site to site. Both U.S. and Aragon networks have suffered from both intelligence gathering and denial of service attacks. None of the attacks within the U.S. have been within networks deemed to be critical infrastructure or key resources. However, the attacks have been highly publicized but not publicly attributed due to U.S. equities for intelligence gathering.

COMMANDER'S INTENT

AM infrastructure has been identified and national level authorities have ordered that a CNA operation be undertaken to stop the attacks. As AM is physically located within this CCMD's area of operations, USCYBERCOM has tasked this CCMD with this operation. USCYBERCOM has dictated that the attack will be demonstrative to both AM and Krasnovia that the U.S. knows they are responsible. However, attribution of the U.S.

cyber operations infrastructure must be protected. Additionally, to prevent collateral damage, the operational effects cannot expand beyond the AM networks. The commander has expressed that he values the outcome of this operation as 50% (Attaining Destruction), 30% (Avoiding Detection), and 20% (Avoiding Attribution). The commander wishes to achieve an overall minimum effectiveness of .59. Because of these risks, this operation is considered to be a low to moderate risk operation. The commander's guidance is that this operation will commence within 13 days. This deadline is based off of guidance from national command authority. If this deadline cannot be met, the staff must inform the commander as soon as possible and provide a timeline of events.

The targeted machines are Lenovo laptops using Window 7, 64 bit with the bitlocker feature turned on. This network is also using a heuristics-based Qihoo 360 personal security product (PSP) with a cloud-based analytical engine. The network consists of Hauwei routers and switches, Lenovo laptops all running the same operating system and PSP, ZTE firewalls, and Dell Power Edge file servers implementing RAID 1. The total usable space of the servers is four terabytes. NSA estimates, from previous operations, that five gigabytes of malware projects are housed within the servers. Success of this operation is two-fold: First, the malware projects must be downloaded and analyzed for future signatures to protect DOD networks. This task will be undertaken by NSA. The CCMD is responsible for the second task, destroying all information residing on the file servers by corrupting the information or by rendering the information inaccessible. In whatever method is used, the information must be unrecoverable.

USCYBERCOM has identified CIA and NSA as other friendly actors within the network. NSA has primacy within the network, however, has agreed to the COCOM actions. NSA has provided a known access point and they, along with the CIA, have withdrawn all their capabilities from the AM network. Additionally, NSA has provided a user credential. This credential is believed to have read/ write access to the file servers.
USCYBERCOM has provided three potential CNA capability courses of action (COA) for consideration and choice by the COCOM Command and Staff. **As the CCMD staff, you must order the COAs within each of the two groups in precedence of most preferred to least preferred for consideration by the commander for a decision.**

GROUP 1 COURSES OF ACTION

COA A: MONKEYSTOMP is a capability that removes all the file allocation pointers, overwrites the hard drives, and then encrypts the hard drive before deleting the key and restarting the device. This capability has the projected ability to overwrite and encrypt drives at a rate of 1GB every five minutes based on the file server specifications. MONKEYSTOMP has not been used in real operations but virtualized testing indicates

host-based PSPs do not detect this capability. However, it is unknown if a cloud-based PSP will detect it due to the inability to create a virtualized environment that replicates the real PSP ability. Due to the past performance of Qihoo 360, is it estimated that a 40% chance of discovery and quarantine will occur prior to activation. This capability can be configured and tested for this specific operation in between one and two weeks with a most likely completion at two weeks.

COA B: HYPEROPOSSUM is a capability that causes device hard drives to accelerate to maximum speed and then the read/ write heads of the server hard drives to drag the plates, rendering them unreadable. This capability has been used limitedly in the past for real operations but on smaller applications such as individual laptops and desktops. This incarnation of the capability performed as expected in virtualized testing but required an on-net operator to activate the capability on each server. Once activated, HYPEROPOSSUM cannot be stopped; however, the risk elevates for detection and attribution for a manual activation of the capability. It is estimated that a 20% chance of detection exists and a 40% chance of attribution exists if detected. This capability can be configured and tested for this specific operation in between one and three weeks with a most likely completion at two weeks.

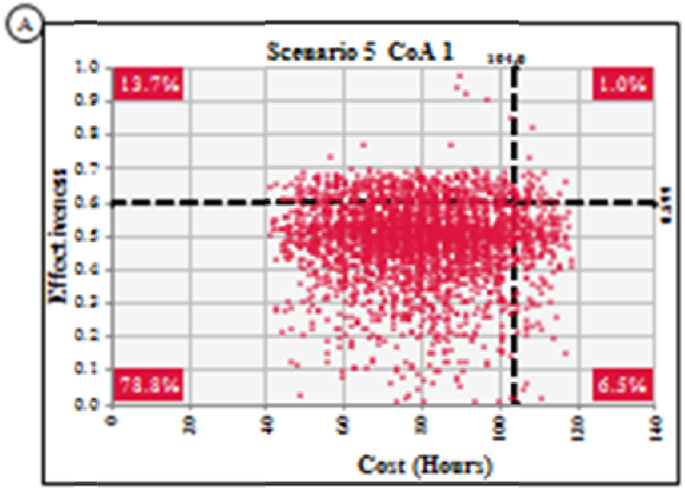
COA C: ANGRYDRAGON is a capability that uses the properties of RAID to propagate and initiate. This capability monitors the RAID controllers to ensure it reaches all RAID participants. When the RAID update is complete, ANGRYDRAGON begins to overwrite all information on the drives. This capability has not been used in real operations. Virtualized testing indicates a 20% chance of propagation outside of the targeted servers if users have mapped a file server as a network drive on a laptop or desktop. If propagation outside of the server occurs, each device ANGRYDRAGON moves to is a possible vector for further propagation if that device is has other mapped network locations, peer to peer connections, USB connected devices or storage, or if the device is dual-homed on the networks. This capability can be configured and tested for this specific operation in between two and three weeks with a most likely completion at three weeks.

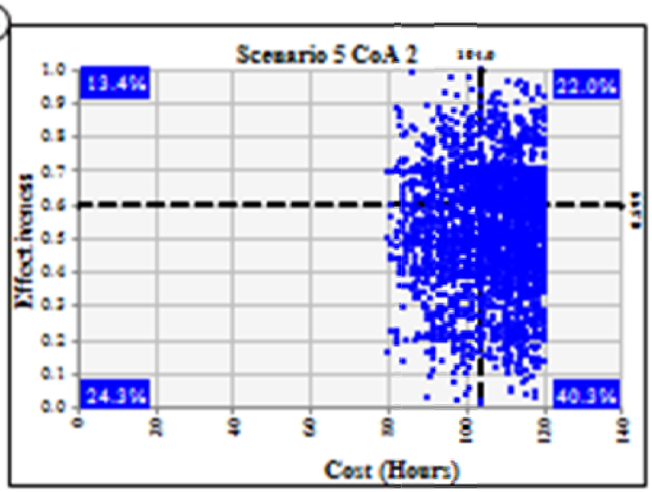
GROUP 1 COA order of preference:

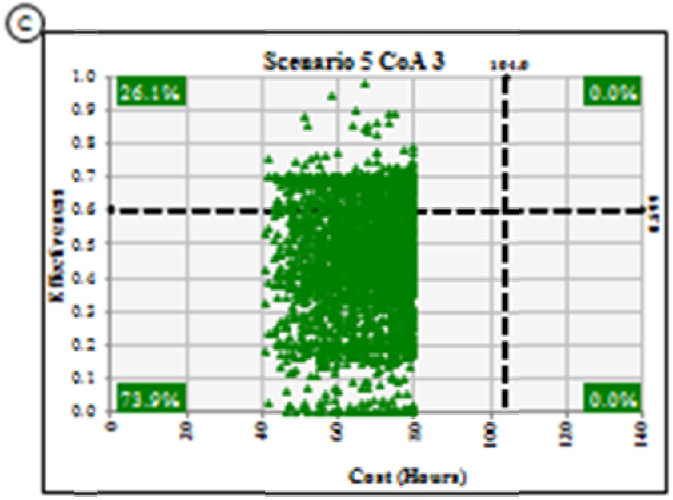
1st Choice _____

2nd Choice _____

3rd Choice _____







GROUP 2 COA order of preference:

1st Choice _____

2nd Choice _____

3rd Choice _____

Scenario 5 Participant #_____

APPENDIX I. IRB APPROVAL

Naval Postgraduate School
Human Research Protection Program

From: President, Naval Postgraduate School (NPS)
To: Dr. Dan Boger, Graduate School of Operation and Information Sciences (GSOIS)
Dr. Kent Wall, Defense Resources Management Institute, (DRMI)
MAJ Michael Klipstein, USA
Via: Chairman, Institutional Review Board (IRB)

Subj: QUANTIFYING RISK FOR OFFENSIVE CYBER OPERATIONS

Encl: (1) Approved IRB Initial Review Protocol

1. The NPS IRB is pleased to inform you that the NPS President has approved your initial review protocol (NPS IRB# NPS.2016.0031-IR-EP7-A). The approved IRB Protocol is found in enclosure (1). Completion of the CITI Research Ethics Training has been confirmed.

2. This approval expires on 16 February 2017. If additional time is required to complete the research, a continuing review report must be approved by the IRB and NPS President prior to the expiration of approval. At expiration all research (subject recruitment, data collection, analysis of data containing PII) must cease.

3. You are required to obtain consent according to the procedure provided in the approved protocol.

4. You are required to report to the IRB any unanticipated problems or serious adverse events to the NPS IRB within 24 hours of the occurrence.

5. Any proposed changes in IRB approved research must be reviewed and approved by the NPS IRB and NPS President prior to implementation except where necessary to eliminate apparent immediate hazards to research participants and subjects.

6. As the Principal Investigator (PI) it is your responsibility to ensure that the research and the actions of all project personnel involved in conducting this study will conform with the IRB approved protocol and IRB requirements/policies

Subj: QUANTIFYING RISK FOR OFFENSIVE CYBER OPERATIONS

7. At completion of the research, no later than expiration of approval, the PI will close the protocol by submitting an End of Experiment Report.

Lawrence G. Shattuck, PhD
Chair
Institutional Review Board

Ronald A. Route
Vice Admiral, U.S. Navy (Ret.)
President, Naval Postgraduate School

Date: 9 March 2016

SUPPLEMENTAL

REPLICATION DATA

Replication data for this research may be found on NPS Calhoun. This data includes the SME packets along with the participant packets for this research. Replication data may be accessed at: http://calhoun.nps.edu/handle/10945/52363.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Arceneau, K. (2012). Cognitive biases and the strength of political arguments. *American Journal of Political Science, 56*(2), 271–285.

Asch, S. E. (1955). Opinions and social pressure. *Scientific American*, *193*(5), 2–6.

Asch, S. E. (1956). Studies of independence and conformity: I. A minority of one against a unanimous majority. *Psychological Monographs: General and Applied*, *70*(9), 1–70. http://doi.org/http://dx.doi.org.libproxy.nps.edu/10.1037/h0093718

Axelrod, R., & Iliev, R. (2014). Timing of cyber conflict. *Proceedings of the National Academy of Sciences of the United States of America*, *111*(4), 1298–1303.

Bell, D. E. (1982). Regret in decision making under uncertainty. *Operations Research*, *30*(5), 961. http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/219159485?accountid=12702

Bennett, R. (2000). Risky business the science of decision making grapples with sex, race, and power. *Science News*, *158*(12), 190–191. http://www.jstor.org/stable/3981298

Bernoulli, D. (1954). Exposition of a new theory on the measurement of risk. *Econometrica*, *22*(1), 23–36. http://doi.org/10.2307/1909829

Bieleny, R. (2012). *Breaking the status quo: Information and the future force*. Carlisle Barracks: Retrieved from http://handle.dtic.mil/100.2/ADA560883

Blais, A.-R., & Weber, E. U. (2006). A domain-specific risk-taking (DOSPERT) scale for adult populations. *Judgment and Decision Making*, *1*(1), 33–47. Retrieved from http://journal.sjdm.org/06005/jdm06005.htm

Bremmer, I. (2015). These 5 facts explain the threat of Ccyber warfare | TIME. Retrieved January 5, 2016, from http://time.com/3928086/these-5-facts-explain-the-threat-of-cyber-warfare/

Broder, J. F., & Tucker, E. (2012). *Risk analysis and the security survey* (4th ed.). Oxford: Butterworth-Heinemann.

Brookins, P., & Ryvkin, D. (2014). An experimental study of bidding in contests of incomplete information. *Experimental Economics*, *17*(2), 245–261. http://doi.org/http://dx.doi.org/10.1007/s10683-013-9365-9

Bruyneel, S. D., Dewitte, S., Franses, P. H., & Dekimpe, M. G. (2009). I felt low and my purse feels light: Depleting mood regulation attempts affect risk decision making. *Journal of Behavioral Decision Making*, *170* (October 2008), 153–170. http://doi.org/10.1002/bdm

Buckshaw, D. (2005). Mission oriented risk and design analysis of critical information systems. *Military Operations Research*, *10*(2), 19–38.

Budescu, D. V., Broomell, S., & Por, H. Improving communication of uncertainty in the reports of the intergovernmental panel on climate change. *Psychological Science*, *20*(3), 299–308.

Buelow, M. T., & Suhr, J. A. (2013). Personality characteristics and state mood influence individual deck selections on the Iowa Gambling Task. *Personality and Individual Differences*, *54*(5), 593–597. http://doi.org/10.1016/j.paid.2012.11.019

Burtscher, M. J., & Meyer, B. (2014). Promoting good decisions: How regulatory focus affects group information processing and decision-making. *Group Processes & Intergroup Relations*, *17*, 663–681. http://doi.org/10.1177/1368430214522138

Clore, G., & Huntsinger, J. (2007). How emotions inform judgment and regulate thought. *Trends in Cognitive Sciences*, *11*(9), 393–399. http://doi.org/ 10.1016(J.tics.2007.08.005

Colwell, L. H. (2005). Cognitive hueristics in the context of legal decsion making. *American Journal of Forensic Psychology*, *23*(2), 17–41.

Cooper, A. C., Woo, C. Y., & Dunkelberg, W. C. (1988). Entrepreneurs' perceived chances for success. *Journal of Business Venturing*, *3*(2), 97–108.

Davis, P. K., Kulick, J., & Egner, M. (2005). *Implications of modern decision science for military decision-support systems*. Arlington, VA: RAND.

De Dreu, C. K. W., Nijstad, B. A., & van Knippenberg, D. (2008). Motivated information processing in group judgment and decision making. *Personality and Social Psychology Review : An Official Journal of the Society for Personality and Social Psychology, Inc*, *12*(1), 22–49. http://doi.org/10.1177/1088868307304092

de Langhe, B., & Puntoni, S. (2015). Bang for the buck: Gain-loss ratio as a driver of judgement and choice. *Management Science*, *61*(5), 1137–1163.

Denning, D. (2015). Rethinking the cyber domain and deterrence. *Joint Forces Quarterly*, *77*(8), 8–15.

Denning, P., & Denning, D. (2010). Discussing cyber attack. *Communications of the ACM*, *53*(9), 29–31.

Department of Defense. (2011a). *Department of Defense Strategy for Operating in Cybersapce*. Washington, DC.

Department of Defense. (2013). JP 3-21(R) *Cyberspace operations*. Washington, DC: Author.

Department of Defense. (2015). *Department of Defense risk, issue, and opportunity Management Guide for Defense Acquisition*. Washington, DC: Department of Defense. Retrieved from http://bbp.dau.mil/docs/RIO-Guide-Jun2015.pdf

Department of Defense. (2016). *JP 1–02: Dictionary of military and associated terms*. (Department of Defense, Ed.). Washington, DC: Department of Defense. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Department of Homeland Security. (2016). *National Cyber Incident Response Plan*. Washington, DC.

Department of the Army. (2012). *ADP 6–0 (Mission Command)*. Washington, DC: Army Publishing Directorate. Retrieved from https://armypubs.us.army.mil/doctrine/index.html

Department of the Army. (2013). *AR 385–10 The Army Safety Program*. Washington, DC: Army Publishing Directorate.

Department of the Navy. (2014). *MCIP 3–40 02- Marine Corps cyberspace operations*. Quantico, VA: Department of the Navy.

Dowd, K. W., Petrocelli, J. V, & Wood, M. T. (2014). Integrating information from multiple sources: A metacognitive account of self-generated and externally provided anchors. *Thinking & Reasoning*, *20*(3), 315–332. http://doi.org/http://dx.doi.org/10.1080/13546783.2013.811442

Dreyer, P., & Davis, P. K. (2005). *A portfolio-analysis tool for missile defense (PAT–MD)*. (DASW01-01-C-0004). Santa Monica, RAND National Defense Research Institute. Retrieved from http://www.rand.org/pubs/technical_reports/TR262.html

Driskell, J. E., & Salas, E. (1991). Group decision making under stress. *Journal of Applied Psychology*, *76*(3), 473–478.

Duggan, J., & Martinelli, C. (2010). A spatial theory of media slant and voter choice. Retrieved December 31, 2015, from http://www.restud.com/wp-content/uploads/2011/01/MS12741manuscript.pdf

Duggan, P. (2015). *Strategic development of special warfare in cyberspace*. Army War College. Retrieved from http://ndupress.ndu.edu/Media/News/News-Article-View/Article/621123/strategic-development-of-special-warfare-in-cyberspace/

Dyer, J. S., & Sarin, R. (1979). Measurable multiattribute value functions on JSTOR. *Operations Research*, *27*(4), 810–822. Retrieved from http://www.jstor.org.libproxy.nps.edu/stable/170296?seq=1#page_scan_tab_contents

Eisenhardt, K. M. (1989). Making fast strategic decisions in high-velocity environments. *Academy of Management Journal*, *32*(3), 543–576.

Ellsberg, D. (1961). Risk, ambiguity, and the Savage axioms. *Quarterly Journal of Economics*, *75*, 643–669. Retrieved from http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/864366624?accountid=12702

Ericsson, K. A., Krampe, R., & Tesch-Romer, C. (1993). The role of deliberate practice in the acquisition of expert performance. *Psychological Review*, *100*(3), 363–404. http://doi.org/0033-295X/93

Ericsson, K. A., Prietula, M., & Cokely, E. (2007). The making of an expert. *Harvard Business Review*, *July-August*, 1–7.

Ernst, D. (2014, November 6). Russian hackers' "Trojan Horse" malware inside U.S. critical infrastructure since 2011. *The Washington Times*. Retrieved from http://www.washingtontimes.com/news/2014/nov/6/russian-hackers-trojan-horse-malware-inside-us-cri/

Ernst, M. D. (2004). Permutation methods: A basis for exact inference. *Statistical Science*, *19*(4), 676–685.

Falliere, N., O Murchu, L, & Chien, E. (2011). *W32.Stuxnet Dossier*. Cupertino, CA. Retrieved from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Figner, B., Mackinlay, R. J., Wilkening, F., & Weber, E. U. (2009). Affective and deliberative processes in risky choice: Age differences in risk taking in the columbia card task. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, *35*(3), 709–730. http://doi.org/http://dx.doi.org/10.1037/a0014983

Financial Times. (2010). Big Oil, Bigger Oil. Retrieved from http://www.ft.com/cms/s/c5b32636-116f-11df-9195-00144feab49a,_i_email=y,Authorised=false.html?_i_location=http://www.ft.com/cms/s/3/c5b32636-116f-11df-9195-00144feab49a,_i_email=y.html&_i_referer=http://texasenterprise.org/article/whats-value-saudi-aramco#axzz3UzCDvrQp

Finucane, M. L., Alhakami, A., Slovic, P., & Johnson, S. M. (2000). The affect heuristic in judgements of risks and benefits. *Journal of Behavioral Decision Making*, *13*, 1–17.

FitzGerald, B., & Wright, P. (2014). Decentralizing cyber command and control. *Disruptive Defense Papers*, (April). Retrieved from https://www.cnas.org/publications/reports/digital-theaters-decentralizing-cyber-command-and-control

Flemming, P., & Stohl, M. (2000). Myths and realities of cyber terrorism. *Countering Terrorism Through International Cooperation,* Alex P. Schmid (ed.), ISPAC (International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Program), Vienna, 2001,pp: 70-105.

Foushee, H. C. (1982). The role of communications, socio-psychological, and personality factors in the maintenance of crew coordination. *Aviation, Space, and Environmental Medicine*, *53*(11), 1062–6. Retrieved from http://www.researchgate.net/publication/16049243_The_role_of_communications_socio-psychological_and_personality_factors_in_the_maintenance_of_crew_coordination

Fox, C. R., & Tversky, A. (1995). Ambiguity aversion and comparative ignorance. *Quarterly Journal of Economics*, *110*(3), 585–603.

Garrick, B. J. (2008). *Quantifying and controlling catastrophic risks*. Burlington, VT: Academic Press.

Garvin, D. A., & Roberto, M. A. (2001). What you don't know about making decisions. *Harvard Business Review*, *September*, 22–32.

Gertz, B. (2014). U.S. Electrical, Financial Networks Mapped for Future Cyber Attacks. Retrieved from http://freebeacon.com/national-security/u-s-electrical-financial-networks-mapped-for-future-cyber-attacks/

Gilbert, D. (2014). U.S. Charges Chinese Cyber-Spies with Stealing Nuclear Power Plant Plans. Retrieved from http://www.ibtimes.co.uk/us-charges-chinese-cyber-spies-stealing-nuclear-power-plant-plans-1449175

Gilovich, T. (1991). *How we know what isn't so*. New York, NY: The Free Press.

Girodo, M. (2007). Personality and cognitive processes in life and death decision making: An exploration into the source of judgment errors by police special squads. *International Journal of Psychology*, *42*(6), 418–426. http://doi.org/http://dx.doi.org/10.1080/00207590701436728

Grant, T., Burke, I., & van Heerden, R. (2012). Comparing models of offensive cyber operations. In *International Conference on Information Warfare and Security*. Retrieved from http://search.proquest.com.libproxy.nps.edu/docview/1545631512/fulltextPDF/B9C35D1DBCD745ABPQ/1?accountid=12702

Grifffin, R. J., Neuwirth, K., Giese, J., & Dunwoody, S. (2002). Linking the Heuristic-Systematic Model and Depth of Processing. *Communication Research*, 29(6), 705-732, Retrieved from http://doi.org/10.1177/009365002237833

Gutnik, L. A., Hakimzada, A. F., Yoskowitz, N. A., & Patel, V. L. (2006). The role of emotion in decision-making: A cognitive neuroeconomic approach towards understanding sexual risk behavior. *Journal of Biomedical Informatics*, *39*, 720–736. Retrieved from http://ac.els-cdn.com/S1532046406000451/1-s2.0-S1532046406000451-main.pdf?_tid=ea873288-b644-11e5-b8e6-00000aab0f6b&acdnat=1452284461_7a53aeda165801feed1627e80eeaa236

Heilbronner, S. R., Hayden, B. Y., & Platt, M. L. (2010). Neuroeconomics of risk-sensitive decision making. In G. Madden, PhD & W. Bickel, PhD (Eds.), *Impulsivity: The behavioral and neurological science of discounting* (pp. 159–187).

Helmreich, R. L. (1979). Social psychology on the flight deck. In *Proceedings of a NASA/ Industry Workshop* (pp. 17–30). San Francisco, CA. Retrieved from http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19800013796.pdf

Hubbard, D. W. (2009). Worse than useless: The most popular risk assessment method and why it doesn't work. In *The Failure of Risk Management: Why It's Broken and How to Fix It* (pp. 117–143). Hoboken, NJ: John Wiley & Sons.

Humphrey, S. J. (2004). Feedback-conditional regret theory and testing regret-aversion in risky choice. *Journal of Economic Psychology*, *25*(6), 839–857. http://doi.org/http://dx.doi.org/10.1016/j.joep.2003.09.004

International Organization for Standardization. (2009). ISO 73:2009 (Risk Management-Vocabulary). Retrieved November 21, 2014, from https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

Isen, A. M., & Geva, N. (1987). The influence of positive affect on acceptable level of risk: The person with a large canoe has a large worry. *Organizational Behavior and Human Decision Processes*, *39*(2), 145. Retrieved from http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/223204585?accountid=12702

ISO. (1989). *Informaiton Processing Systems—Open Systems Interconnection—Basic Refernce Model Part 4: Management Framework*. Geneva, Switzerland. Retrieved from http://standards.iso.org/ittf/PubliclyAvailableStandards/s014258_ISO_IEC_7498-4_1989(E).zip

Jarmon, J. (2014). *The new era in U.S. national security: an introduction to emerging threats and challenges*. Lanham, MD: Roman & Littlefield. Retrieved from http://books.google.com/books?hl=en&lr=&id=YfQ3AwAAQBAJ&oi=fnd&pg=PR7&dq=The+New+Era+in+US+National+Security:+An+Introduction+to+Emerging+Threats+and+Challenges&ots=Lkni_Q5Ars&sig=EnhKr34554onzlH_2j6PJ-dKr9E

Kahneman, D. (2003). A Perspective on judgement and choice. *American Psychologist*, *58*(9), 697–720. http://doi.org/10.1037/0003-066X.58.9.697

Kahneman, D. (2013). *Thinking fast and slow* (2nd ed.). Farrar, Straus and Giroux.

Kahneman, D., & Lovallo, D. (1993). Timid choices and bold forecasts—a cognitive perspective on risk taking. *Management Science*, *39*(1), 17–31. Retrieved from http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/38481183?accountid=12702

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, *47*(2), 263–291. Retrieved from http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/56137572?accountid=12702

Kahneman, D., & Tversky, A. (1984). Choices, values, and frames. *American Psychologist*, *39*(4), 341–350.

Kane, J., & Webster, G. D. (2013). Heuristics and biases that help and hinder scientists: Toward a psychology of scientific judgment and decision making. In G. P. Feist & M. P. Gorman (Eds.), *Handbook of the Psychology of Science* (1st ed., pp. 437–459). New York, NY: Springer.

Kania, E. (2015). The latest indication of the PLA's network warfare strategy. Retrieved September 9, 2016, from http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=44925&tx_ttnews%5BbackPid%5D=789&no_cache=1#.V9MKMpgrLmw

Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis*, *1*(1), 11–27. Retrieved from http://doi.wiley.com/10.1111/j.1539-6924.1981.tb01350.x\nfile:///Users/johnlee/Documents/Dropbox/Papers2/Files/

Keeney, R. l. (1992). *Value focused thinking*. Cambridge: Harvard University Press.

Keeney, R. l. (1996). Value-focused thinking Identifying decision opportunities and creating alternatives. *European Joumal of Operational Research*, *92*, 537–549.

Keeney, R. L. (Duke U., & Greogory, R. S. (Decision R. (2005). Selecting attributes to measure the achievement of objectives. *Operations Research*, *53*(1), 1–11.

Keeney, R. L., & Raiffa, H. (1976). *Decisions with multiple objectives: Preferences and value tradeoffs* (1st ed.). New York, NY: Wiley.

Keeney, R. L., Raiffa, H., & Rajala, D. W. (1976). *Decisions with Multiple Objectives: Preferences and Value Trade-Offs*. *IEEE Transactions on Systems, Man, and Cybernetics* (1st ed., Vol. 9). Cambridge: Cambridge University Press. http://doi.org/10.1109/TSMC.1979.4310245

Keren, G. (1987). Facing uncertainty in the game of bridge: A calibration study. *Organizational Behavior and Human Decision Processes*, *39*(1), 98–114.

Kirkwood, C. (1997). *Strategic decision making*. (C. Hinrichs, Ed.). Belmont, CA: Wadsworth Publishing Company.

Kleespies, P. M. (2014). Decision making under stress: Theoretical and empirical bases. In *Decision making in behavioral emergencies: Acquiring skill in evaluating and managing high-risk patients.* (pp. 31–46). Washington, DC: American Psychological Association. Retrieved from http://dx.doi.org/10.1037/14337-003

Koch, A., Matthias, E., & Pollatos, O. (2014). Increased attentional bias towards food pictures in overweight and obese children. *Journal of Child & Adolescent Behavior*, *2*(2). Retrieved from http://www.esciencecentral.org/journals/increased-attentional-bias-towards-food-pictures-in-overweight-and-obese-children-2375-4494.1000130.pdf

Labs, K. (2015). *Equation group: Questions and answers*. Moscow. Retrieved from https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf

Leed, M. (2013). *Offensive cyber capabilities at the operational level: The way ahead*. Washington, DC.

Lerner, J., & Keltner, D. (2001). Fear, anger, and risk. *Journal of Personality and Social Psychology*, *81*(1), 146–159. http://doi.org/10.1037//O022-3514.81.1.146

Levin, J. (2006). Choice under Uncertainty. In *Lecture Notes*. Stanford, CA. Retrieved from http://web.stanford.edu/~jdlevin/Econ 202/Uncertainty.pdf

Lichtenstein, S., Fischhoff, B., & Phillips, L. D. (1977). *Calbration of probabilities: The state of the art*. (H. Jungermann & G. De Zeeuw, Eds.)*Decision Making and Change in Human Affairs: Proceedings of the Fifth Research Conference on Subjective Probability, Utility, and Decision Making*. Darmstadt: Springer Netherlands.

Loomes, G., & Sugden, R. (1982). Regret theory: An alternative theory of rational choice under uncertainty. *Economic Journal*, *92*(368), 805–824. Retrieved from http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/56182625?accountid=12702

Ludvig, E. A., Madan, C. R., & Spetch, M. L. (2013). Extreme outcomes sway risky decisions from experience. *Journal of Behavioral Decision Making*, *27*, 146–156. http://doi.org/10.1002/bdm.1792

Macnamara, B., Hambrick, D., & Oswald, F. (2014). Deliberate practice and performance in music, sports, education, and professions: A meta-analysis. *Association for Psychological Science2*, *25*(8), 1608–1618.

Mandiant. (2013). *APT1 exposing one of China's cyber espionage units*. Alexandria, VA. Retrieved from http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Markowitz, H. M. (1952). The utility of wealth. *Journal of Political Economy*, 60, Retrieved January 7, 2016, from http://www3.uah.es/econ/MicroDoct/Markowitz_1952_Utility of wealth.pdf

McGregor, J. (2013). Is the specter of a "Cyber Cold War" real?—The Atlantic. Retrieved January 5, 2016, from http://www.theatlantic.com/china/archive/2013/04/is-the-specter-of-a-cyber-cold-war-real/275352/

Merriam-Webster. (2015). Merriam-Webster definition of risk. Retrieved from http://www.merriam-webster.com/dictionary/risk

Milkman, K. L., Chugh, D., & Bazerman, M. H. (2009). How can decision making be improved? *Perspectives on Psychological Science*, *4*(4), 379–383. http://doi.org/http://dx.doi.org/10.1111/j.1745-6924.2009.01142.x

Netmarketshare. (2016). Desktop Operating Systems Market Share. Retrieved January 28, 2016, from https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0

NIST (2014). *Framework for improving critical infrastructure cybersecurity*. Washington, DC, Retrieved from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Novrmsky, N., & Ratner, R. K. (2003). The time course and impact of consumers' erroneous beliefs about hedonic contrast effects. *Journal of Consumer Research*, *29*(4), 507–516. Retrieved from http://cat.inist.fr/?aModele=afficheN&cpsidt=14691317

Nygren, T. E., Isen, A. M., Taylor, P. J., & Dulin, J. (1996). The influence of positive affect on the decision rule in risk situations: Focus on outcome (and especially avoidance of loss) rather than probability. *Organizational Behavior and Human Decision Processes*, *66*(1), 59. Retrieved from http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/223179153?accountid=12702

ODNI. (2008). *2008 Annual threat assessment of the Director of National Intelligence*. Retrieved from http://www.investigativeproject.org/documents/testimony/348.pdf

Orr, D., & Guthrie, C. (2006). Anchoring, information, expertise, and negotiation: New insights from meta-analysis. *Ohio State Journal on Dispute Resolution*, *21*(3), 597–628. Retrieved from http://poseidon01.ssrn.com/delivery.php?ID=289004112008115087022124104101023099025007057017006013098022076026017107009085093105005060043107058047118077070094085013004031047055012022010120000070077000125042065077116086072097083014115010101005121024096067 10

Oskarsson, A. T., Boven, L. Van, McClelland, G. H., & Hastie, R. (2009). What's next? Judging sequences of binary events. *Psychological Bulletin*, *135*(2), 262–285. http://doi.org/10.1037/a0014821

Oxford University. (2016). Oxford Dictionary definition of risk. Retrieved from https://en.oxforddictionaries.com/definition/us/risk

Pachur, T., Hertwig, R., & Wolkewitz, R. (2014). The affect gap in risky choice: Affect-rich outcomes attenuate attention to probability information. *Decision*, *1*(1), 64–78. http://doi.org/10.1037/dec0000006

Parrish, K. (2016). London Metropolitan Police pays Microsoft to keep its 27K Windows XP PCs Running. Retrieved September 1, 2016, from http://www.digitaltrends.com/computing/london-metropolitan-police-windows-xp-updates/

Pratto, F., Glasford, D. E., & Hegarty, P. (2006). Weighing the prospects of war. *Group Processes & Intergroup Relations*, *9*(2), 219–233. http://doi.org/http://dx.doi.org/10.1177/1368430206062078

Prelec, D., & Loewenstein, G. (1991). Decision making over time and under uncertainty: A Common Approach. *Management Science*, *37*(7), 770. Retrieved from http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/213167765?accountid=12702

Prietula, M., & Simon, H. (1989). The experts in your midst. *Harvard Business Review*, (January-February 1989), 120–124.

Puiu, T. (2015). Your smartphone is millions of times more powerful that all of NASA's combined computing in 1969. Retrieved May 27, 2016, from http://www.zmescience.com/research/technology/smartphone-power-compared-to-apollo-432/

Ramirez, P. A., & Levine, D. S. (2013). A review of the certainty effect and influence of information processing. *Economics: The Open-Access, Open-Assesment E-Journal*, *2013*(47). Retrieved from http://www.economics-ejournal.org/economics/discussionpapers/2013-47/file

Redding, C. (1999). Overview of LEO satellite systems. In *International Symposium on Advanced Radio Technologies* (p. 29). Retrieved from http://www.its.bldrdoc.gov/media/30335/red_s.pdf

Reuters. (2012). Aramco Says Cyberattack Was Aimed at Production. Retrieved from http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=1

Rhoads, C., & Fassihi, F. (2011). In Censorship Move, Iran Plans Its Own, Private Internet. *Wall Street Journal*. Retrieved from http://www.wsj.com/articles/SB10001424052748704889404576277391449002016

Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*.

Riley, M. (2014). How Russian Hacker Stole the NASDAQ. Retrieved from http://www.bloomberg.com/bw/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq

Risen, T. (2015, July 28). Flaw Exposes Android Phones to Stagefright Hack. *U.S. News and World Report*. Retrieved from http://www.usnews.com/news/articles/2015/07/28/flaw-exposes-android-phones-to-stagefright-hack

Sanger, D. E. (2015, July 31). U.S. Decides to Retalliate Against China's Hacking. *New York Times*. Retrieved from http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html?_r=0

Saudi Aramco Oil Company. (2015). Saudi Aramco Home Page. Retrieved from http://www.saudiaramco.com/en/home.html#our-company|/en/home/our-company/at-a-glance.baseajax.html

Savage, S. (2012). *The flaw of averages*. Hoboken, NJ: Wiley.

Schneider, D. (2007). The belief machine. In R. J. Sternberg, D. F. Halpern, & H. L. Roediger III (Eds.), *Critical Thinking in Psychology* (pp. 251–270). Cambridge: Cambridge University Press.

Schneider, J. (2016). *Digitally-enabled warfare: The capability-vulnerability paradox*. Washington, DC.

Sheppard, B., Crannel, M., & Moulton, J. (2013). Cyber first aid: proactive risk management and decision-making. *Environmental Systems Decisions*, (33), 530–535.

SIboni, G., & Kronenfeld, S. (2014). The Iranian cyber offensive during Operation Protective Edge. *INSS Insight2*, *598*. Retrieved from https://nps.illiad.oclc.org/illiad/illiad.dll?Action=10&Form=75&Value=153819

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*, *185*(4157), 1124–1131. http://doi.org/http://dx.doi.org/10.1126/science.185.4157.1124

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science*, *211*(4481), 453–458. http://doi.org/http://dx.doi.org/10.1126/science.7455683

Tversky, A., & Kahneman, D. (1992). Advances in prospect theory. *Journal of Risk and Uncertainty*, *5*, 297–323.

U.S.-China Economic and Security Review Commission. (2008). *USCC 2008 Annual Report*. Washington, DC, Retrieved from http://origin.www.uscc.gov/sites/default/files/annual_reports/2008-Report-to-Congress-_0.pdf

Van Creveld, M. (1985). *Command in war* (1st ed.). Cambridge: Harvard University Press.

Vazzano Ltd. (2011). History of marine cargo insurance. Retrieved from http://www.cargoins.com/history_content.html

Wall, K. D. (2011). *The Kaplan and Garrick Definition of Risk and Its Application to Managerial Decision Problems*. DRMI Working Paper, Naval Postgraduate School, Monterey, CA, Retrieved from http://hdl.handle.net/10945/32571

Wang, Y., Liu, D., & Ruhe, G. (2004). Formal description of the cognitive process of decsion making. In *Proceedings of the Third IEEE International Conference on Cognitive Informatics*. IEEE.

Wang, Y., & Ruhe, G. (2007). The cognitive process of decision making. *International Journal of Cognitive Informatics and Natural Intelligence*, *1*(2), 73–85.

Warrick, J. (2011). Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack. *Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021506501.html

Weber, B. J., & Chapman, G. B. (2005). Playing for peanuts: Why is risk seeking more common for low-stakes gambles? *Organizational Behavior and Human Decision Processes*, *97*(1), 31–46. http://doi.org/http://dx.doi.org/10.1016/j.obhdp.2005.03.001

White House, The. Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, Presidential Policy Directive 9 (2013). US: Homeland Security Digital Library. Retrieved from https://www.hsdl.org/?abstract&did=731087

Wilson, R. A., & Keil, F. C. (1999). *The MIT Encyclopedia of the Cognitive Sciences (MITECS)*. (R. A. Wilson & F. C. Keil, Eds.) (1st ed.). Cambridge: A Bradford Book; New Ed edition.

Yadron, S., & Gorman, D. (2013, January 16). Banks seek U.S. help on Iran cyberattacks. *Wall Street Journal*. Retrieved from http://www.wsj.com/news/articles/SB10001424127887324734904578244302923178548

Yingxu Wang, Wang, Y., Patel, S., & Patel, D. (2006). A layered reference model of the brain (LRMB). *IEEE Transactions On Systems, Man, And Cybernetics—Part C: Applications And Reviews*, *36*(2), 124–136.

Yudkowsky, E. (2008). Cognitive biases potentially affecting judgment of global risks. In N. Bostrom & M. M. Ćirković (Eds.), *Global Catastrophic Risks* (pp. 91–119). New York: Oxford University Press.

Zetter, K. (2015, January). A cyberattack has caused confirmed physical damage for the second time ever. *Wired*. Retrieved from http://www.wired.com/2015/01/german-steel-mill-hack-destruction/

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California