

Assessing and Managing Risks to Information Assurance: A Methodological Approach

**A Thesis Presented to
the Faculty of the School of Engineering and Applied Science,
University of Virginia**

**In Partial Fulfillment of the Requirements for the Degree
Masters of Science (Systems Engineering)**

**by
Gregory A. Lamm**

May 2001

REPORT DOCUMENTATION PAGE

1. REPORT DATE (DD-MM-YYYY) 01-05-2001	2. REPORT TYPE Master's Thesis	3. DATES COVERED (FROM - TO) xx-xx-2001 to xx-xx-2001
4. TITLE AND SUBTITLE Assessing and Managing Risks to Information Assurance: A Methodological Approach Unclassified	5a. CONTRACT NUMBER	
	5b. GRANT NUMBER	
	5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Lamm, Gregory A. ;	5d. PROJECT NUMBER	
	5e. TASK NUMBER	
	5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME AND ADDRESS University of Virginia School of Engineering and Applied Science Charlottesville , VA 00000	8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS ,	10. SPONSOR/MONITOR'S ACRONYM(S)	
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT A PUBLIC RELEASE		

<p>'</p>
<p>13. SUPPLEMENTARY NOTES</p>
<p>14. ABSTRACT Recent events such as the Yahoo! denial-of-service attack and the ?I Love you? virus have sparked a dramatic interest in information assurance (IA) and the future security of information infrastructures. Information systems are facing an increase in interconnectedness, interdependency and complexity. Information assurance attempts to answer critical questions of trust and credibility associated with our digital environment and it represents a myriad of considerations and decisions that transcend technological advancement, legal, political, economic, social, cultural, institutional, organizational, and educational dimensions. Despite spending millions of dollars on firewalls, encryption technologies, and intrusion detection software, information infrastructure vulnerabilities and incidents continue to happen. These trends have a significant impact on military operations in the next decades.</p>
<p>15. SUBJECT TERMS</p>

<p>16. SECURITY CLASSIFICATION OF:</p>			<p>17. LIMITATION OF ABSTRACT Public Release</p>	<p>18. NUMBER OF PAGES 304</p>	<p>19a. NAME OF RESPONSIBLE PERSON Fenster, Lynn lfenster@dtic.mil</p>
<p>a. REPORT Unclassified</p>	<p>b. ABSTRACT Unclassified</p>	<p>c. THIS PAGE Unclassified</p>			<p>19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703 767-9007 DSN 427-9007</p>

REPORT DOCUMENTATION PAGE

1. REPORT DATE (DD-MM-YYYY) 01-05-2001	2. REPORT TYPE Master's Thesis	3. DATES COVERED (FROM - TO) xx-xx-2001 to xx-xx-2001
4. TITLE AND SUBTITLE Assessing and Managing Risks to Information Assurance: A Methodological Approach Unclassified	5a. CONTRACT NUMBER	
	5b. GRANT NUMBER	
	5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Lamm, Gregory A. ;	5d. PROJECT NUMBER	
	5e. TASK NUMBER	
	5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME AND ADDRESS University of Virginia School of Engineering and Applied Science Charlottesville , VA 00000	8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS ,	10. SPONSOR/MONITOR'S ACRONYM(S)	
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT A PUBLIC RELEASE		

13. SUPPLEMENTARY NOTES
14. ABSTRACT Recent events such as the Yahoo! denial-of-service attack and the ?I Love you? virus have sparked a dramatic interest in information assurance (IA) and the future security of information infrastructures. Information systems are facing an increase in interconnectedness, interdependency and complexity. Information assurance attempts to answer critical questions of trust and credibility associated with our digital environment and it represents a myriad of considerations and decisions that transcend technological advancement, legal, political, economic, social, cultural, institutional, organizational, and educational dimensions. Despite spending millions of dollars on firewalls, encryption technologies, and intrusion detection software, information infrastructure vulnerabilities and incidents continue to happen. These trends have a significant impact on military operations in the next decades.
15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Public Release	18. NUMBER OF PAGES 304	19a. NAME OF RESPONSIBLE PERSON Fenster, Lynn lfenster@dtic.mil
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703 767-9007 DSN 427-9007

APPROVAL SHEET

This thesis is submitted in partial fulfillment of the requirements for the degree of
Masters of Science (Systems Engineering).

Gregory Allen Lamm (Author)

This thesis has been read and approved by the Examining Committee:

Professor Yacov Y. Haimes (Thesis Advisor)

Professor James H. Lambert (Chairperson)

Professor Barry W. Johnson

Accepted for the School of Engineering and Applied Science:

Dean, School of Engineering and Applied Science

May 2001

DEDICATION

I dedicate this thesis to my best friend and wonderful spouse Linda and our beautiful daughter, Shelby Marie.

ACKNOWLEDGMENTS

I thank the soldiers, noncommissioned officers and officers who mentored me so I could have an opportunity to attend graduate school and write this thesis.

I thank Tom Longstaff and Jeff Carpenter at the Software Engineering Institute and the Computer Emergency Response Team/Coordination Center at Carnegie Mellon, Pittsburgh for their assistance, information and guidance.

I thank Professor Yacov Haimes for his guidance on all my endeavors and this thesis. I consider Professor Haimes a great mentor and friend. I am grateful for the time and effort that Professor Haimes spent on furthering my knowledge as a Systems Engineer.

Most importantly, I thank Linda for her patience, guidance, understanding and love. Her smile and inspiration were essential to motivating me during the last two years. I also thank her for her positive attitude, which allowed us to go to graduate school together.

ABSTRACT

Recent events such as the Yahoo! denial-of-service attack and the ‘I Love you’ virus have sparked a dramatic interest in information assurance (IA) and the future security of information infrastructures. Information systems are facing an increase in interconnectedness, interdependency and complexity. Information assurance attempts to answer critical questions of trust and credibility associated with our digital environment and it represents a myriad of considerations and decisions that transcend technological advancement, legal, political, economic, social, cultural, institutional, organizational, and educational dimensions. Despite spending millions of dollars on firewalls, encryption technologies, and intrusion detection software, information infrastructure vulnerabilities and incidents continue to happen. These trends have a significant impact on military operations in the next decades.

This thesis identifies and develops a methodological framework for assessing and managing IA risks. The methodology builds on the framework of the Systems Engineering Design Process (SEDP), and the tools and fundamentals of the risk assessment and management framework. The methodology includes Hierarchical Holographic Modeling (HHM), Risk Filtering and Ranking Management (RFRM), risk management, IA metric analysis among others, and case-study analysis in order to gain an acceptable understanding of the problem. The HHM identifies a myriad of risk scenarios and sources of risk that are innate to current complex information systems. The flexibility of the HHM philosophy permits limitless representations of a system’s perspectives, constrained only by the knowledge, creativity, and imagination of the analyst and the appropriateness of the modeling efforts. RFRM is an eight-phase process that filters and ranks the hundreds of risk scenarios to a manageable few (10-20). Risk management identifies the policy options deemed acceptable from the RFRM

and analyzes the trade-offs among the various policy options by using quantifiable risk management tools. Through case studies, we will: 1) demonstrate the efficacy of the developed methodology, 2) identify appropriate metrics to gauge the usefulness of the methodology, and 3) verify the suitability of the methodology as a “prototype” for this complex problem. The case study process compares examples of organizations that employ or fail to employ risk assessment measures. This process analyzes the wealth of statistical data on losses due to system failures, to intrusions or to vulnerabilities of information assurance.

List of Acronyms

Acronym	Definition
AAR	After Action Review
ACERT	Army Computer Emergency Response Team
ADDS	Army Data Distribution System
AF	Air Force
AFATDS	Advanced Field Artillery Tactical Data System
ASAS	All-Source Analysis System
BCIS	Battlefield Combat Identification System
BER	Bit Error Rate
C4I	Command, Control, Computers and Communications
C4ISR	Command, Control, Computers, Communications, Surveillance and Reconnaissance
CDF	Cumulative Distribution Function
CERT/CC	Computer Emergency Response Team/Coordination Center
CIA	Central Intelligence Agency
CIAO	Critical Information Assurance Office
CIP	Critical Infrastructure Protection
COMSEC	Communication Security
COTS	Commercial-off-the-shelf Software
DII	Defense Information Infrastructure
DoD	Department of Defense
DOS	Denial of Service
EO	Executive Order
FAADC2	Forward-Area Air Defense Command and Control System
FBI	Federal Bureau of Investigations
FII	Federal Information Infrastructure
GAO	Government Accounting Office
GIG	Global Information Grid
GII	Global Information Infrastructure
GQM	Goal-Question-Metric Method
HHM	Hierarchical holographic Modeling
IA	Information Assurance
IARI	Information Assurance Research Institute
IEW	Intelligence Electronic Warfare
II	Information Infrastructure
IITF	Information Infrastructure Task Force
INFOSEC	Information Security
IO	Information Operations
I-O	Input-Output
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
IT	Information Technology
JV	Joint Vision
LCC	Lifecycle Costs
LOC	Lines of Code
MTBF	Mean Time Between Failures

MTTF	Mean Time to Failures
MTTHE	Mean Time to Human Error
MTTR	Mean Time to Repair
NASA	National Aeronautical Science Agency
NII	National Information Infrastructure
NIPC	National Information Protection Center
NSA	National Security Agency
NSC	National Security Council
OPFOR	Opposing Forces
OPSEC	Operations Security
PCCIP	President's Commission on Critical Infrastructure Protection
P-CMM	People Capability Maturity Model
PDD	Presidential Decision Directive
PDF	Probability Distribution Function
PMRM	Partitioned Multi-objective Risk Method
PPTP	Point-to-point Tunneling Protocol
RA	Risk Assessment
RFRM	Risk Filtering and Ranking Method
SEDP	Systems Engineering Design Process
SPB	Security Policy Board
TTP	Tactics, Techniques, and Procedures
USD	United States Dollar
USMA	United States Military Academy
VPN	Virtual Private Network
Y2K	Year 2000

Table Of Contents

<u>CHAPTER 1</u>	<u>BACKGROUND</u>	<u>1</u>
1.1	<u>OVERVIEW</u>	1
1.2	<u>PROBLEM STATEMENT</u>	4
1.3	<u>STATEMENT OF NEED</u>	5
1.4	<u>STAKEHOLDERS</u>	6
1.5	<u>THESIS TASKS AND CONTRIBUTIONS</u>	7
1.5.1	<i>Thesis Tasks Completed</i>	7
1.5.2	<i>Thesis Contributions Completed</i>	8
<u>CHAPTER 2</u>	<u>INFORMATION ASSURANCE TRENDS</u>	<u>10</u>
2.1	<u>CRITICAL INFRASTRUCTURE PROTECTION (CIP) [CLARK, 2000]</u>	10
2.1.1	<i>Executive Order 13010</i>	10
2.1.2	<i>PCCIP Findings</i>	11
2.2	<u>CYBER TRENDS WITHIN INFORMATION ASSURANCE</u>	12
2.3	<u>MILITARY AND DEFENSE TRENDS</u>	17
2.3.1	<i>What's at stake for the military?</i>	17
2.3.2	<i>Military Trends</i>	17
2.3.3	<i>Rome Laboratory Incident</i>	20
2.3.4	<i>Solar Sunrise Incident</i>	22
2.3.5	<i>Conclusions</i>	23
<u>CHAPTER 3</u>	<u>INFORMATION ASSURANCE</u>	<u>24</u>
3.1	<u>INFORMATION ASSURANCE OVERVIEW</u>	24
3.2	<u>INFORMATION ASSURANCE DEFINITIONS</u>	25
3.3	<u>INFORMATION ASSURANCE CHALLENGES</u>	26
3.3.1	<i>Information Assurance Example 1: Y2K</i>	28
3.3.2	<i>Information Assurance Example 2: Microsoft's VPN</i>	29
<u>CHAPTER 4</u>	<u>INFORMATION ASSURANCE METHODOLOGY</u>	<u>30</u>
4.1	<u>OVERVIEW OF METHODOLOGY</u>	30
4.2	<u>METHODOLOGY CONCEPTION AND FRAMEWORK</u>	31
<u>CHAPTER 5</u>	<u>HIERARCHICAL HOLOGRAPHIC MODELING</u>	<u>38</u>

5.1	INTRODUCTION	38
5.2	HHM HEAD TOPICS	43
	A. Organizational	43
	B. People (Human Factors)	47
	C. Assets	48
	D. Software Failures	49
	E. Threats	50
	F. Architecture	52
	G. Information Environment	53
	H. Information Operations	55
	I. Knowledge Management	57
	J. Models and Methodologies	58
CHAPTER 6	INFORMATION ASSURANCE METRICS	60
6.1	INTRODUCTION	60
6.2	METRICS OVERVIEW	61
6.3	METRIC ASSIGNMENTS	63
	6.3.1 Types of Measurement	63
	6.3.2 Metric Categories	64
	6.3.3 Metric Scales	64
6.4	METRIC TAXONOMY DEVELOPMENT	66
	6.4.1 Objective Oriented Metrics	66
	6.4.2 Metric Taxonomy	67
	6.4.2.1 Step 1 (Determine the Organizational or Systems Objectives)	69
	6.4.2.2 Step 2 (Determine Impacts and Consequences needed to be Measured)	73
	6.4.2.3 Step 3 (Determine the Appropriate Metrics)	73
	6.4.2.4 Step 4 (Determine Range, Benchmark, and Metric Units)	73
	6.4.2.5 Step 5 (Determine Validation and Implementation Rules)	74
6.5	INFORMATION ASSURANCE METRICS (DEFINITIONS AND REPRESENTATION)	74
6.6	INFORMATION ASSURANCE METRIC CHARACTERISTICS AND VALUE	74
CHAPTER 7	DESCRIPTION AND DEMONSTRATION OF THE IA	
METHODOLOGY		75
7.1	METHODOLOGY DESCRIPTION AND INTRODUCTION	75
7.2	INFORMATION ASSURANCE SCENARIO	76

7.3	<u>STEP A: PROBLEM DEFINITION</u>	79
7.3.1	<u>Step A.1: Address All Decision Making Levels</u>	81
7.3.2	<u>Step A.2: Address Risk Assessment: Question One</u>	82
7.3.3	<u>Step A.3: Hierarchical Holographic Modeling</u>	85
7.3.4	<u>Step A.3.1: Addressing Sources of Failure</u>	91
7.4	<u>STEP B: ANALYTICAL SYSTEM EVALUATION</u>	95
7.4.1	<u>Step B.1: Address Risk Assessment: Questions Two and Three</u>	95
7.4.2	<u>Step B.2: Risk Filtering, Ranking and Management (RFRM)</u>	96
7.4.2.1	<u>Step B.2.1: Filtering Based on Level of Decisionmaking, Organizational Scope, and Temporal Domain</u>	96
7.4.2.2	<u>Hierarchy Decisionmaking Process</u>	99
7.4.2.3	<u>Step B.2.2: Filtering and Ranking Using the Ordinal Version of the US Air Force Risk Matrix</u>	99
7.4.2.4	<u>Step B.2.3: Multi-Attribute Evaluation</u>	105
7.4.2.5	<u>Step B.2.4: Filtering and Ranking Using the Cardinal Version of the US Air Force Risk Matrix</u>	113
7.5	<u>STEP C: SYSTEM MODELING AND ANALYSIS</u>	119
7.5.1	<u>Step C.1 Model Building and Model Representation (Input-Output Modeling)</u>	121
7.5.2	<u>Step C.2: Influence Diagrams and Event Trees Diagrams</u>	124
7.5.2.1	<u>Influence Diagrams</u>	124
7.5.2.2	<u>Event Tree Diagrams</u>	127
7.6	<u>STEP D: SYNTHESIS OF ALTERNATIVES</u>	131
7.6.1	<u>Step D.1: Metric Identification</u>	131
7.6.1.1	<u>STEP 1 (Determine the organizational or system objectives)</u>	132
7.6.1.2	<u>STEP 2 (Determine the impacts and consequences needed to be measured)</u>	133
7.6.1.3	<u>STEP 3 (Determine the appropriate metrics for the filtered risk scenarios)</u>	135
7.6.1.4	<u>STEP 4 (Determine range, benchmark, and metric units)</u>	135
7.6.1.5	<u>STEP 5 (Determine metric validation and implementation rules)</u>	136
7.6.2	<u>Step D.2: Address Risk Management Questions</u>	137
7.6.3	<u>Step D.3: Risk Management</u>	138
7.6.4	<u>Step D.4: Quantitative Risk Identification and Analysis</u>	141
7.6.4.1	<u>Fault-tree Analysis</u>	142
7.6.4.2	<u>Risk of Extreme Event Analysis</u>	144
7.6.4.3	<u>Partitioned Multi-objective Risk Method</u>	145

7.6.4.4	Fractile Distribution Analysis	147
7.6.4.5	Uncertainty and Sensitivity Analysis	147
7.7	STEP E: ALTERNATIVE REFINEMENT	149
7.7.1	Step E.1: HHM Refinement	149
7.7.2	Step E.2: Information Assurance Case Studies	150
7.8	STEP F: DECISIONMAKING	150
7.8.1	Step F.1: Multi-objective Trade-off Analysis	150
7.8.2	Step F.2: Addressing the Affect Heuristic	151
7.9	STEP G: PLAN OF ACTION	153
7.9.1	Step G.1: Decision Making Process (Execute Recommendations)	153
7.9.2	Step G.2: Gather Additional Information (Re-evaluate)	153
7.9.3	Step G.3: Iterate (Repeat Steps E and F)	153
CHAPTER 8	FAULT-TREE ANALYSIS AND FRACTILE DISTRIBUTION METHOD	
ANALYSIS		154
8.1	FAULT-TREE ANALYSIS	154
8.1.1	Problem Definition	154
8.1.2	Reliability	157
8.1.2.1	Series Systems	158
8.1.2.2	Parallel Systems	159
8.1.3	Description of each event	161
8.1.3.1	Event 1: Division Command Radio Net Failure	164
8.1.3.2	Event 2: Organizational Failure	164
8.1.3.3	Event 3: Relay Elements	164
8.1.3.4	Event 4: Retransmission Elements	164
8.1.3.5	Event 5: Field Unit Radio Elements	165
8.1.3.6	Event 6: Operator Failure	165
8.1.3.7	Event 7: Leadership Failure	165
8.1.3.8	Event 8: Antenna	165
8.1.3.9	Event 9: Power	166
8.1.3.10	Event 10: COMSEC	166
8.1.3.11	Event 11: Radio	166
8.1.3.12	Event 12: Hardware Failure	166
8.1.3.13	Event 13: Software Failure	167

8.1.3.14	Event 14: Human Failure.....	167
8.1.4	<i>Policy Option Designs</i>	167
8.1.5	<i>Analysis of the Fault-Tree</i>	171
8.2	FRACTILE DISTRIBUTION ANALYSIS.....	174
CHAPTER 9	INFORMATION ASSURANCE CASE STUDIES	184
9.1	INTRODUCTION.....	184
9.2	ANALYSIS OF CASE STUDIES.....	190
CHAPTER 10	CONCLUSIONS AND FUTURE RESEARCH	191
10.1	CONCLUSIONS.....	191
10.2	FUTURE RESEARCH.....	192
APPENDIX A: FAULT-TREE DIAGRAMS	193
APPENDIX B: HHM FIGURES	196
APPENDIX C: IA METRIC DEFINITIONS AND REPRESENTATIONS	241
APPENDIX D: IA METRIC CHARACTERISTICS	270
REFERENCES	274

List Of Figures

<u>FIGURE 1: CERT/CC REPORTED INCIDENTS [CERT/CC, 1999]</u>	13
<u>FIGURE 2: SOURCES OF NETWORK FAILURE [SVP, 1992]</u>	14
<u>FIGURE 3: INTERNET USER AND NODE EXPANSION VERSES INTRUSIONS PREDICTION</u>	16
<u>FIGURE 4: ATTACK SOPHISTICATION VERSES REQUIRED KNOWLEDGE</u>	18
<u>FIGURE 5: DISA VULNERABILITY ASSESSMENT (1996) [US GAO, 1996]</u>	19
<u>FIGURE 6: ROME LAB INCIDENT [US GAO, 1996]</u>	22
<u>FIGURE 7: RISK ASSESSMENT AND MANAGEMENT FRAMEWORK [HAIMES, 1998]</u>	31
<u>FIGURE 8: SYSTEM ENGINEERING DESIGNING PROCESS (SEDP) AND INFORMATION ASSURANCE METHODOLOGY</u>	35
<u>FIGURE 9: INFORMATION ASSURANCE METHODOLOGY</u>	36
<u>FIGURE 10: OVERVIEW OF COMPLETE INFORMATION ASSURANCE HHM (HEAD-TOPICS A, B, C, D, AND E)</u>	41
<u>FIGURE 11: HHM OVERVIEW OF COMPLETE INFORMATION ASSURANCE HHM (HEAD-TOPICS F, G, H, I, AND J)</u>	42
<u>FIGURE 12: INFORMATION ASSURANCE TRADEOFF ANALYSIS [SAYDIARI, 1999]</u>	53
<u>FIGURE 13: INFORMATION OPERATIONS ELEMENT STATE SPACE [FM 100-6, 2000]</u>	56
<u>FIGURE 14: METRIC CHARACTERISTICS</u>	63
<u>FIGURE 15: GENERIC OBJECTIVE VALUE HIERARCHY STRUCTURE [WILLIS, 2000]</u>	67
<u>FIGURE 16: INFORMATION ASSURANCE METRIC GENERATION FRAMEWORK</u>	68
<u>FIGURE 17: INFORMATION ASSURANCE METRIC VALUE HIERARCHY STRUCTURE (EXAMPLE 1: OVERALL)</u>	72
<u>FIGURE 18: INFORMATION ASSURANCE METRIC VALUE HIERARCHY STRUCTURE (EXAMPLE 2: CONDENSED)</u>	72
<u>FIGURE 19: INFORMATION ASSURANCE INTERLOCKING COMMUNITY COMPLEXITY</u>	86
<u>FIGURE 20: PARTIAL HHM (HEAD-TOPIC A.8)</u>	88
<u>FIGURE 21: PARTIAL HHM BASED (HEAD-TOPICS B.2, C.5, D.7, AND E.9)</u>	89
<u>FIGURE 22: PARTIAL HHM BASED (HEAD-TOPICS F.3, G.5, H.7, I.3, AND J.7)</u>	90
<u>FIGURE 23: SOURCES OF FAILURE [HAIMES, 1998]</u>	91
<u>FIGURE 24: INFORMATION LOSS BREAKDOWN (CRIME/LOSS BREAKDOWN)</u>	94
<u>FIGURE 25: COMPUTER NETWORK OPERATING SYSTEM FAILURES [SCHWEBER, 1997]</u>	94
<u>FIGURE 26: RISK MATRIX WITH NATURAL LANGUAGE FOR STEP B.2.2</u>	102
<u>FIGURE 27: COLOR ASSESSMENT AND INTERPRETATION TABLE</u>	103

FIGURE 28: ATTRIBUTES AND SUB-CATEGORIES FOR FILTERING SCENARIOS	108
FIGURE 29: CARDINAL RISK MATRIX VERSION [HAIMES ET AL., 2001C]	114
FIGURE 30: MODELING DIAGRAM ROADMAP	121
FIGURE 31: INFORMATION ASSURANCE I-O MODEL	124
FIGURE 32: QUALIFIED PERSONNEL INFLUENCE DIAGRAM	125
FIGURE 33: SITUATIONAL AWARENESS INFLUENCE DIAGRAM	127
FIGURE 34: RADIO COMMUNICATIONS EVENT TREE DIAGRAM	129
FIGURE 35: QUALIFIED PERSONNEL EVENT TREE DIAGRAM	130
FIGURE 36: FILTERED RISK SCENARIO METRIC REPRESENTATION	132
FIGURE 37: IA DIVISION PROJECT TEAM EXERCISE METRIC VALUE HIERARCHY STRUCTURE	133
FIGURE 38: FAULT-TREE SYMBOLS	143
FIGURE 39: PROBABILITY DENSITY FUNCTION OF FAILURE RATE DISTRIBUTIONS	146
FIGURE 40: MAJOR SOURCES OF UNCERTAINTY [HAIMES, 1998]	148
FIGURE 41: MULTI-OBJECTIVE TRADE-OFF ANALYSIS	151
FIGURE 42: COMMAND OPERATION FM NET [FM 11-32, 2000]	155
FIGURE 43: RADIO NET CONFIGURATION EXAMPLE 1	156
FIGURE 44: RADIO NET CONFIGURATION EXAMPLE 2	157
FIGURE 45: COMPONENTS IN SERIES	158
FIGURE 46: OR GATE	159
FIGURE 47: COMPONENTS IN PARALLEL	160
FIGURE 48: AND GATE	160
FIGURE 49: FAULT-TREE FOR POLICY OPTION D	163
FIGURE 50: RELIABILITY RATE DESIGN	170
FIGURE 51: COST AND UNRELIABILITY PLOT	173
FIGURE 52: CUMULATIVE DISTRIBUTION FUNCTION FOR POLICY E	176
FIGURE 53: PROBABILITY DENSITY FUNCTION (POLICY E)	176
FIGURE 54: COST VERSES TRADITIONAL EXPECTED VALUE (F_5)	179
FIGURE 55: EXCEEDANCE PROBABILITY AND UNRELIABILITY RATE FOR POLICY E	181
FIGURE 56: TRADITIONAL AND CONDITIONAL EXPECTED VALUE COMPARISON	183
FIGURE 57: CASE STUDY ANALYSIS	185
FIGURE 58: FAULT-TREE DIAGRAMS FOR POLICY OPTIONS A, B, C, F, G, H, AND I	194
FIGURE 59: FAULT-TREE DIAGRAM FOR POLICY OPTION E	195
FIGURE 60: HHM DIAGRAM (HEAD-TOPIC: A.1)	197
FIGURE 61: HHM DIAGRAM (HEAD-TOPIC: A.2)	198

FIGURE 62: HHM DIAGRAM (HEAD-TOPICS: A.3)	199
FIGURE 63: HHM DIAGRAM (HEAD-TOPIC: A.4)	200
FIGURE 64: HHM DIAGRAM (HEAD-TOPICS: A.5, A.6 AND A.7)	201
FIGURE 65: HHM DIAGRAM (HEAD-TOPIC: A.8)	202
FIGURE 66: HHM DIAGRAM (HEAD-TOPIC: A.9)	203
FIGURE 67: HHM DIAGRAM (HEAD-TOPIC: A.10)	204
FIGURE 68: HHM DIAGRAM (HEAD-TOPICS: A.11, A.12, A.13 AND A.14)	205
FIGURE 69: HHM DIAGRAM (HEAD-TOPICS: A.15, A.16, A.17 AND A.18)	206
FIGURE 70: HHM DIAGRAM (HEAD-TOPIC: A.18)	207
FIGURE 71: HHM DIAGRAM (HEAD-TOPICS: A.19 AND A.20)	208
FIGURE 72: HHM DIAGRAM (HEAD-TOPICS: B.1, B.2 AND B.3)	209
FIGURE 73: HHM DIAGRAM (HEAD-TOPIC: B.4)	210
FIGURE 74: HHM DIAGRAM (HEAD-TOPICS: B.5 AND B.6)	211
FIGURE 75: HHM DIAGRAM (HEAD-TOPICS: B.7 AND B.8)	212
FIGURE 76: HHM DIAGRAM (HEAD-TOPIC: C.1)	213
FIGURE 77: HHM DIAGRAM (HEAD-TOPICS: C.2, C.3 AND C.4)	214
FIGURE 78: HHM DIAGRAM (HEAD-TOPICS: C.5, C.6 AND C.7)	215
FIGURE 79: HHM DIAGRAM (HEAD-TOPIC: D.1)	216
FIGURE 80: HHM DIAGRAM (HEAD-TOPICS: D.2, D.3, D.4 AND D.5)	217
FIGURE 81: HHM DIAGRAM (HEAD-TOPICS: D.6, D.7, D.8, D.9 AND D.10)	218
FIGURE 82: HHM DIAGRAM (HEAD-TOPIC: D.11A-D.11E)	219
FIGURE 83: HHM DIAGRAM (HEAD-TOPIC: D.11F-D.11K)	220
FIGURE 84: HHM DIAGRAM (HEAD-TOPICS: E.1, E.2 AND E.3)	221
FIGURE 85: HHM DIAGRAM (HEAD-TOPIC: E.4)	222
FIGURE 86: HHM DIAGRAM (HEAD-TOPICS: E.5, E.6, E.7, AND E.8)	223
FIGURE 87: HHM DIAGRAM (HEAD-TOPIC: E.9)	224
FIGURE 88: HHM DIAGRAM (HEAD-TOPICS: E.10 AND E.11)	225
FIGURE 89: HHM DIAGRAM (HEAD-TOPICS: F.1, F.2 AND F.3)	226
FIGURE 90: HHM DIAGRAM (HEAD-TOPICS: F.4, F.5 AND F.6)	227
FIGURE 91: HHM DIAGRAM (HEAD-TOPICS: F.7, F.8 AND F.9)	228
FIGURE 92: HHM DIAGRAM (HEAD-TOPICS: G.1, G.2 G.3 AND G.4)	229
FIGURE 93: HHM DIAGRAM (HEAD-TOPICS: G.5, G.6, G.7 AND G.8)	230
FIGURE 94: HHM DIAGRAM (HEAD-TOPICS: H.1 AND H.2)	231
FIGURE 95: HHM DIAGRAM (HEAD-TOPICS: H.3, H.4, H.5, H.6 AND H.7)	232

FIGURE 96: HHM DIAGRAM (HEAD-TOPICS: I.1, I.2, I.3 AND I.4)	233
FIGURE 97: HHM DIAGRAM (HEAD-TOPIC: I.5)	234
FIGURE 98: HHM DIAGRAM (HEAD-TOPICS: I.6 AND I.7)	235
FIGURE 99: HHM DIAGRAM (HEAD-TOPIC: J.1)	236
FIGURE 100: HHM DIAGRAM (HEAD-TOPIC: J.2)	237
FIGURE 101: HHM DIAGRAM (HEAD-TOPIC: J.3A-J.3F)	238
FIGURE 102: HHM DIAGRAM (HEAD-TOPIC: J.3G-J.3K)	239
FIGURE 103: HHM DIAGRAM (HEAD-TOPIC: J.4)	240

List Of Tables

<u>TABLE 1: IA CHALLENGES WITH ASSOCIATED STATISTICS</u>	27
<u>TABLE 2: SEDP TO INFORMATION ASSURANCE HEAD-TOPIC CHANGES</u>	32
<u>TABLE 3: INFORMATION ASSURANCE SYSTEMS DESIGN METHODOLOGY ACTIVITIES AND RESULTS</u>	37
<u>TABLE 4: IA METRIC VALUE HIERARCHY OBJECTIVE CHARACTERISTICS</u>	71
<u>TABLE 5: STAKEHOLDER-OBJECTIVE PRIORITY TABLE</u>	81
<u>TABLE 6: HHM GLOBAL AND SUB-TOPICS SELECTED FOR THE IA METHODOLOGY</u>	87
<u>TABLE 7: SOURCES OF FAILURE IN THE PUBLIC SWITCHED TELEPHONE NETWORK</u>	93
<u>TABLE 8: STEP B.2.1 RISK FILTERING CONSIDERATIONS</u>	97
<u>TABLE 9: INITIAL HHM TRACKING TABLE</u>	98
<u>TABLE 10: RISK SEVERITY FOR RISK SCENARIOS IN STEP B.2.2</u>	104
<u>TABLE 11: RISK SCENARIO DESCRIPTIONS</u>	107
<u>TABLE 12: DEFENSIVE ATTRIBUTES OF THE SYSTEM</u>	110
<u>TABLE 13: SCALE LEVELS FOR THE CRITERIA [HAIMES ET AL., 2001C]</u>	111
<u>TABLE 14: RATING RISK SCENARIOS AGAINST THE SEVEN ATTRIBUTES</u>	112
<u>TABLE 15: RESULTS FROM STEP B.2.4</u>	116
<u>TABLE 16: METRIC IMPACT AND CONSEQUENCES [LAMM, L., 2001]</u>	134
<u>TABLE 17: METRIC IMPACT INTERPRETATION [LAMM, L., 2001]</u>	134
<u>TABLE 18: OBJECTIVE-CONSEQUENCE MAPPING TABLE FOR MISSION IMPACTS</u>	135
<u>TABLE 19: SUBTOPIC IA METRIC MAPPING</u>	136
<u>TABLE 20: RISK MANAGEMENT QUESTIONS AND SUB-QUESTIONS</u>	138
<u>TABLE 21: POLICY OPTIONS FOR THE RISK SCENARIO: QUALIFIED PERSONNEL</u>	140
<u>TABLE 22: POLICY OPTIONS FOR RISK SCENARIO: RADIO COMMUNICATIONS</u>	141
<u>TABLE 23: QUANTITATIVE ANALYSIS EFFORT</u>	142
<u>TABLE 24: RADIO NET POLICY OPTIONS</u>	162
<u>TABLE 25: RELIABILITY DATA FOR POLICY OPTIONS</u>	171
<u>TABLE 26: FAULT-TREE ANALYSIS DATA</u>	172
<u>TABLE 27: RISK SCENARIO (RADIO) UNRELIABILITY PROBABILITIES</u>	175
<u>TABLE 28: PROBABILITY DENSITY FUNCTION STATISTICS FOR FIGURE 53</u>	177
<u>TABLE 29: COST AND TRADITIONAL EXPECTED VALUE</u>	178
<u>TABLE 30: WORST 10% UNRELIABILITY CALCULATIONS FOR POLICY OPTIONS</u>	180
<u>TABLE 31: SUMMARY OF RESULTS FOR POLICY OPTIONS</u>	182

<u>TABLE 32: INFORMATION ASSURANCE CASE STUDY ATTRIBUTES</u>	187
<u>TABLE 33: INFORMATION ASSURANCE CASE STUDY ATTRIBUTES (CONTINUED)</u>	188
<u>TABLE 34: INFORMATION ASSURANCE CASE STUDY ATTRIBUTES (CONTINUED)</u>	189
<u>TABLE 35: CASE STUDY RESULTS</u>	190
<u>TABLE 36: INFORMATION ASSURANCE METRICS</u>	269
<u>TABLE 37: INFORMATION ASSURANCE METRIC CHARACTERISTICS</u>	273

List Of Equations

<u>EQUATION 1: TRADITIONAL EXPECTED VALUE</u>	146
<u>EQUATION 2: EXTREME EVENT CONDITIONAL EXPECTED VALUE</u>	146
<u>EQUATION 3: CUMULATIVE DISTRIBUTION FUNCTION</u>	147
<u>EQUATION 4: PROBABILITY DISTRIBUTION FUNCTION</u>	147
<u>EQUATION 5: SYSTEM SERIES RELIABILITY</u>	159
<u>EQUATION 6: SYSTEM SERIES RELIABILITY</u>	161
<u>EQUATION 7: TRADITIONAL EXPECTED VALUE</u>	177
<u>EQUATION 8: POLICY E TRADITIONAL EXPECTED VALUE CALCULATIONS</u>	178
<u>EQUATION 9: PROBABILITY OF EXCEEDANCE AT THE 0.10 (POLICY E)</u>	180
<u>EQUATION 10: CONDITIONAL EXPECTED VALUE FOR POLICY E</u>	181
<u>EQUATION 11: CONDITIONAL EXPECTED VALUE FOR POLICY E BY INTEGRATION</u>	182

Chapter 1 Background

1.1 Overview

The US maintains the most developed information infrastructure in the world. The increasing threats to our critical infrastructures are complex, and their extremely advanced technologies are widely distributed. The President's Commission on Critical Infrastructure (PCCIIIP) [PCCIP, 1997] conducted a yearlong study and concluded that critical infrastructure attacks and information infrastructure attacks via cyberspace are a great risk to our nation. The government recognized that a threat against any of the eight critical infrastructures could "disrupt our daily lives"¹ but also significantly impact our national and economic security. The nation's growing dependency on the National Information Infrastructure (NII) [Lewis, 2000] makes it vulnerable against physical and cyber attacks.

Prior to information technology and computer systems, infrastructures were simple, independent, and single layer entities, making them relatively easy to protect. Information technology (IT) [Longstaff and Haimes, 2000] greatly increased the complexity of infrastructures, specifically the information infrastructure, the kernel of the other eight national infrastructures. An isolated failure of the past, caused by human error, weather, or malicious attack now results in widespread disasters, happening sequentially over time or simultaneously.

Infrastructures are increasing the size of their computer networks by adding hardware, and new dimensions of complexity and connectivity. This multidimensional information infrastructure crosses both organizational and national boundaries with no single entity (government or private sectors) in control or responsible for protecting the

¹ Information Warfare, Brian C. Lewis, [Lewis, 2000]

information within these infrastructures. For that reason alone protecting, reacting and reconstituting information as an infrastructure is extremely difficult, and a shared concern.

Critical infrastructures are interconnected and interdependent allowing cyber attacks to more easily disrupt, destroy or modify information across many layered networks. Cyber attacks focus on destructive infringement of the information infrastructure. An example of this infringement is virus propagation, which causes system and information chaos. In severe cases services cannot be provided, information cannot be sent or retrieved, and productivity is lost.

With the overwhelming number of cyber attacks that cause information degradation, loss and damage, steps are needed to combat future attacks. Cyber attacks are a great threat because they can be accomplished from a great distance and little cost to our adversaries and enemies. Current tools for threat, vulnerability, and risk analysis are not suited for cyber attacks. New strategies, models and approaches must be developed to protect and defend our critical infrastructures.

The military depends on the availability of the national critical interconnected infrastructures for deployments, logistic sustainability, and current and future operations. The infrastructures are highly dependent on each other. For example, the NII requires telecommunications and power generation so information can be shared, transported, stored and communicated. Power generation is dependent on gas and oil delivery systems and these delivery systems are dependent on transportation systems and so on. The size, complexity, physical nature, organizational distribution and rate of change in the dimensions of the information networks makes it difficult to fully diagram or model the information component of an infrastructure. Information assurance (IA) [Skroch, 1999] if properly defined and executed can simplify the interconnectedness and interdependency of our nation's infrastructures. Albert Einstein said it best, "Everything

should be as simple as possible, but no simpler.² Information assurance is critical to functionally understanding system interaction, cascading effects, and cross-infrastructure behavior but a methodology is needed to improve the way organizations design, implement, protect and recovery information and systems, in order to increase the trust between user and system.

Cyber attacks on the nation's critical infrastructures increased drastically over the last three years. The Internet is doubling every 12 months and security incidents are increasing at a rate equal to the square root of the number of Internet connections. Many forecasts predict that the cost and manpower needed to combat incidents and intrusions will continue to increase annually. Chapter 2 offers further evidence of the challenges within IA across all organizations.

Information assurance has the ability to offer insight and problem solution concepts within a complex and difficult area. Information assurance is not about security *per se*, but about trust that information presented by the system is accurate and is properly represented; its measure of the level of acceptable risk depends on the critical nature of the system's mission [Longstaff and Haimes, 2000]. Longstaff and Haimes [2000] specified IA as a quality attribute of the information in both the input and output variables of the system connoting the level of trust affecting that system.

Other definitions and scopes for IA are contained in Chapter 3 but for this thesis the following definition is used: "Information Assurance represents the trust and credibility associated with information systems as well as a myriad of considerations and decision associated with our digital environment." Chapter 4 presents an IA methodology that uses various system engineering tools and risk assessment processes to identify, assess and manage the risks associated with IA. Chapter 5 identifies

² <http://rescomp.stanford.edu/~cheshire/einsteinquotes.html>

Hierarchical holographic Modeling as a key component in identifying risks to the system. Chapter 6 illustrates IA metrics used to measure the systems and organizational generated policies. Chapter 7 illustrates each step of the methodology by applying a scenario-based example. Chapter 8 depicts fault-tree and fractile distribution analyses as methods needed to quantify the risks associated with IA. Chapter 9 shows the importance of systematic and comprehensive risk assessment and management through case study analysis. Chapter 10 concludes the thesis with final thoughts and future research.

1.2 Problem Statement

Cyber attacks can be catastrophic events potentially costing dollars, lives, and assets. Probabilistic risk assessment and management along with decision support tools minimizes the uncertainty and improves IA within an organization. The complexity of IA represents a myriad of considerations and decisions that exceed technological advancement, and surpass legal, political, economic, social cultural, institutional, organizational, and educational dimensions. This may explain the difficulties associated with IA. Gallanger and Appenzeller [1999] define a complex system as one whose properties are not fully explained by an understanding of its components parts [Haimes, 2000a]. There are several hundred organizations, individuals and systems committed to providing protection to our physical and cyber critical infrastructures. This multiple hierarchy framework associated with IA, contributes to the overall complexity of IA. To add more complexity to the problem, there is a large hierarchical, interdependent, and interconnected decisionmaking process associated with IA. Weng et al., [1999] argue that complexity arises from the large number of components, from the connections among component, and from the spatial relationships between components [Haimes, 2000a].

We lack an understanding of what components are associated with IA and how those components are arranged or selected in the mitigating risks associated with IA. The problem is then, in order to achieve an acceptable level of IA, we have to understand and model the complexity, uncertainty, interconnectedness, and interdependencies associated with the information infrastructure. This translates to having full situational awareness of all the Army's command and control systems and their interrelationships. This thesis focuses on developing a methodological framework for assessing and managing the risks posed by all IA threats (e.g., cyber attacks, design flaws, weather, human error). It also serves as a "prototype" for applying risk assessment and management to IA, which we believe is important in mitigating the risks associated with cyber attacks. With a comprehensive and systematic risk assessment- and management-integrated processes, IA protects the most important non-human element of an organization – its information.

1.3 *Statement of Need*

Several important issues exist when considering how to improve IA as a science and as a methodology. As a science there is very little understanding of IA. The current models offer no quantitative risk assessment or metrics in modeling and problem evaluation. Currently, there are very few IA metrics to assess the design, and quantify the progress of IA systems, policies and measures. A comprehensive engineering approach and specific engineering tools is needed to understand the complete IA problem. Because there is a lack understanding of IA, we are repeating the same mistakes and in most cases we are reacting to our mistakes. This thesis presents a risk assessment and management framework that quantitatively evaluates the policies generated from the IA methodology, which is the major contribution of this thesis.

If information assurance has a 99.99 percent success rate, what is the damage in cost, time and lives within the 10,000th organization? That organization might be providing emergency medical treatment, military assistance, military defense or emergency disaster services. Those organizations might not think 99.99 percent success rate is good enough [Donahue, 2000].

1.4 Stakeholders

There are four groups that can benefit from this Information Assurance Thesis. The first and most important group is the US Army and the hard working men and women who have a need to improve IA. Secondly, the Department of Defense (DoD) [Lewis, 2000], which provides direction for the US Army with policy and support. DoD is also an organization that is looked at by other federal and private sector organizations, as a leader in IA. Industry and academia can benefit greatly from this thesis because these organizations provide the hardware and software tools, education curriculum, and the research dollars for IA. Lastly, the general public can benefit from the thesis because they form the personnel pool within the first three groups. All stakeholders have a vested interest in IA's success and share similar objectives – profit, cost, risk, security, trustworthiness, survivability, etc. Many of these objectives are conflicting. Industry seeks to maximize profit, while the US Army and DoD seek to minimize cost and risk. The trade-offs among multiple non-commensurate and conflicting and competing objectives is the heart of risk management [Haimes, 1998].

The need for an IA methodology is particularly important to the military. Joint Vision 2020 commits the US military to rely heavily on information technology, information superiority in C4ISR, and on information systems [Haimes et al., 2001b]. Risk assessment and management within the Joint Vision 2020 framework is crucial because some technologies, tactics, techniques and procedures will not mature based

on the vision's blueprint. Changes in the world, technology, and visions will render some points debatable. The uncertainty the military and its soldiers face in world order (enemy forces), technological advances, budget, manpower reductions, and tactics must be addressed through systematic and comprehensive risk assessments.

Information assurance will play a pivotal role in the success of the joint vision framework. Unfortunately, there is little discussion on the subject of IA. Woodward [2001] cites IA as a subset of Information Operations but it is the core concept in achieving information superiority and its operational capabilities. Information assurance attempts to answer critical questions of trust and credibility associated with our digital environment. Joint Vision 2020 plans to upgrade division- and brigade- level command posts with numerous C4ISR systems that convey large amounts of information and knowledge to the decisionmaker and their staffs about operations and the battlespace. However, when conflicting information between systems arise, which systems should the decisionmaker trust? The infantry squad leader has the same dilemma in battlespace management and situational awareness (e.g., "I see a friendly unit but the information system is telling me it is an enemy unit."). Lack of useful information coupled with technological limitations will remain an obstacle to decisionmakers and make IA critically important.

1.5 Thesis Tasks and Contributions

1.5.1 Thesis Tasks Completed

1. Methodology Selection and Development: Determined a methodological framework for identifying, assessing and managing sources of risks associated with the US Army.

- Used hierarchical holographic modeling (HHM) [Haimes, 1981, 1998] as a holistic methodology to better understand the complexity, uncertainty, interconnectedness and interdependencies with IA.
 - Used risk filtering, ranking and managing to reduce, simplify and classify the sources of risk to a manageable level.
2. Model Selection: Determined appropriate models in order to analyze the relationship of the variables and attributes associated with the filtered sources of risk. Develop a model selection framework to understand the connectedness and dependencies between risk scenarios and other components.
 3. Metric Selection: Developed a list of appropriate IA metrics (i.e., measures of effectiveness, risk, cost and trust metrics) for organizations to measure the effectiveness of risk mitigation policy selection. The IA metrics form a “grab bag” used to compare systems and functions within an organization and compare policy options generated by the organization to mitigate IA risks. Developed a metric taxonomy for organizations to select appropriate objectives and metrics associated with information systems. As part of the methodology, a few subtopics are assigned metrics in order to gauge the usefulness of the policy options and methodology.
 4. Quantifiable Risk Analysis: Determined the appropriate risk analysis tools to facilitate decisionmaking within IA. The tools are applied to the IA methodology and model to validate, and demonstrate the benefits of risk analysis and management for IA problems. The analysis forms the basis for trade-off analysis among various competing attributes.
 5. Case Study Analysis: Identified examples of organizations that employ or fail to employ risk assessment measures to illustrate proactive risk assessment investment equates to an increase in IA. The case studies verify the suitability of the methodology as a “prototype” for this complex problem, and identify gaps and weakness of the methodology.

1.5.2 Thesis Contributions Completed

The major contribution is the development of a methodological framework, which decisionmakers can assess risks associated with information assurance and assist them

in formulating and selecting policies consistent with protecting information systems.

Other contributions to the thesis consist of:

1. Constructed metrics and a metric taxonomy needed to gauge the suitability of the methodology and potential policy options.
2. Developed case study material to demonstrate the efficacy of the methodology.
3. Developed policy options associated with using risk management.
4. Developed quantifiable risk assessment tools, and techniques in order to make improved IA decisions.

Chapter 2 Information Assurance Trends

2.1 Critical Infrastructure Protection (CIP) [Clark, 2000]

“Our responsibility is to build the world of tomorrow by embarking on a period of construction – one based on current realities but enduring American values and interests....”

President William J. Clinton
National Security Strategy

Terrorist bombings of US forces in Saudi Arabia, the World Trade Center and the Oklahoma City Federal building reminded Americans and government leaders that the hostile threats against the United States were not eliminated after the end of the Cold War [PCCIP, 1997]. In 1993, President Clinton issued Executive Order (EO) #12864 which established the Information Infrastructure Task Force (IITF) [Lewis, 2000]. The task force's main responsibilities lied on addressing issues such as national security, emergency preparedness, system security, and network protection implications. In 1995, Presidential Decision Directive (PDD) 39 [Schwartau, 2000] (US Policy on Counterterrorism) was issued in response to the worst US “soil” terrorist attack in our nation's history, the Oklahoma City Federal Building bombing [PCCIP, 1997]. The PDD had specific goals aimed at reducing vulnerabilities and identifying threats associated with physical attacks.

2.1.1 Executive Order 13010

On July 15, 1996, President Clinton issued Executive Order #13010, which established a commission to conduct critical infrastructure risk assessment and risk

mitigation for critical infrastructures. Executive Order #13010 recognized that there are national, critical infrastructures and that their destruction, degradation, or incapacity would have a debilitating impact on the defense of United States of America. The EO #13010 also created the President's Commission on Critical Infrastructure Protection (PCCIP) and three key organizations. These organizations include: (1) Critical Infrastructure Assurance Office (CIAO); (2) National Information Protection Center (NIPC); and (3) Information Sharing and Analysis Center (ISAC) [PCCIP, 1997]. The organizations are interagency organizations that span across law enforcement, defense, counter terrorism, cabinet offices, research, academia and the private sector.

The PCCIP was charged to: (1) assess vulnerabilities and threats to the critical infrastructures, (2) identify relevant legal and policy issues, (3) recommend to the president a national policy and implementation strategy for protecting critical infrastructures, and (4) propose any necessary statutory or regulation changes. The PCCIP created a certain institutional structure for understanding the interdependencies and interconnectedness of our critical infrastructures.

2.1.2 PCCIP Findings

The final PCCIP report outlined that significant problem with the critical infrastructure protection architecture. The report summarized five major problems:

1. "Our economy is increasing reliant upon interdependent and cyber-supported infrastructure and non-traditional attacks on our infrastructures and information systems may be capable of significantly harming both our military power and economy" [PCCIP, 1999],
2. Cyber threats and vulnerabilities are poorly understood,
3. Capabilities to damage information networks are inexpensive and available,
4. Old and current tools for threat and vulnerability analysis for risk assessment to cyber attacks are not suited,

5. Risk mitigation crisis response management tools lack coordination to create and maintain national awareness of problems and solutions.

The preceding events lead President Clinton to sign PDD 63 on May 22, 1998. The PPD directs the federal government to lead by example and be the “model” for the private sector [Minihan, 1999]. Overall PDD 63 outlined that by May 2000, all government agencies would have “an initial operational capability” and by May 2003, all agencies should achieve and maintain capability to protect the nation’s critical infrastructure against any threat that would diminish the ability to perform essential national security missions, ensure the general public health, and safety, and ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services [PCCIP, 1999].

2.2 Cyber Trends within Information Assurance

The world has recently seen such events as the World Trade Center bombing, the Tokyo subway chemical attack, the terrorist assault on the military on the Khobar Towers in Dhahran, Saudi Arabia, and the U.S.S. Cole in Yemen. Lives, property, resources, and money were lost in these physical attacks. Cyber attacks represent the new wave of threats that cause greater damage plus the loss of critical information. The risk is great for us and very little to our adversaries. Attacks can come from anywhere in the world, through dial-up lines, over the Internet or other related information networks and come singularly or as a distributed combination of attacks. This makes tracing the intruders very difficult. Attackers against system and information assurance have the advantage over the current policies and technologies that we have in place.

The US maintains the most developed information infrastructure in the world. The increasing threats to our critical infrastructures are complex, and their extremely

advanced technologies are widely distributed. Computer Emergency Response Team/Coordination Center (CERT/CC) [CERT, 1999] is an organization at the forefront of improving information assurance for the nation and the world and has seen a 64% increase in intrusions each year from 1998 to 2000 (Figure 1). Computer system vulnerabilities have also increased according to CERT with JAVA and Windows operating systems at times reporting one-security vulnerability per month [CS 551, 2000].

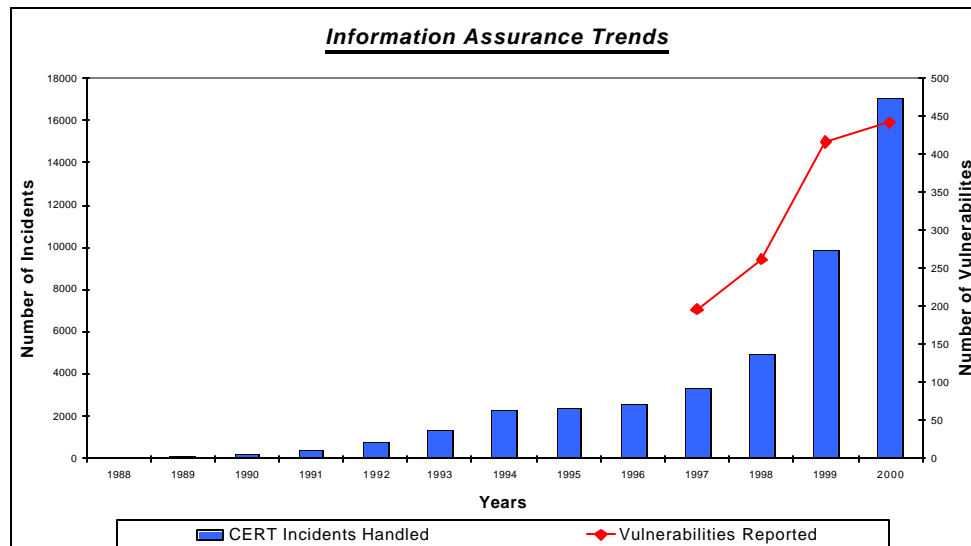


Figure 1: CERT/CC Reported Incidents [CERT/CC, 1999]

One can argue that vulnerability is simply evaluating where exposure is greatest and access is weakest [NSTAC, 1997]. Exposures to our infrastructures have increased since the conception of the Internet in 1969 due to increased interconnectedness, interdependency and complexity of information infrastructures. As an example, in April 1988, a disgruntled employee unleashed a logic bomb that destroyed a New Jersey engineering company's computer file system, which controlled its production line [MITRE, 1999]. The logic bomb corrupted the company's backup computer files and disabled company operations permanently. The company could not reconstitute its file

system and was forced into bankruptcy. The United States is vulnerable to many threats such as hackers, terrorists, hardware and software failures, cyber criminals, insiders and deliberate attacks from our adversaries. The sources of risks are not just software and hardware related and includes human and organizational aspects (Figure 2).

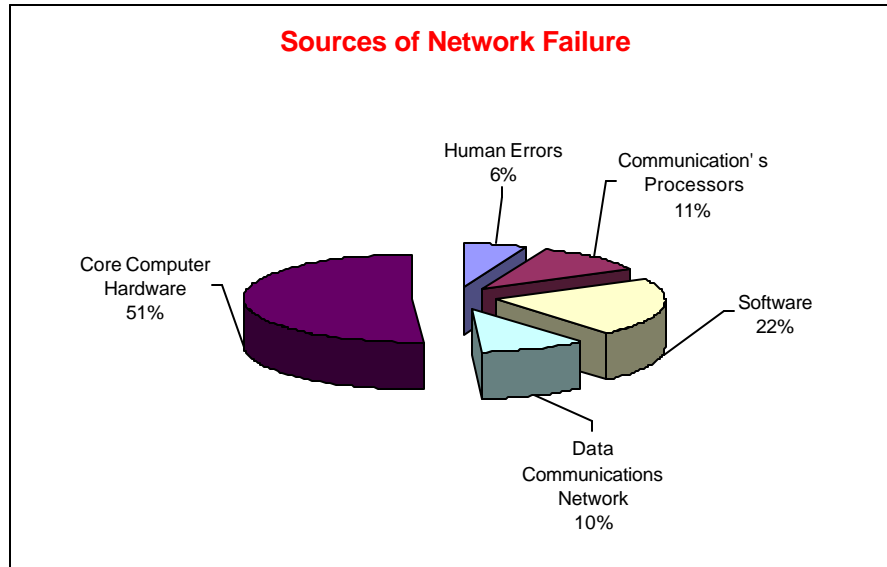


Figure 2: Sources of Network Failure [SVP, 1992]

According to MI2G, a security company, there are more than 300 new viruses discovered every month [Adams, 2000]. These viruses include the very serious and costly Melissa, Chernobyl, ExploreZip and "I love you" virus outbreaks. The Melissa virus in March 1999, Chernobyl virus in April and the ExploreZip worm virus in June cost corporations in unplanned and unbudgeted resources. Melissa and Chernobyl cost businesses approximately \$7 billion [Adams, 2000]. MI2G added the cost of disabled computers and their downtime is already exceeding \$2.5 billion for each major cyber warfare incident. The overall cost for lost productivity; network downtime and virus eradication for 1999 was \$12 billion [Adams, 2000]. The "I love you" virus cost approximately \$10 billion alone. This cost explosion is caused largely by the expansion

of the Internet and email connectivity. In 1999, AOL estimated that its networks transport 760 million email messages a day. In comparison the US Postal Service averages only half as many letters and most of the viruses are transported via email.

A fairly new form of attack is the denial of service (DOS) attack, which is used by hackers or criminals to deny service to customers. On a CSI/FBI (Computer Security Institute/ Federal Bureau of Investigations) computer security survey 2000 [CSI, 2000], 27% of the 273 organizations surveyed had a DOS attack. In the previous three years (1997-1999), 93% reported a DOS attack from the 521 security practitioners in US corporations, government agencies and financial institutions that were surveyed [CSI, 1999]. These attacks temporarily crippled Yahoo! and the eBay Web sites in February 2000, costing \$8.2 million. In 1998 and 1999, losses from DOS were on average \$77,000, and \$116,250 per organization, respectively for a survey conducted by the FBI of 640 corporations [CSI, 1999].

Information assurance is a multidimensional problem involving not only external aspects but also internal aspects. Insider attacks accounted for 55% of the security problems in their organizations [CSI, 1999]. For the military and the federal government, insider attacks have national security and military readiness impacts. In surveys conducted on computer crime, most organizations cite an Internet connection as the frequent point of attack. System penetration by outsiders has also increased between 1997 and 1999, and is projected to steadily increase [CSI, 1999]. Overall, hackers caused 50% of the financial losses by using the Internet 57% of the time [CSI, 1999].

The number of Internet users worldwide was 300 million users as of March 2000 and estimated to be one billion by 2005 [Computer Almanac, 2000]. This tremendous usage increase is doubling the traffic on the Internet every 100 days and increasing the amount of possible intrusions into communication, and computer networks (Figure 3).

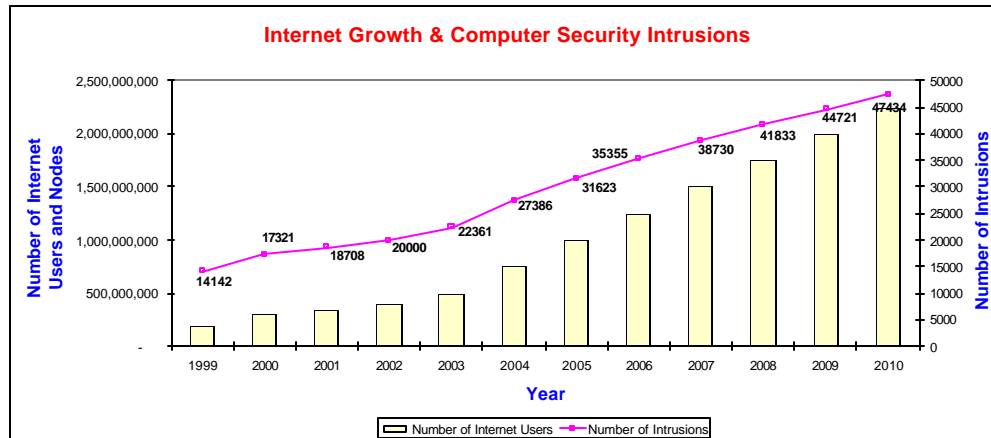


Figure 3: Internet User and Node Expansion verses Intrusions Prediction

[CERT/CC, 2000]

“If somebody wanted to launch an attack, it would not be at all difficult.³ There are plenty of opportunities for an IA incident. The US is the last military super-power with over 40% of the world's computers and the most Internet users. The US GNP is measured in the trillion dollars, our national infrastructure is complex and extremely interdependent and the military relies on information infrastructures and technology to execute operations. Information assurance related incidents (e.g., viruses, intrusions, system failures) appear regularly in the news headlines, which may be prevented with a risk assessment and management methodology.

³ Fred B. Schneider, [Christensen, 1999]

2.3 Military and Defense Trends

2.3.1 What's at stake for the military?

The military has downsized (right-sized) since Desert Shield/Storm in 1991. The forces are smaller, more mobile, and have an increase operational tempo and increase reliability on information technology to achieve mission success. No rogue nation would try to take on our nation's Navy, Army or Air Force but a rogue nation could take out a vulnerable infrastructure using fewer resources than with a physical attack. Information dominance and possible mission success are seriously affected by information infrastructure attacks. Information networks used by the military across the NII and military owned networks must be protected.

DoD is the most targeted US organization and requires a much greater need for intelligence to increase the ability to react to IA threats and recover from IA incidents.

Information assurance failure could result in:

- Decline in effective military operations.
- Defense of our nation and its interests.
- Lives, manpower and resources.
- Un-forecasted expenditures and increased military budget.
- Ability to gain a military advantage.
- Loss of information dominance and superiority.

2.3.2 Military Trends

Some critical infrastructures using .edu, .com or .net domain names enjoy less exposure than .mil or .gov [Ezell, 1997]. The military uses the Internet to exchange electronic-mail, log on to remote sites, download and upload information from remote locations, conduct video-teleconferencing, and conduct logistics and training functions. During the Persian Gulf War, the military used the Internet to communicate with its

Allies, and gather and disseminate intelligence and counter-intelligence information. Many top leaders predict an increase in the reliance of the Internet in future operations.

Each year, the attacks increase along with the sophistication of the hacker tools (Figure 4). At a minimum the attacks are a multimillion-dollar nuisance, and at worse they are a serious threat to national security and military operations. Military systems are increasingly dependent on civilian critical infrastructures. The information systems support critical functions such as daily logistics operations, weapons system research, command and control functions, and numerous other military functions.

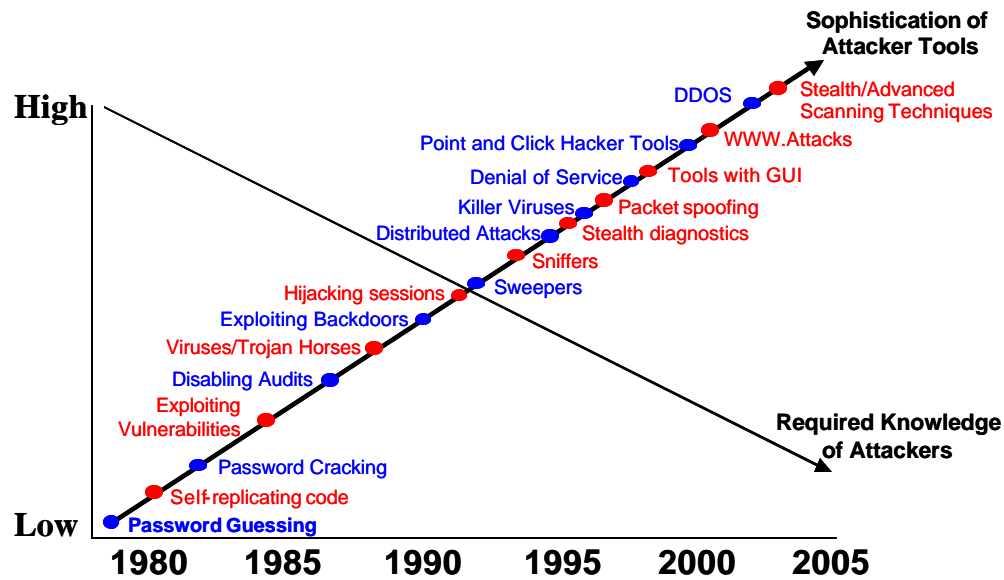


Figure 4: Attack Sophistication versus Required Knowledge

[US GAO, 1996]

The National Security Agency (NSA) [Lewis, 2000] conducted a cyberwar “fire drill” in 1997, code-named “Eligible Receiver,” in which 35 hackers were hired to gain access into government computer systems. The hackers accessed 36 of the 40,000 government networks within four days. And gained control of major power grids and could have disrupted power in Los Angeles, Chicago, Washington and New York

[Sullivan, 2000]. The hackers caused parts of the 911 services in Washington to fail; caused disruptions on DoD e-mail and telephone systems, and officers aboard an US Navy cruiser found their computer systems were attacked [Christensen, 1999].

DoD received 80 to 100 "low-level" attempts at intrusion every day [US GAO, 1996]. Each incident is researched at a great cost to budget, time and manpower. Of these, approximately 10 require detailed investigation [MITRE, 1999]. DoD cyber attacks increase every year with very serious military implications. The Department of Defense admits that a portion of the attacks may be improper log-ins by its personnel. In 1995, 250,000 cyber incidents were estimated on DoD computer networks or systems. In 1996, there were 500,000 estimated attacks with an estimated 65% causing an intrusion, which caused information compromise, network downtime, or an investigation into the intrusion, and only four percent of the attacks were detected (Figure 5).

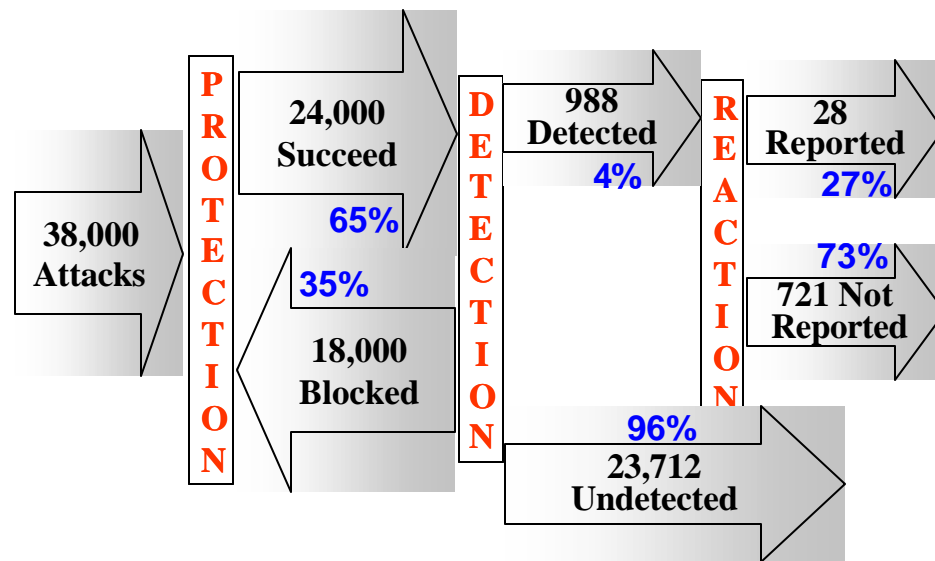


Figure 5: DISA Vulnerability Assessment (1996) [US GAO, 1996]

Cyber attacks can affect military operations and in the spring of 1999, pro-Serbian hackers infiltrated government and military sites. Serbian hackers caused a

"denial of service " but had not actually hacked into the system. The attack affected NATO's web site, which was not connected to classified systems [London Press, 2000]. In 1994, unknown attackers from two US universities and three other countries penetrated the US Naval Academy's computer systems. The attack targeted 24 servers and one router in which files were deleted and changed, two encrypted password files were compromised and over 12,000 passwords were changed. In 1995 and 1996, Argentina hackers used an US University system to break into a Naval Research Laboratory. Between 1990 and 1991, hackers from the Netherlands penetrated 34 Defense computer systems sites. The hackers browsed directories and modified systems to obtain privileges allowing for future access. The hackers copied files, e-mail, and sensitive data and stored that information on US University computers. During the Gulf War, Dutch hackers stole information about US troop movements from US Defense Department computers. The Dutch hackers tried to sell it to the Iraqis who declined because they thought the information was a hoax [Christensen, 1999]. There are other cases and each of these cases the military was unable to determine what the total information compromise cost. Two highly publicized intrusions were the Rome Laboratory Incident (Section 2.3.3) and the Solar Sunrise Incident (Section 2.3.4). These incidents illustrate the need for a methodology to reduce the risks associated with IA.

2.3.3 Rome Laboratory Incident

In one specific case, hackers attacked the Rome Laboratory, the Air-Forces premier command and control research facility. Two hackers seized control of the lab support systems, established remote links to foreign Internet sites and stole tactical and intelligence research data. In all cases, the security breaches caused service disruptions and are very expensive. The 1994 Rome Laboratory incident was estimated

to cost over \$500,000 to assess the damage, ensure system reliability, patch vulnerabilities and attempt to identify the attackers and showed the vulnerable nature of computer systems [GAO, 96-84]. It was difficult to estimate the value of the lost data but some of the files associated with the "air tasking order" research project were equal to three years of total research and four million of invested dollars.

Between March and April of 1994, over 150 Internet intrusions were made on the Rome Laboratory, which is a large Air Force command and control research facility. The attackers were identified as a British hacker and an unidentified hacker. The Air Force facility develops new technologies for command, control, communications and computers (C4I) [C4ISR, 2000] and includes the development of sensors, surveillance equipment, software engineering, artificial intelligence and battlefield management. During that period, Air Force personnel discovered a sniffer program on their computer systems. The attackers used this sniffer program and a Trojan horse to gain access and control Rome's computer network. They also took specific countermeasures to avoid being traced as depicted in Figure 6 (Page 22) by bouncing their connection from multiple routing stations.

For days, they were able to seize control of Rome's operational and support networks and established foreign Internet links, copied and downloaded critical information and masqueraded as a trusted Rome administrator to attack other government sites including: National Aeronautical Science Agency, defense contractors and Wright-Patterson Air Force Base. This incident like most used the long-haul capability of the Internet and went undetected for sometime costing time and money.

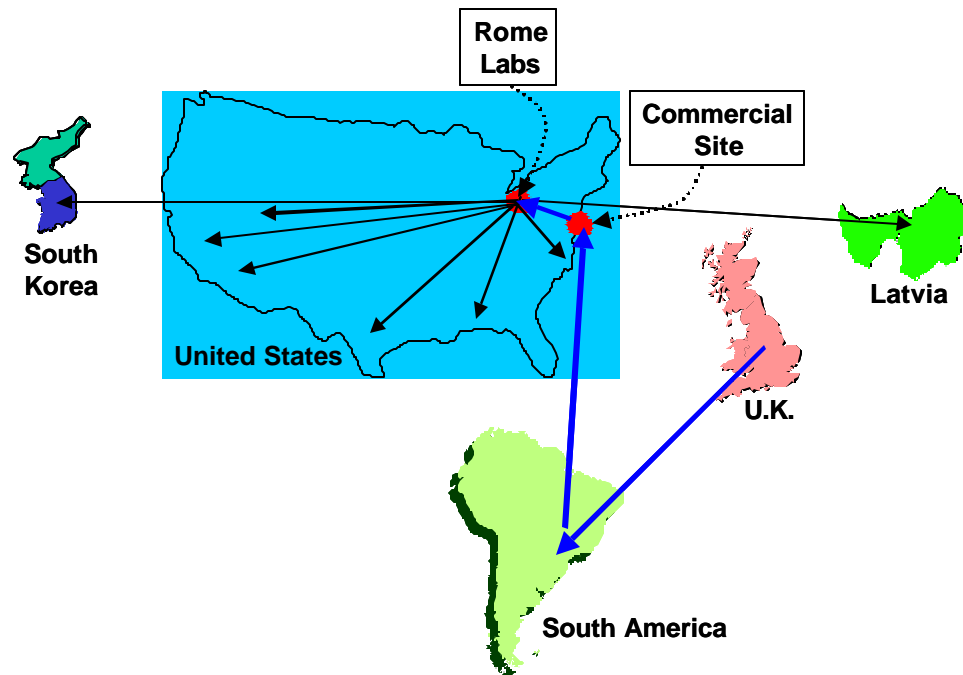


Figure 6: Rome Lab Incident [US GAO, 1996]

2.3.4 Solar Sunrise Incident

During February 1998, two 16-year old boys in California were assisted by an Israeli teenage to systematically attack DoD computer systems. The teenage boys were given the tools and knowledge from the Israeli teenager via email and chat room correspondences. The hackers targeted: 1) DoD network domain name servers, exploiting a well-known vulnerability on the SOLARIS operating system, and 2) DoD unclassified network, including key support systems for the Global Transportation System, Defense Finance System, Medical, Personnel, Logistics and electronic mail systems. The hackers obtained passwords and used a two prong coordinated effort to target the systems.

2.3.5 *Conclusions*

Defense Department has to protect a vast, complex and critical information infrastructure. It has over two million computers, 10,000 local area networks, 100 wide area networks, and 100 long-distance networks [US GAO, 1996]. Although it owns the computers and the local area networks, it owns very little of the wide area and long-distance networks. The military has moved from a stand-alone computer and information environment that performed a specific function to a globally integrated information structure called the Global Information Grid (GIG) [Woodard, 2000]. The GIG relies on the civilian infrastructure to provide network services and the information security on those networks, which it uses for communication, surveillance, information sharing, research, weapons design, finance, mobilization, targeting, operational command and control and information dominance.

The threats are real and information security costs dollars, time and manpower. These costs have increased every year for the US Army with a significant increase projected for the next five years [Schalestock, 2000]. Internet connections make it possible for enemies of the military and the US to pose a threat to the military readiness. They can gain information dominance with a smaller price tag and at a farther distance. These trends have a substantial impact on current and future military operations, and Joint Vision 2020.

Chapter 3 Information Assurance

“The art of war teaches us to rely not on the likelihood of the enemy’s not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable,” cited by Sun Tzu in *The Art of War* [Stallings, 1999].

3.1 Information Assurance Overview

Information assurance was born from a need for increased information security in our computer networks and organizational hierarchy. This is not a new concept in the military and IA builds on past security concepts such as information security (INFOSEC), communication security (COMSEC) and operations security (OPSEC). Information assurance addresses many questions about organizational, human, knowledge management and technology components within our information infrastructures, but centers on one specific question: “what will we do today to prepare ourselves for tomorrow’s information trustworthiness issues?” Individual users as well as organizations are more likely to trust a service provider who integrates quality technology with expert personnel and an efficient organizational infrastructure [Haimes, 2000c]. Trust is then a key ingredient in the outcome of IA systems, and requires contributions from multiple disciplines beyond science and engineering.

Information assurance attempts to answer critical questions of trust and credibility associated with our digital environment. It represents a myriad of considerations and decisions that transcend technological advancement, legal, political, economic, social, cultural, institutional, organizational, and educational dimensions. Despite spending millions of dollars on firewalls, encryption technologies, and intrusion detection software, information infrastructure failures, vulnerabilities and incidents continue to occur. Addressing the role of IA in the protection of intra- and inter-

dependent, and interconnected information infrastructures yields several different definitions based on the organization and their mission. The following section identifies several definitions as characterized by academia, military and government, and industry, which demonstrate the variability and complexity of IA.

3.2 Information Assurance Definitions

Academia defines IA as not about security per se but about trust that information presented by the system is accurate, available and is properly represented [Longstaff and Haimes, 2000]. As stated in Section 1.1, Longstaff and Haimes specified IA as a quality attribute of the information in both the input and output variables of the system connoting the level of trust affecting that system. Information assurance is represented in the state of the system by three attributes: accuracy (indicating a level of information integrity), representativeness (indicating a level of correct labeling of information) and criticality (indicating the importance of the system's mission).

The Information Assurance Research Institute (IARI) defines IA as one that addresses the creation of policies, procedures, and systems that provide assurance to people and organizations that [CERT/CC, 2000]:

- Individuals can trust the information they use,
- The information they are responsible for will be shared only in the manner that they expect,
- The information is available when they need it, and
- The systems process information in a timely and trustworthy manner.

IARI extends the IA definition to all information systems (i.e., large-scale, distributed, control, and embedded systems) encompassing hardware, software, and human components. The two-academia definitions represent IA as two different ideas in which neither is established or used as a standard definition.

The military and the government define IA as “information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection and reaction capabilities, and encompasses Information Security (INFOSEC) [Joint Publication 3-13, 1998].”

1. *Authentication*: Validates where the data was originated.
2. *Confidentiality*: Limits access to authorized personnel.
3. *Integrity*: Checks for errors and ensures there was no tampering of the data.
4. *Availability*: Ensures that information and the infrastructure are obtainable when needed.
5. *Non-Repudiation*: Certifies and confirms the sender of the data.

Industry defines IA as systems that ensure the right information is delivered to the correct individual(s) or system(s) at the appropriate time. In order for IA systems to achieve an acceptable level of assurance, then information systems must possess properties of survivability [Walczak, 2000], which fundamentally avoids risks to achieve its mission objectives in a timely manner. Other IA definitions exist but we chose these four definitions to illustrate that there is no one accepted definition. The purpose of this thesis is not to define IA but to define a methodology for solving IA problems. The principle of trust serves as the foundation within the IA methodology.

3.3 Information Assurance Challenges

Challenges to this problem serve as motivation and foundation for the methodology. Table 1 (Page 27) depicts some of the IA challenges and is represented by associated statistics.

IA Challenge	Associated Statistics
Attacker Motivation	Over \$1 trillion is moved electronically each day [Computer Crime, 1995].
Overall Costs	Over 90% of Fortune 500 networks have been hacked. Costs are estimated in the millions per company. Computer hacking alone exceeded \$300 billion in 1997. In 1997, 241 organizations reported \$7 million loss from computer viruses and \$2.1 million from sabotage of data or networks [CSI, 1999].
Manpower Costs	Several organizations had computer system compromised by intruders. One organization reported the loss of productivity equal to 1500 employees and another reported more than 15,000 hours of lost productivity [CERT/CC, 1999].
Complexity	There are at least 400 connected networks nationally and internationally. Estimates are that one network can have more than 1 million users [Icove et al., 1995].
Model Accuracy	Only 11% of computer crimes are reported [Stites, 1990].
Detection	Over 58% of companies have detected outsiders trying to gain computer access and 30% of companies do not know if there were attempts from outsiders to gain computer access [Sunbelt, 1999].
Threat Evaluation	FBI statistics reveal that more than 100 nations engage in corporate espionage against US companies, the federal government and the military. More than 1,100 documented incidents of economic espionage and 550 suspected incidents were reported in 1997 [Sunbelt, 1999].
Military/Defense	There were 250,000 attempts to break into DoD computer systems in 1995. 65% of the attempts were successful [US GAO, 1998].
Organizational & Human Factors	Insiders cause 60% of computer abuse and 85% of computer break-ins occur internally [Sunbelt, 1999].
Human Factors	Approximately 32% of computer network operating system failures are caused by human errors.
Viruses	There are over 100,000 known computer viruses. As many as 60% of major US corporations has experienced a virus attack [CSI, 1999].
Software & Hardware Engineering	There is no evidence of improvement in the security features products. In 1995 there were 171 total vulnerabilities reported. In 1999, that number jumped to 417 and for the first quarter of 2000 there was 106 vulnerabilities. Most of the vulnerabilities are software but hardware vulnerabilities do exist and are reported [CERT/CC, 1999].
Reconstitution Costs	Viruses and hackers cost business around the world an estimated USD 1.6 trillion in losses in 1999 [Interactive, 2000].
Interconnected Complexity	An Army tactical network consists of more than 20 C4ISR networks tied to the Internet, which itself contains thousands of complex networks.
Metrics	There are few IA metrics to determine the effectiveness of our methodologies and countermeasures. There is very little understanding of IA metrics and how to use them in measuring systems.
Education	Education and skilled IT personnel are important shortcomings in the efforts to protect critical infrastructures [Haimes, 2000c].
Risk Assessments	The CSI/FBI 2000 survey cited that only 35% of the organizations surveyed can quantify their losses. This implies a lack of risk management and IA assessments.

Table 1: IA Challenges with Associated Statistics

Information assurance success (e.g., Year 2000 (Y2K) rollover [Bennett, 1999]) and horror (e.g., Microsoft's Virtual Private Network (VPN) [Anonymous, 1998]) stories provide insight and direction into our current processes and methodologies. The next two sections describe two IA examples and illustrate the importance of risk assessments.

3.3.1 Information Assurance Example 1: Y2K

The largest IA event in history was the preparation, execution and response activities associated with the Y2K rollover. Y2K was a large success due to the preparation, focus and large-scale cooperation of all organizations involved. Y2K was a static and unique event in our understanding of information assurance and critical infrastructures.

Y2K is deemed a “special IA topic” [Bennett, 1999] because we knew exactly when, where, how and why it existed. The Y2K glitch like most of the vulnerabilities that exist in hardware and software, today, existed because programmers put it there. In the 1970's, allowing computer systems to keep track of the last two digits of the year, saved memory due to its expense. The problem existed because systems could not differentiate the two-digit year '00' between the years 1900 and 2000. Globally countries spent a trillion of dollars with the US spending about 60% [Bennett, 1999]. Even with the tremendous cost spent on Y2K, there were still incidents. As an example, a British credit card company was affected by Y2K in which retailers lost \$5 million in sales [Associated Press, 2000]. Months after 01 January 2000, CERT, the President's Y2K council, DoD and many other organizations still track Y2K related incidents. Currently, CERT has tracked zero related impacts in the US. Globally, organizations were able to leverage resources, and assess risk toward a common goal. Current resources and organizations

are stove-piped in many cases and must reconfigure unilaterally to solve future IA problems.

3.3.2 Information Assurance Example 2: Microsoft's VPN

Each month, hackers break an industry-standard security mechanism. Our next vulnerability is right around the corner and IA is needed to gain vision into that next vulnerability. An example of an unforeseen vulnerability is the Microsoft Point-to-Point Tunneling Protocol (PPTP) [Anonymous, 1998]. The protocol is used in Virtual Private Networks (VPN), which allows secure, encrypted connections between multiple link points. Virtual Private Networks are a smart way to eliminate lease lines, use the Internet long-haul capability and increase security. PPTP was viewed as the most solid and complete security system. In 1998, Microsoft's PPTP was broken by an encryption authority and later four other flaws were discovered. The question is not "will our information infrastructures get attacked", but "what will we do when it occurs and what risk assessment and management techniques will mitigate those risks?"

Chapter 4 Information Assurance Methodology

4.1 Overview of Methodology

Information assurance documents are rich on “what to do” but not on “how to do it?” An IA methodology is necessary in order to develop a common picture of the complexity, inherent risks and scale of the problem, and comprehensively quantify and manage IA risk scenarios. The purpose of the methodology is threefold. First, gain an increased understanding of the complexity, uncertainty, interconnectedness, and intra- and inter-dependencies of IA. Second, comprehensively and systematically identify, assess, and manage the risks associated with IA. Third, determine and evaluate the appropriate policies with metrics and quantitative risk analysis.

There are several design methodologies in use by engineers and scientists to solve all types of problems that exist in the real world. Most methodologies are tailored for the specific problems and parameters but include defining the problem either mathematically, figuratively or written; generating solution sets; analyzing and comparing the solution sets; and selecting the best solution through qualitative or quantitative means. The core of the methodology lies on the concepts of “risk” and “risk scenarios”. Risk is defined as a measure of the probability and severity of adverse effects, and is a quantitative entity; to manage it, we must quantify it [Lowrance, 1976]. A *risk scenario* is a combination of risk elements of that describes the causes, triggering events or the impacts of risks [Kontio, 2000]. The IA methodology presented in this thesis is based on the United States Military Academy (USMA) Systems Engineering Design Process (SEDP) [Willis, 2000], and a risk assessment and management framework. The methodology builds on the framework of the SEDP, and the tools and fundamentals of the risk assessment and management framework (Figure 7). This SEDP framework is

useful in the design of other multidisciplinary engineering systems, such as IA but also is appropriate for many other large-scale or complex problems.

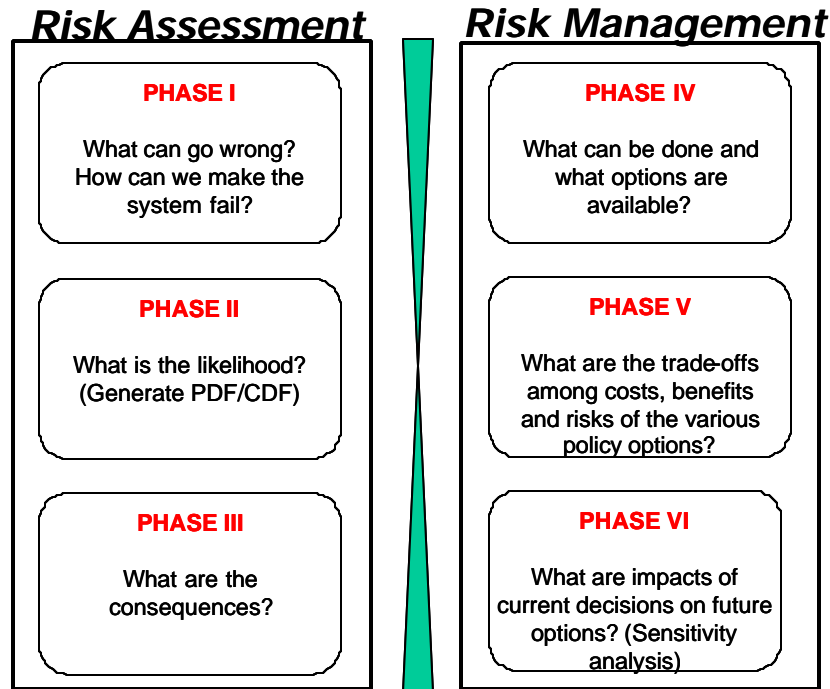


Figure 7: Risk Assessment and Management Framework [Haimes, 1998]

4.2 Methodology Conception and Framework

The US Military Academy's SEDP was chosen as the best methodology for IA because it is a proven military systematic problem-solving methodology. The SEDP has three head topics: formulation, analysis and interpretation (Figure 8, Page 35) and seven subtopics consisting of: problem definition, value system design, synthesis of alternatives, system modeling and analysis, alternative refinement, decision-making, and plan of action (labeled A through G).

Current IA methodologies have a number of weaknesses. First, current methodologies are slow, non-adaptive, and based on human assessment [Craft, 1999].

The process often leads to a checklist instead of science-based comparison or assessment of the system and its components. This drives IA processes to be expensive, inefficient, inconsistent, and incomplete [Craft, 1999]. Second, current methodologies cannot accurately model the various parameters of the system from the beginning to the end points. Addressing the total system rather than the parts of the system helps represent all the important entities, processes and components affecting the total system. Assuring the individual parts of IA systems does not guarantee the assurance of the total system. Finally, current methodologies use abstract languages to capture information assurance processes. Terms like “vulnerabilities,” “threats,” and “impacts” are too abstract to be the building blocks from which assessment methods and tools are constructed [Craft, 1999]. For these reasons, the SEDP methodology is adapted to address the current IA problems and weaknesses by integrating a framework for assessing and managing risks within IA. This framework is flexible to adapt to the risks and challenges presented by IA. Table 2 represents the head-topic changes from the SEDP methodology to the proposed IA methodology.

SEDP Head-topic		IA Head-topic	Reason for Change
Value System Design	▷	Analytical System Evaluation	Evaluate the system in order to gain an increased understanding of a large-scale system prior to adding a value to the system.
Synthesis of Alternatives	▷	System Modeling and Analysis	Model prior to generating alternatives. For this reason the head-topics are transposed.
System Modeling and Analysis	▷	Synthesis of Alternatives	

Table 2: SEDP to Information Assurance Head-topic Changes

Initially, the SEDP is integrated with the risk assessment and management tools discussed in two documents: 1) Risk Modeling, Assessment and Management [Haimes, 1998], and 2) Risk Filtering, Ranking, and Management Using Hierarchical Holographic Modeling Framework [Haimes et al., 2001c]. The SEDP subtopics not applicable to the

IA methodology are deleted, and the risk assessment and management tools are placed in a logical order beneath the head-topics by expert knowledge and literary research.

The complete IA methodology process is graphically depicted in Figure 9 (Page 36) and described in Table 3 (Page 37). The IA tools represent a range of risk assessment methods that enables decisionmakers and organizations to quantify risks and assess the challenges associated with IA. The methodology is tailored for the specific problem and the parameters of IA but is extremely flexible. The methodology includes problem definition, risk analysis and management, Hierarchical Holographic Modeling (HHM) [Haimes, 1998], Risk Filtering, Ranking and Management (RFRM) [Haimes et al., 2001c], Risk Assessment and Management Tools, Metric Analysis, Case Study Analysis, and Quantifiable Risk Assessment Analysis. There are eight major phases to the RFRM method, which were integrated throughout the methodology and form the majority of effort. The RFRM process constitutes the following phases [Haimes et al., 2001c]:

1. Scenario identification using Hierarchical Holographic Modeling (HHM) [Haimes, 1998]
2. Identified risk scenarios in phase I are filtered according to the responsibilities and interests of the current system user to about 100 scenarios (Phase II).
3. Phase III (Bi-Criteria Filtering) filters the number to 50 using a qualitative, ordinal matrix-scale of livelihoods and consequences.
4. Phase IV (Multi-Attribute Evaluation), evaluates the risk scenarios using a set of attributes, related to the ability of the scenario to defeat the resiliency, robustness, redundancy and assurance of the underlying system. This phase helps risk scenario reduction in the next phase (Phase V).
5. Phase V (Quantitative Ranking) filters the list to 10 using a quantitative matrix-scale of absolute likelihood and absolute consequence to represent the absolute importance of the remaining scenarios.

6. In Phase VI a decision analysis is performed involving estimates of cost, performance-benefits, and risk-reduction, of management options for dealing with the most urgent remaining scenarios [Haimes et al., 2001c].
7. In Phase VII, examination of the performance options selected in the previous phase is examined against the scenarios that were filtered in phases II to V.
8. In Phase VIII, experience and information gained throughout the process is used to update the scenario filtering and decision process. Also, conducting case studies assists in improving the overall methodology.

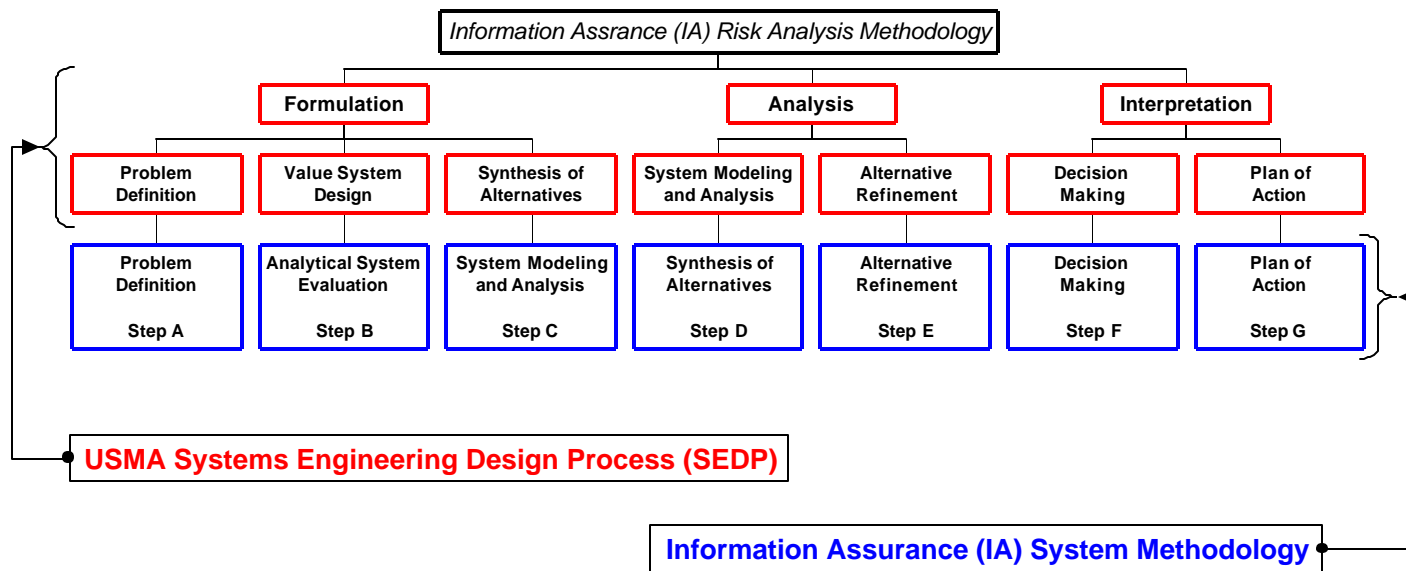


Figure 8: System Engineering Designing Process (SEDP) and Information Assurance Methodology

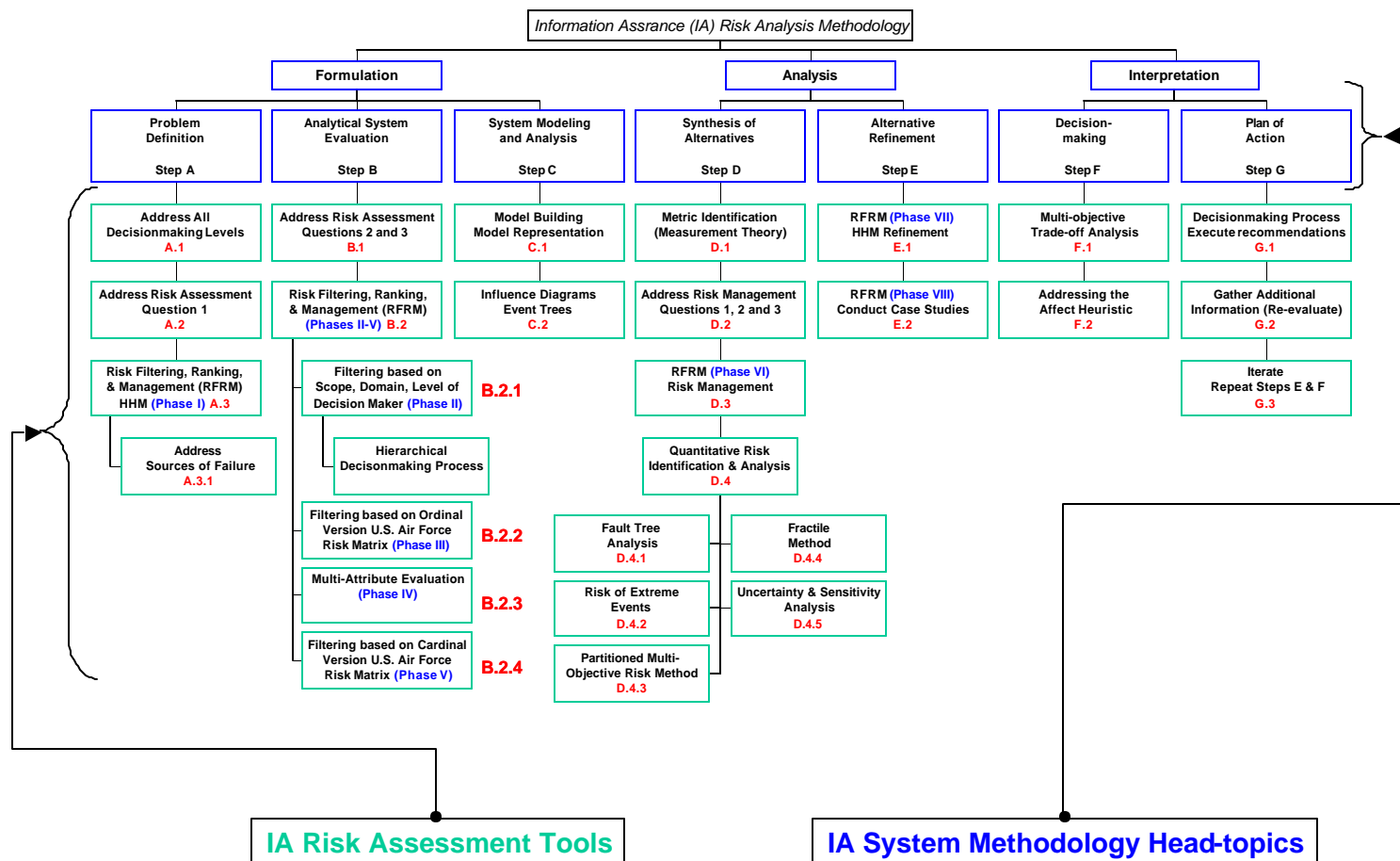


Figure 9: Information Assurance Methodology

	STEP ⁴	PROCESS	ACTIVITIES	RESULTS
Formulation	A	Problem Definition	1. Address Decision-making levels 2. Address Risk Assessment Question 1 3. Risk Filtering, Ranking & Management (RFRM); HHM Construction & Development 4. Address Sources of Failure	1. Initial road map 2. Sub-component description 3. Risk scenarios identification 4. Decision-making levels identified 5. Engineering Problem Statement 6. Overall problem and complexity understanding
	B	Analytical System Evaluation	1. Address Risk Assessment Questions 2 and 3 2. RFRM, Phases II-IV; Risk Filtering and Ranking	1. HHM Reduction (to Top 50-100) 2. HHM Reduction (to Top 25-50) 3. HHM Reduction (to Top 10-25)
	C	System Modeling and Analysis	1. Model Building (I-O Model) 2. Model Representation 3. Influence Diagrams 4. Event Tree Diagrams	1. Input/Output Model and State Space representation 2. Cascading effects understood 3. Sub-component interaction understood
Analysis	D	Synthesis of Analysis	1. Metric Identification 2. RFRM Phase V, Risk Management 3. Quantitative risk identification and analysis 4. Risk of Extreme Events 5. Fractile Method 6. Uncertainty and Sensitivity analysis 7. Fault Tree Analysis	1. IA Metrics for each filtered risk scenario (Top 10) 2. Policy generation 3. Develop quantitative results based on risk scenarios and data (e.g., probabilities). 4. Uncertainty understood and quantified 5. Use Risk Analysis tools
	E	Alternative Refinement	1. RFRM Phase VI; HHM Refinement 2. RFRM Phase VII; Conduct Surveys and Case Study Analysis	1. Reevaluate risk scenarios 2. Conduct risk assessment and management surveys to verify methodology and policies.
Interpretation	F	Decision Making	1. Interpretation of Quantitative Risk Analysis Tools 2. Trade-offs with multi-objectives 3. Addressing the Affect Heuristic	1. Decisionmaking using Quantitative Risk Interpretation and Analysis 2. Show improvement using risk and trade-off analyses 3. Decisionmaker's "gut feelings" addressed
	G	Plan of Action	1. Recommendations 2. Decisionmaking process (Execute Plan) 3. Gather additional information 4. Iterate	1. Road map complete; Planning for future operations 2. Working model or process complete 3. Making changes to original plan by repeating Steps E & F

Table 3: Information Assurance Systems Design Methodology Activities and Results

⁴ Steps A through G indicate the Methodology Head-topics located in Figure 9.

Chapter 5 Hierarchical Holographic Modeling

5.1 Introduction

Information assurance is a complex system of components performing a myriad of functions, responding to diverse elements and is composed of hundreds, and thousands of entities. Hierarchical holographic Modeling is a philosophy and methodology that enables the analyst and decisionmaker to identify most, if not all sources of risk. Building a complete or nearly complete HHM of a given organizational or technology-based system defines the risks associated within the subsystems and ultimately the total system. An HHM may be built from the ground-up if no expert evidence or documentation on the system exists, but this is very rare and a special case. Brainstorming, checklists, critical path analysis, benchmarking and simulation are a group of techniques to facilitate the HHM risk scenario identification step [Kontio, 2000]. These approaches do not bias the model but introduce a family of participants as well as the size and boundaries of the problem. The advantages of the HHM approach are as follows:

- HHM is comparable to a functional decomposition.
- HHM is a “living and breathing” modeling technique allowing for changes within the system.
- HHM bases itself on the premise that for large-scale and complex systems, more than one mathematical or conception model is possible. A mathematical model represents only one dimension and offers little insight into IA. An IA single-model analysis and interpretation does not clarify and document the sources of risk that are innate to current complex information systems, including social aspects (legal, cultural, sociological, temporal, spatial and political) and knowledge management aspects (human, management, training, and education).
- The HHM does not make any distinction between probabilities of occurrence.
- Through HHM, the decisionmakers’ visions, goals and perspectives are captured. The HHM head-topics and subtopics are decomposed for the purpose of

qualitatively or quantitatively characterizing the knowledge sought by decision-makers with different needs [Haimes, 1998].

- HHM is a holistic framework, which adds strength to the system analysis offering multiple visions and perspectives to a specific problem. HHM is extensively used in government organizations to include: PCCIP, FBI and NASA. From the HHM, all analytical methods and model are possible.
- Risk is a multi-attribute concept [Morgan et al., 2000]; HHM offers a framework in which risk attributes can be evaluated in each category.
- The flexibility of the HHM philosophy permits limitless representations of a system's perspectives, constrained only by the knowledge, creativity, and imagination of the analyst and the appropriateness of the modeling efforts [Longstaff and Haimes, 2000]. Overlapping subtopics are permitted and encouraged in order to represent the complete system from multiple perspectives and visions.

The HHM structure for IA is written primarily from a US Army perspective, which is a diversified, complex and global organization that provided a unique perspective into IA systems. It serves as an excellent model for organizations in industry, academia, and the federal government. The HHM structure is a comprehensive mechanism for risk identification and consists of a hierarchy of "Head-topics," "Subtopics," "Sub-Subtopics," etc. The HHM structure consists of 10 global categories and 92 head-topics. Figure 10 (Page 41) depicts global topics: Organizational (A), People (B), Assets (C), Software (D) and Threats (E). Figure 11 (Page 42) depicts global topics: Architecture (F), Information Environment (G), Information Operations (H), Knowledge Management (I), and Models and Methodologies (J). The 92 head-topics are further segregated into subtopics to equate to over a thousand risk-prone IA scenarios representing the "success scenarios" or the "as planned-scenarios." These as planned-scenarios become risk scenarios when disrupted and cannot be realized [Haimes, 2001c].

In this chapter only head-topics (designated by A.1, A.2, etc.) are addressed by brief explanations in this chapter. Although subtopics (designated by A.1.1, A.1.2, etc.) are crucial to comprehensively bounding and understanding IA problems, for brevity purposes all sub-topics are not addressed by explanations (Section 5.2). The HHM is not an inclusive document and requires constant reevaluation. There is no claim that the 92 head-topics or over 1300 subtopics encompass all possible IA risk scenarios for the US Army. Within the IA methodology, the 93^d head-topic may eventually surface because the HHM is a living and breathing document, and the methodology affords several iterations.

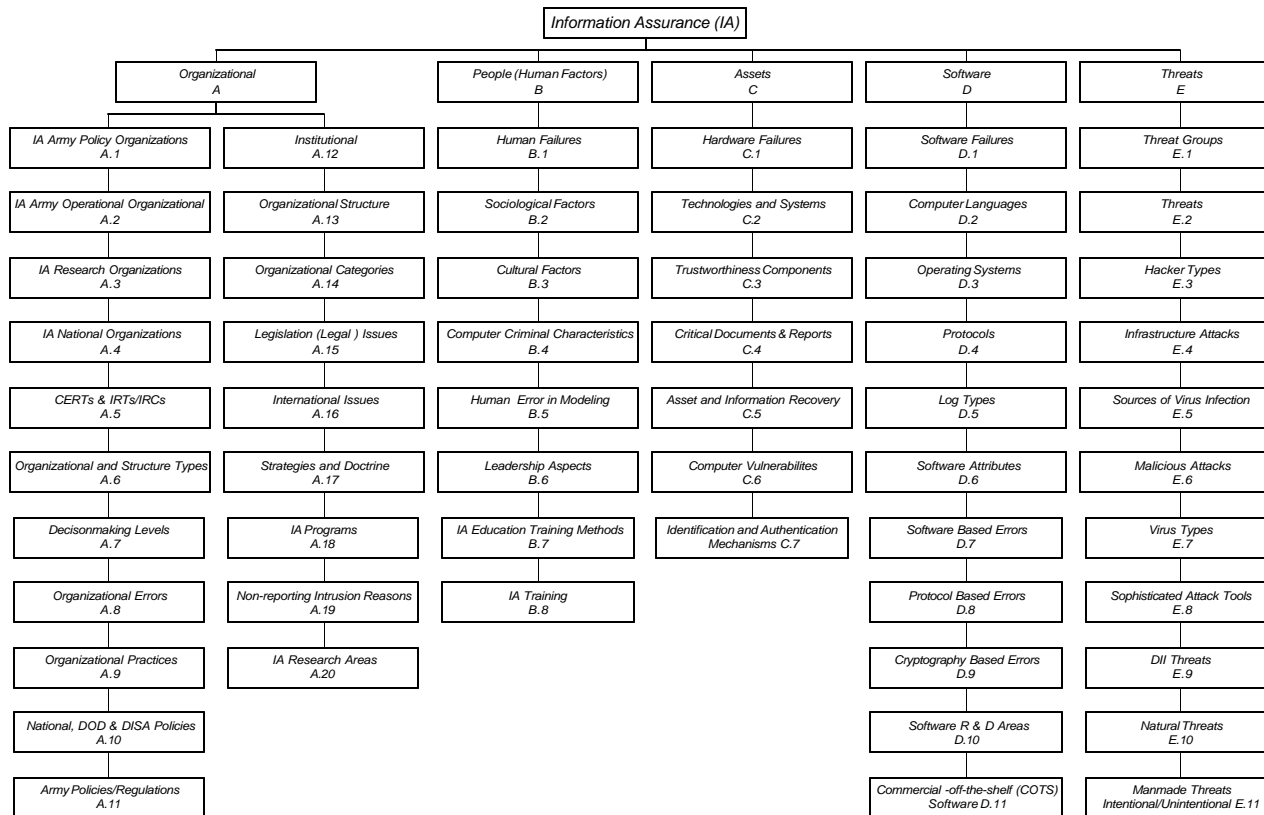


Figure 10: Overview of Complete Information Assurance HHM (Head-topics A, B, C, D, and E)

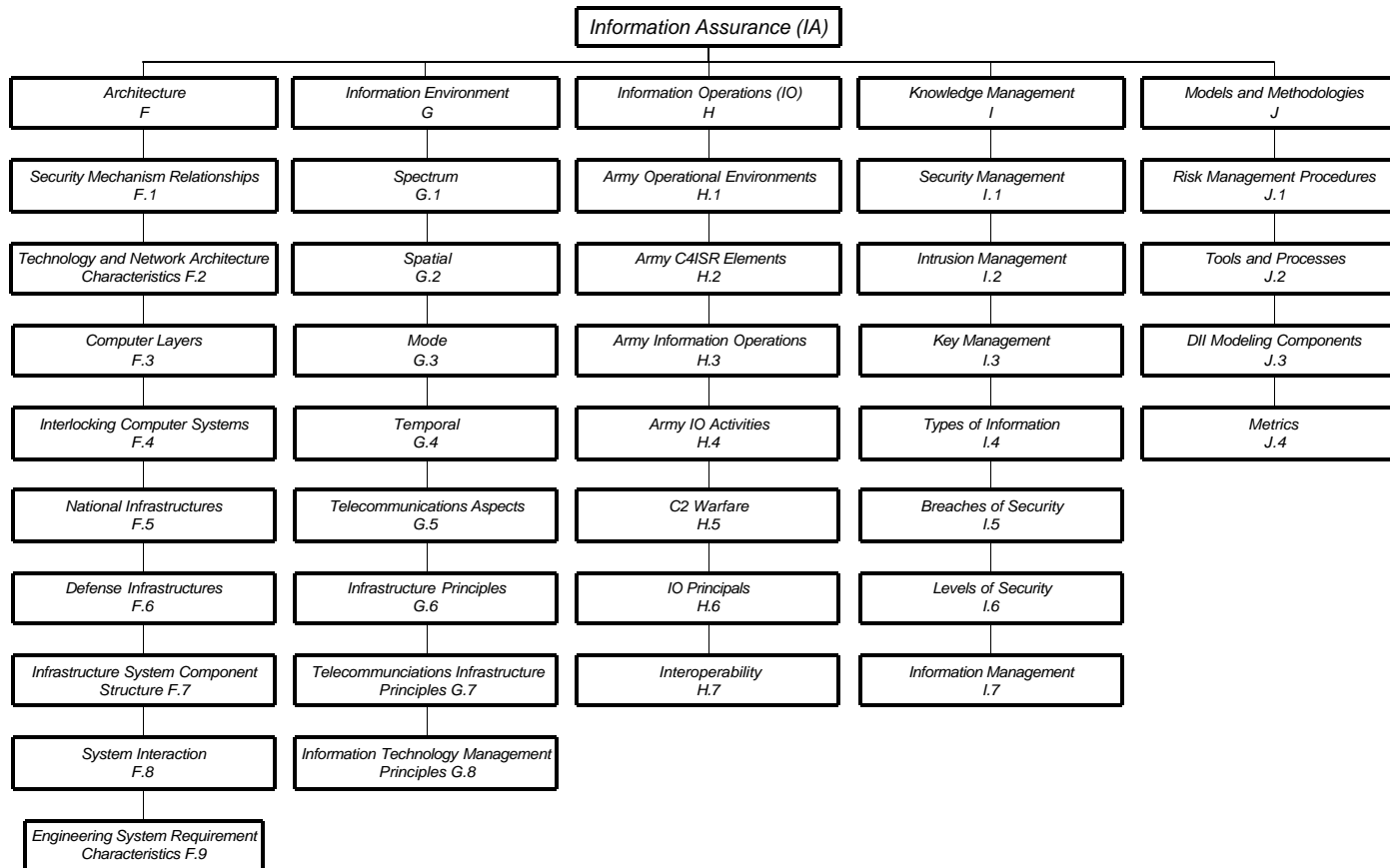


Figure 11: HHM Overview of Complete Information Assurance HHM (Head-topics F, G, H, I, and J)

5.2 HHM Head Topics

All HHM Figures for each global topic (A through J) are illustrated in Appendix B.

A. Organizational

Identifying the role and relationships that organizations play in large-scale systems (e.g., military operations, training exercises, joint military operations) is extremely critical. Organizational errors contribute a major source of error in engineering systems but most solutions tend to focus on technical solutions because of the way risks and failures are analyzed. Kuhn [1997] found that approximately 50%⁵ of the AT&T network downtime documented was caused by organization errors. Perrow [1999] identified organizational errors as one that contributes a double-penalty to complex systems. The double-penalty stems from the controls organizations place on systems and the operators that use them. Common organizational errors include: overlooking and/or ignoring defects, breakdown in communication, lack of incentives to find problems, and loss of institutional memory, etc. Organizations are structured with people who solve problems through the use of technology, common sense and knowledge and therefore, are not static but dynamic entities that are shaped by such attributes as leadership, knowledge, mission, and behavior.

⁵ Kuhn combined organizational and human errors into his calculations of network downtime

The type of boundary also defines organizations: vertical, horizontal, external and geographic [Ashkenas et al., 1995].

- Vertical: the boundaries between levels and ranks of people (e.g., Joint Chiefs of Staff, CINC's, Joint Staff, Corps and Division Commanders).
- Horizontal: the boundaries between functions and disciplines (e.g., Corps, Divisions, Marines, Air Force and Navy).
- External: the boundaries between the organization and its suppliers, customers, and regulators (e.g., contractors, vendors, and commercial telephone companies).
- Geographic: the boundaries between nations, cultures, and markets.

Organizations are at the root of dealing with IA problems and implementing their solutions. Ashkenas et al., [1995] identified the paradigm that must take place for successful organizations to make it in the digital age. Those organizations must be “boundaryless,” i.e., they must possess such fluid qualities as permeability and adaptability (technically, managerially, and culturally). Ashkenas et al., [1995] addresses organizational success factors that are measured by size, role clarity (division of labor), and specialization and control. Today, however, they are measured by speed, flexibility, integration, and innovation.

Organizational failures play an important role in major accidents and incidents but little attention is paid to the relationship between organizational failure and operator error. Johnson [1998] explains that tools and techniques, which have been developed to analyze human and system failures, cannot easily be applied to reason about organizational problems. Organizational errors create the necessary preconditions for human error and exacerbate the consequences of those errors. Organizational

practices have more significant effects in comparison to individual practices [Workplace Practices, 2000]. Poor work environment, morale, trust relations, and low commitment are correlated with lower productivity and higher production cost. Poor work climate diminishes return from other organizational changes and improvements [Workplace Practices, 2000] and can also lead to low individual trust, security violations, and insider intrusions.

Several other organizational factors have a significant role in IA and specifically in implementing Joint Vision 2020, e.g., decisionmaking, policy, legislation and international factors, strategies, and organizational programs. Decisionmaking is integrated in all aspect of daily operations and involves multiple hierarchical levels and multiple diverse situations within an organization. Policies affect IA by directing resources, providing research dollars and direction, issuing resource priorities, and influencing the relative course of actions taken against threats. Policies and procedures reflect the organization's philosophy on IA and computer security.

Legislation, policies and strategies are intertwined such that together they define standards and direction for technology, organizations and people. The inclusion of human and organizational components within any complex sociological system brings about societies use of laws and legal action against criminals. Today, as the US enters the information age, new laws are needed to combat future threats. Several legislations are used nationally and internationally in combating computer crime and vary in scope, severity and framework. International issues effect how we protect, detect, react, and recovery from computer attacks (e.g., the "I Love You" virus).

Strategies for protection of our critical infrastructures and architectures has come from a need to defend, protect and manage information against all types of threats. Strategies for enhancing our critical infrastructures and capabilities usually have three basic fundamentals: 1) increased protection from cyber attacks, 2) the ability to detect

and predict attacks, and 3) the capability to recover and respond to an attack. Strategies work efficiently, when agencies and organizations are empowered to make decisions based on real time information and analysis. Strategies must not just include the direction but the relationships between the key players (government, industry, military and academia) and the rules of engagement. Information assurance strategies and programs allow for sharing of information between the private sector and the government. These reporting schemes allow for sharing of intrusions and incidents in order to improve IA methodologies and technologies. The HHM identifies gaps, weaknesses and risks associated with risk scenarios across organizations and captures the risk scenarios associated with these factors.

B. People (Human Factors)

During unfamiliar and unanticipated situations, people rely on knowledge-based performance grounded on experience, training, common sense and perceived rules. Human error can be defined as a lack of recovery from previous unacceptable effects. With automation increasingly taking over routing tasks, operators are using less skill-based and rule-based behavior and more knowledge-based behavior [Leveson, 1995]. Mindy Blodgett states that the most sophisticated, technologically advanced security system in the world cannot protect your company's data if the people in your organization won't use it [Leveson, 1995]. More than half of all reported security violations are caused by unintentional employee action or lack of action. Technologies show promises toward protecting critical information systems but some technologies are very expensive and no single technical solution is foolproof. Investing in non-technical solutions (i.e., sociological and cultural policies, and education and training) has a significant impact on IA because social and organizational contexts are linked to a number of well-publicized disasters [Leveson, 1995].

The Software Engineering Institute (SEI) [US GAO, 1996] estimates that at least 80 percent of the security problems it addresses involve poorly chosen or poorly protected passwords by computer users. Awareness, technical- and leadership-training is essential skills for the military in this digital age. Personnel who understand the organizational policies, goals, and objectives, and are fully trained can contribute to the overall protection of the organization and help to achieve its goals. Sometimes training is available for individuals but cost, resources and time cause IA training to have a low priority. The Joint Security Commission studied the problem and stated, "because of a lack of qualified personnel and a failure to provide adequate resources, many information systems security tasks are not preformed adequately. Too often critical security responsibilities are assigned as additional or ancillary duties [US GAO, 1996]."

Culture, like sociological factors, plays an important role on our reaction to threats, errors (intentional and unintentional), education, and problem solving. Sociological factors had a profound impact on the world during the industrial age of the 19th and 20th centuries. Schein [1992, 1996] defines culture as a set of basic tacit assumptions about how the world is and ought to be that a group of people share; it determines their perceptions, thoughts, feelings, and to some degree, their overt behavior. Our culture about information technology affects the organizational and individual norms, responsibilities, and the risks society, organizations and individuals deem acceptable. For example, many organizations support teamwork and cooperation, but organizations reward individuals and feel that the best results come from a system of individual competition and rewards [Grabowski, 1998].

Leadership plays a critical role within IA. The Army defines leadership as “**influencing** people-by providing purpose, direction, and motivation-while **operating** to accomplish the mission and improving the organization [FM 22-100, 2000].” “Influencing” means getting people to do what you want them to do while “operating” are those actions taken to influence others to accomplish the mission. People will make the difference in finding and implementing IA solutions. Information assurance takes leaders that can: 1) transform tomorrow while continuing to operate today, 2) manage an uncontrollable change process, 3) lead to an unclear destination,, 4) deal with disruption, and 5) confront the need for change. The HHM identifies human factor issues (e.g., human failures, sociological and cultural factors, leadership, and organization staffing) that affect IA.

C. Assets

Defining the components both tangible and non-tangible entities, which constitute information networks is a critical step in protecting military personnel and equipment,

and executing countermeasures against all types of threats. Tangible assets include hardware and physical entities, and non-tangible assets include information or data commonly called digital or intellectual assets. Although information cannot be assured 100% of the time, it is important to: 1) understand what assets need protection, 2) understand what risks are associated with protection and restoration of critical assets, and 3) understand what resources are available in assuring information.

Trustworthiness is extremely important where dependence of systems is essential to the overall performance of the entire system. A trustworthy entity is one that deserves to be trusted and is something you attribute to a system [Survivability, 1990]. The notion of trustworthiness is a core attribute within IA and developing information systems. The hardware, and information systems are the backbone in achieving information superiority and full spectrum dominance. The assets should not be limited to command, control, communications, computers, intelligence, reconnaissance and surveillance (C4ISR) [C4ISR, 2000] systems, and include lethality technologies. The GIG encompasses many of the systems that will be used in executing operations in the upcoming decades. The HHM encompasses the risk scenarios relevant to military assets (e.g., asset restoration, hardware vulnerabilities, hardware security mechanisms and hardware failures) in order to understand what assets need protection, what risk are associated with protecting and restoring critical assts, and what resources are available within a specific operational environment.

D. Software Failures

Software is an expression of human thought and consciousness, which allows the necessary interface between hardware and the user. Currently, commercial-off-the-shelf software constitutes over 90% of the information system procured by DoD [IW Defense, 2000]. Millions of lines of codes currently represent one program or application

and one flaw in one line of code could cause failure or security vulnerability during a military operation. Algorithms, protocols, applications, detectors and databases make up only a few of the ways in which software is used. Complex communication and information systems require reliable software code. The interdependencies and interconnectedness of information systems increase the complexity of software and great precautions must be taken in the software design, testing, and engineering phases of software development. A router failure in one line of code cannot affect a robust network but if all the routers in the network were running the same software, cascading events would occur. The HHM depicts several factors (e.g., computer languages, operating systems, protocols, software attributes, and software failures) affecting software reliable, availability and trustworthiness, which are essential components for military information systems and information assurance.

E. Threats

There are groups that target military organizations and operations to convey their opposition and change national opinion. Although some of these groups use physical attacks to destroy infrastructures, others have turned their attention to cyber attacks. Distant attacks provide less exposure to adversaries; enhance their capabilities; cause more damage and use fewer adversarial resources. This asymmetric war is very attractive to adversaries [Haimen, 2001b]. Some nation-states are developing information warfare capabilities and currently practicing offensive computer network attacks. Current intelligence numbers estimate 30 or more countries with a robust information warfare capability [US GAO, 1996]. Although no country would attempt to fight conventional US military forces, targeting the US by destroying or damaging its critical infrastructures is very probable. Adversaries are likely to attack our infrastructures, specifically targeting the information infrastructure in order to achieve

four objectives: 1) assist foreign government-sponsored corporations to gain a competitive edge against US corporations, 2) damage US economic, financial, and industrial resources, and 3) affect military operations, and 4) damage to our national security.

Information assurance threats (e.g., natural and manmade threats) appear in all shapes and sizes and from many directions while representing varied impacts to an organization. It is critical to technically, culturally, and socially understand all facets about the threats that pose the greatest risk to an organization. Natural events are part of the everyday occurrences that cause a majority of the outages in telecommunications systems. Tornadoes, hurricanes, strong windstorms and water from floods and rain cause service outages to information systems and networks but are limited to geography and time. Manmade (unintentional) threats are grouped into blunders, errors and omissions. Evidence suggests that incompetent personnel, and unintentional errors cause a large fraction of system incidents, information loss and system downtime. Manmade (intentional) threats have varied approaches to destroy, degrade or manipulate a critical infrastructure. Manmade intentional threats are planned and executed by attackers or attacker groups with the willful goal of gaining access to an organization's computer systems. Deliberate unauthorized attacks on a system continue to make sense for any potential threat when: 1) the attacker benefits in some capacity from the intentional attack, and 2) the act requires very little exposure and effort in comparison to the potential gains.

Information networks continue to assist commanders, decisionmakers and warfighters gain information superiority and information dominance on this digital battlefield. The HHM captures the multi-dimensional threats affecting information superiority, and information assurance in military operations. The HHM also helps to identify consequences about protecting critical assets and information networks.

F. Architecture

The architecture HHM identifies the structure, position and connectedness of the systems storing, processing, and moving essential data in planning, directing, coordinating, and executing military operations. Mike Martin and Roland Schinzinger cited in *Ethics in Engineering* that, "Engineers should recognize that reducing risk is not an impossible task, even under financial and time constraints. All it takes in many cases is a different perspective on the design problem [Leveson, 1995]".

Information superiority and dominance necessitates designing and implementing several different architectures to meet specific decisionmaking and knowledge requirements. Military information systems must be dynamic and adjustable to assure information between systems. This assurance property represents a tradeoff with other critical properties such as system functionality and performance (Figure 12). The characteristic or function of an information system may define system 2 (Figure 12) representing a specific assurance, functionality and performance but each not at a 100% level. Although 100% assurance is currently unachievable, it is an objective within organizations.

Current architectures are interdependent, and highly complex systems that require some basic quality attributes such as reliability, robustness, survivability, mobility, and security [Ahlin, 2001 and Alberts et al., 1999]. Other attributes (e.g., unrestrictedness, controllability, attentiveness, adaptability [Dublin, 2001]) may form trade-offs with secondary attributes (i.e., light and small (transportability)). Each attribute represents different risk scenarios for the total system. For example there is often a trade-off between reliability, mobility and security. This trade-off forms the basis for risk scenarios affecting the system.

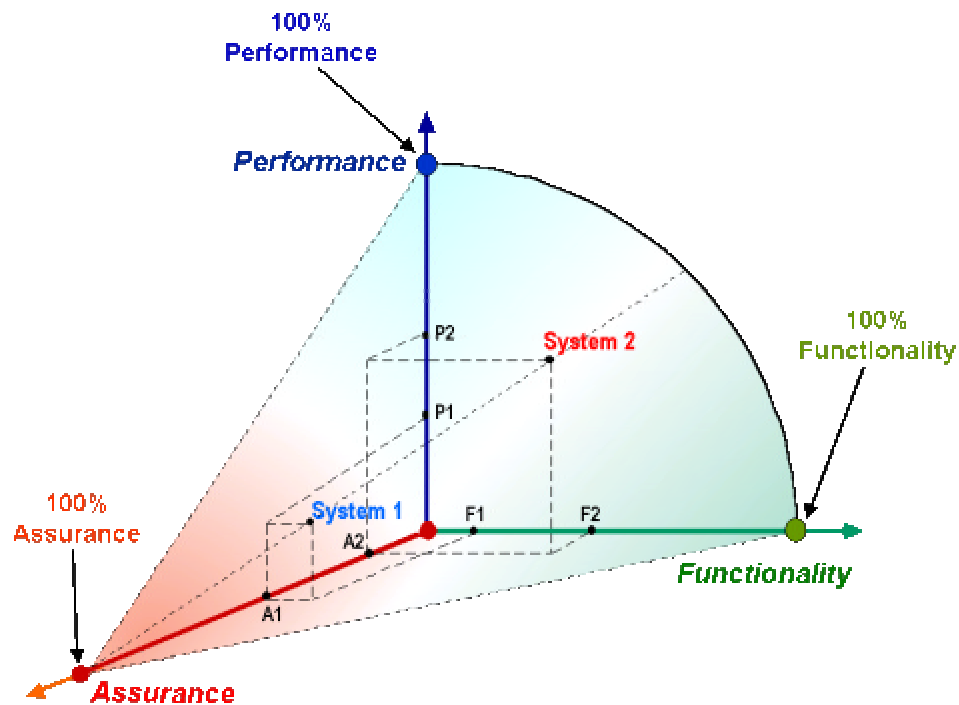


Figure 12: Information Assurance Tradeoff Analysis [Saydiari, 1999]

Other architecture attributes (i.e., speed and optimization) form two-dimensional trade-off relationships between less than optimal allocations and decisionmaking control, and optimization with centralized control [Alberts, 2001]. The military must maximize these attributes within the multidimensional-layered information networks that will link decisionmakers, and users to information as well as give them reach back capabilities via the Internet to various places (i.e., higher headquarters and home station). The HHM identifies the architecture and infrastructure attributes, and system interaction characteristics relevant to IA.

G. Information Environment

Army forces today are likely to encounter conditions of greater ambiguity and uncertainty. Doctrine must be able to accommodate this wider variety of threats. In so

doing, the Army is prepared to respond to these worldwide strategic challenges across the full range of possible operations as part of a joint and combined team [FM 100-5, 2000]. Military forces, specifically the US Army must be trained and be able to conduct military operations in any environment. These environments range from the usual tactical environments of the past to recent peace enforcement operations (e.g., Bosnia), humanitarian assistance operations (e.g., Somalia), domestic support (e.g., Hurricane Andrew) and counter operations (e.g., drug enforcement in South America and border patrol operations). Other military environments including Noncombatant Evacuation Operations (NEO) [FM 100-5, 2000], show of force operations (e.g., Desert Shield), sanctions enforcement (e.g., Iraq), and information operations (e.g., Bosnia) show the wide range of IA conditions that will exist in the future.

Decisionmakers are forced to make appropriate decisions using past information and current intelligence that is affected by spatial, temporal, spectrum and mode considerations. Temporal is usually a greatly overlooked category to most risk based systems but must be expressed in a dynamic, and complex system. Joint Vision 2020 revolves around global telecommunications using a heavy reliance on commercial assets. The environment alone constitutes a major source of failure due to the composition of complex, non-linear subsystems. It is important to understand the roles and relationships within a system's environment because the environment has interaction with even the smallest and simplest system [Leveson, 1995]. Army forces today are likely to encounter conditions of greater ambiguity and uncertainty. Doctrine must be able to accommodate this wider variety of threats. In so doing, the Army is prepared to respond to these worldwide strategic challenges across the full range of possible operations as part of a joint and combined team [FM 100-5, 2000]. Military forces, specifically the US Army must be trained and be able to conduct military

operations in any environment representing different risks to the organization, its objectives and its personnel.

The HHM captures information environmental factors including environmental and system interaction principles relevant to information systems. Successful execution of new technologies by designers, implementers and maintainers is a result of having strong infrastructure principles and understanding coupling interactions. The potential risks of a system are associated with their system interaction (i.e., complex or linear) and coupling attribute (i.e., tight or loose) [Perrow, 1995].

H. Information Operations

Former Secretary of Defense William S. Cohen stated “The Army's ability to use information to dominate future battles will give the United States a new key to victory, I believe, for years, if not for generations to come [Shanahan, 2000]. Information operations (IO) [Shanahan, 2000] integrate all aspects of information to support and enhance the elements of combat power, with the goal of dominating the battlespace at the right time, at the right place, and with the right weapons or resources [FM 100-6, 2000]. Information operations is defined as “continuous military operations within the military information environment that enables, enhances, and protects the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations; IO includes interacting with the Global Information Environment (GIE) and exploiting or denying an adversary's information and decision capabilities [FM 100-6, 2000].

Effective C4ISR systems are a critical element in the success of all military operations. The overall systems of a C4ISR information network is composed of several individual networks integrated to provide military service and support to all US military

units, multinational military forces (i.e., British and French coalition forces), and possibly local or world humanitarian organizations (e.g., Red Cross).

These systems provide situational awareness for integration and coordination of joint element maneuvers and sensor-to-shooter connectivity for weapons employment. The networks that support C4ISR must be integrated, operable, highly trustworthy and reliable. The Army Command and Control areas are the key components of a successful military operation and IA operation. Real-time, accurate, and reliable information requires parallel and mutually supported network to carry critical information to commanders (decisionmakers) and soldiers in order to execute decisive operations. The networks are communications systems comprised of the voice, data, and video spectrums connected to the Internet using leased lines and commercial systems. The synergy of the spectrums depends on the size of the operation, types of units deployed, environment and communication support required.

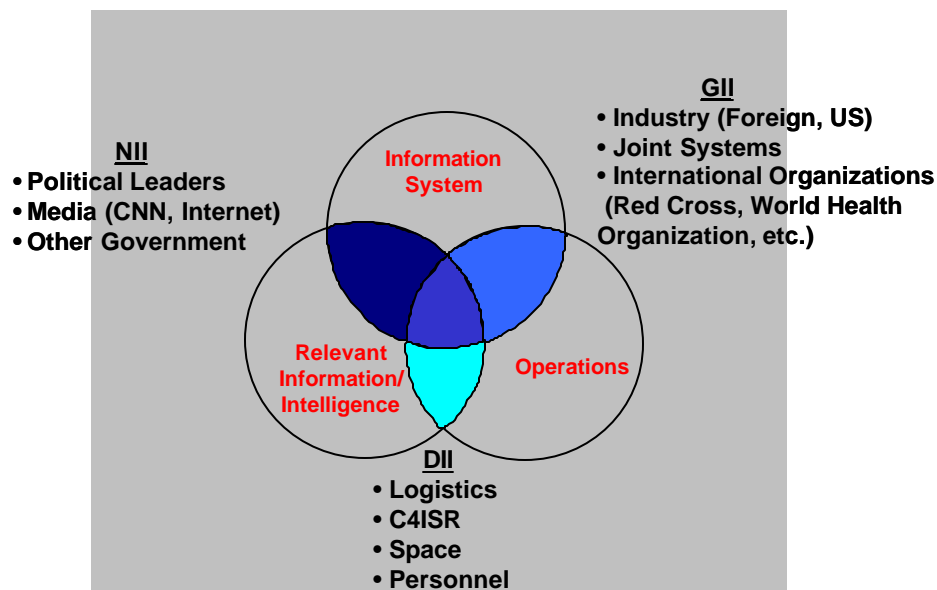


Figure 13: Information Operations Element State Space [FM 100-6, 2000]

Information operations (Figure 13) depend on a range of assorted activities in support of military operations on the battlefield. The activities include: 1) acquiring information on the enemy or threats, 2) denying critical information to the enemy or threat, 3) using information to gain a decisive edge in current and future operations, 4) exploiting gained enemy or threat information to disrupt the enemy decision making cycle and operations, and 5) protect and manage critical information to allow our forces to make accurate real-time decision, and delay and interrupt their decision making ability. [FM 100-5, 2000] The HHM depicts an assorted array of command and control areas representing possible areas of failure, and attack across a wide-range of operations.

I. Knowledge Management

This HHM head-topic identifies knowledge management as the core component of effective information superiority. With the plethora of information systems currently being tested within the military, the commander inherently faces information overload. Knowledge management sometimes called dominant battlespace management or situational awareness encompasses all facets of managing information and its environment. It has the ability to filter the information based on current and future assessments. As used here, knowledge means a dynamic mix of information in context, experience, insight, and values. It encompasses understanding information and its relevance through inputs, and known relationships. It is important to derive knowledge from information to minimize risks, and minimize uncertainty. The definition accepted by the NSA for *knowledge management* is “strategies and processes to create, identify, capture, organize, and leverage vital skills, information, and knowledge to enable people to best accomplish the organizations missions [Joint Military Intelligence College Foundation, 2000]”. By this definition, the emphasis is on people where the knowledge

resides. People within organizations will ultimately make the difference in IA and JV2020.

Knowledge management addresses the processes, and behavioral norms and practices that are key to knowledge creation and use in any organization [Joint Military Intelligence College Foundation, 2000]. Knowledge management and IA have similar foundations. The HHM captures various management aspects, i.e., security, intrusion, encryption-key, and IA aspect relevant to knowledge management.

J. Models and Methodologies

This HHM head-topic identifies the risks associated with IA methods and functions. “To manage risk, one must measure it” constitutes the scope for risk management. Models and methodologies are the road maps that guide the organization throughout the journey of risk assessment. [Haimes, 1998] Risk is commonly defined as a measure of the probability and severity of adverse effects [Lowrance, 1976].

There are risks associated with modeling and implementing the wrong technology, tactic, technique, or procedure. Methodologies and procedures are roadmaps and frameworks that allow for continuous improvement in dynamic systems. A roadmap establishes a focal point, identifies certain random and exogenous variables, develops possible prevention processes and technologies, employs reaction procedures, and formally iterates the process using certain techniques.

Processes are sequential steps that begin and end with events, and have applications such as planning, system and process design, and continuous improvement. Processes focus organizational efforts and resources in order to solve the problem. Tools are those resources used in support of execution of process steps.

Metrics equate to standard measures used to record events. Metrics are then used to compare events, both current and past measurements, and make decisions

based on those measurements. The success of information assurance methodologies relies on mitigating risks within the processes, tools and metric implementation. The subtopics listed in the HHM build a foundation to accurately assess risks across the models and methodologies head-topic.

Chapter 6 Information Assurance Metrics

Werner Karl Heisenberg (1901-1976) cited in *Physics and Philosophy*, “Since the measuring device has been constructed by the observer...we have to remember that what we observe is not nature itself, but nature exposed to our method of questioning.” [Berard, 2000]

6.1 Introduction

One objective of this thesis is to determine and develop a set of appropriate Information Assurance Metrics (e.g., measures of effectiveness, risk, cost, etc.) to determine and measure the usefulness of the risk scenario mitigation policies generated from model and methodology, or compare information assurance systems (e.g., cryptographic system A is more reliable than cryptographic system B). The topic of IA metrics is not the core subject of the thesis and is itself its own research topic.

The problem in developing IA metrics is the violation of the Heisenberg Uncertainty Principle, which states that it is physically impossible to measure both the exact position and exact momentum of a particle at the same time. In IA terms, it relates to simultaneously measuring the risks to the system, and the efficacy of deploying risk assessment and management on the system when no protective actions are taken and the system has fundamentally changed [Longstaff et al., 2000]. Information assurance metrics have a crucial operational impact on many organizations to include improving situational awareness and intelligence about the costs, risks, benefits and security about IA initiatives. In order to generate appropriate IA metrics, this chapter is arranged as a taxonomy for metric development. The results of this chapter are to: 1) present an IA metric taxonomy, 2) add value and context to IA metrics, and 3) provide a well-researched list of metrics that organizations can apply to risk scenarios to gauge the

usefulness of current and future policies. Information assurance metrics should have the following qualities [Skroch, 1999]:

1. Computable within a time frame that is useful to decisionmakers and cost to obtain the metrics must be considered.
2. Makes intuitive sense and is easily understood.
3. Has consistency across systems and can be repeated.
4. Measures what you think it measures. Metrics are comprehensive, relevant, easy to use and measure what their intent.
5. The scale (bounds on the metric) is meaningful to the user and the decision maker.
6. Quantifiable metrics should have precision within its significant digits and its uncertainty has a known source.
7. Metrics have value to an organization in order to meet goals of the system (e.g., design, operation).
8. Information assurance metrics are needed to reduce, transfer, eliminate or accept the effect of risk.

6.2 Metrics Overview

Prudent management of any entity calls for making cost effective decisions about resource investment [Longstaff et al., 2000]. Information assurance risk assessment and management must have metrics that evaluates the efficacy of risks within each system. Metric identification, and evaluation has proven difficult but it is extremely valuable and must not be abandoned.

Metrics are stand alone measurements chosen to specify and record a situation, compare it to similar past measure, and make decisions through figures of merit [Skroch, 1999]. Metrics for IA must have special qualities, which quantify the costs, risks and benefits of any action as well as represent the level of trust or credibility of the system. Metrics must have a common language and understanding between the hierarchies of people associated with the systems (e.g., designers, operators, maintainers). Metrics

are related to the concept of benchmarks, which provide insight that humans can readily understand and utilize [Skroch, 1999].

Security metrics attempt to assess the degree to which a system can provide some security related property (i.e., system security against a given set of attacks). Many literary documents and papers from academia and industry relate IA metrics to security. The “Development of a Science-Based Approach for Information Assurance” [Skroch, 1999] and “Challenge: Assurance Metrics” [Koob, 2000] relate IA metrics to security attacks. For example, a security metric for “insiders” may answer: 1) how to differentiate an insider threat from a non-threat within an organization or 2) what is the organization's performance in reference to “insiders.”

Information assurance metrics are much broader and relate to system trust and credibility. Information assurance metrics answer a different set of questions, which are related to trust and credibility such as:

1. How quickly does the organization return trust to the systems and its users?
2. What policies or education is the organization providing to ensure that there is increased awareness for “insiders”?
3. Is it difficult for an un-trusted source to access the organization's trusted sources?

They should support the objective of improving, renewing and stabilizing the trust between user and system or information within an information infrastructure. Information assurance metrics are useful in allowing a system designer to evaluate design trade-offs for assurance and other design factors [Koob, 2000]. It can also serve to determine if a system design criterion meets the specified requirements. It may be necessary to develop metrics for different parts of a system or component's lifecycle. “If you do not know where you are, any direction will do [Koob, 2000].” Metrics will tell us our location and direction and serve as a navigation system for future IA problems.

6.3 Metric Assignments

Metrics have value when we assign the units and context within a specific measurement scenario. Measurement is the assignment of numbers to a system, process or event that attempts to represent or preserve observed relations [Roberts, 1979]. In order to assign measurements to a process, two fundamental issues must be addressed: representation and uniqueness [Roberts, 1979]. These issues are illustrated in Figure 14, which describes three IA metrics characteristics: type of measurement, metric category, and metric scale.

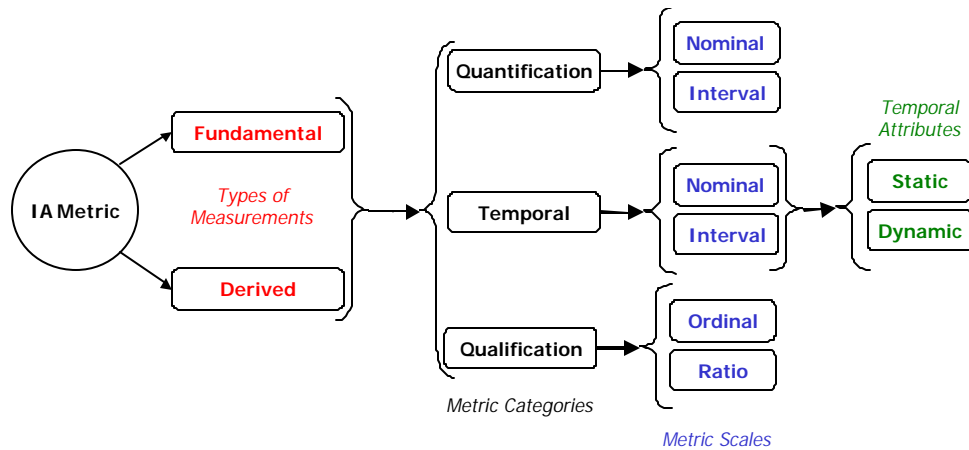


Figure 14: Metric Characteristics

6.3.1 Types of Measurement

The measurement type defines when the measurements are taken. Fundamental measurements are taken at the initial stages of system operation or design while derived measurements are taken during the duration of system operations, and are defined in terms of previously taken measurements [Dombroski, 2001].

6.3.2 *Metric Categories*

Metrics are expressed within three fundamental categories: quantity, quality, and time [Cramer, 1997]. For this thesis, the terms “Quantification”, “Qualification”, and “Temporal” are used to denote the IA metric categories. Temporal metrics or time-based metrics have an additional representation. Temporal metrics are taken at a specific time t (e.g., beginning of an operation) or constantly measured throughout the lifetime of an IA process or system. The first scenario describes a static measurement and the later describes a dynamic measurement.

Quantitative and temporal metrics can be used in automated tools (e.g., simulation and analytic software) verses qualitative metrics. Quantitative and temporal metrics are science-based measurements that have mathematical relationships to other metrics. Qualitative metrics are categorical measurements that are not represented by numbers *per se*. Qualitative metrics need a common reference, language, and understanding. All IA metrics should allow the user to correlate and extract information, and apply benchmarks to metrics.

6.3.3 *Metric Scales*

The difficulty in developing metrics and measurement scales is the preservation of relations [Dombroski, 2001] and the accuracy and value of those relationships. A relation is a comparison of two or more entities or properties pertaining to a system. Chankong and Haimes [1983] describe in detail relational properties and system comparisons.

Scales are important because they provide uniqueness, and meaningfulness [Dombroski, 2001]. There are many types of measurement scales (e.g., absolute, multidimensional) but this thesis addresses four scale types when identifying IA metrics such as Nominal, Interval, Ordinal and Ratio. Each scale represents different functions

and meaningfulness. The highest form of measurement equating to the most useful is ratio scales followed by interval, ordinal and nominal scales, respectively. The stronger the scale type, the more arithmetic operations can be performed on the data without losing information or meaning.

Measurement scales form a relationship between characteristics of entities (e.g., risk scenarios) we want to measure and a corresponding number system. Each measurement involves a mapping of one relational system to another in order to preserve the correct context. For example, specifying a system is twice as available as another is meaningless without the scale. A scale is meaningful if and only if its truth (or falsity) remains unchanged under all admissible transformations of all scales developed [Roberts, 1979].

Ratio scales have a “natural zero,” preserves ordering, and multiplying the scale by a positive constant changes the measurement units. It is sometimes useful to represent a system by comparing two or more systems. System A is more reliable than System B. Length is an example of a ratio scale because a length of zero corresponds to no length and conversion from one unit of length to another (e.g., miles to kilometers) involves multiplying by a positive constant.

Interval scales lack an “absolute zero” while preserving order and difference but are not ratios. Their scales can be defined equal interval along the scale. Interval scales capture information about the size of the jump from one class to another [Fenton, 1996]. The transition between Fahrenheit and Celsius scales is an interval scale because no zero point is varied for each scale. Addition and subtraction are acceptable operators on interval scales but not multiplication and division [Fenton, 1996].

Ordinal scales have objects that can be ranked and ordered. The ordinal scales represent information about an ordering of classes or categories, and defines a monotone increasing transformation function. The numbers represent ranking only and

applying arithmetic operations (e.g., addition and subtraction) has no meaning [Fenton, 1996].

Nominal scales have categorical distinctions but no distinct counting order. Any distinct numbering or symbolic representation of the classes is an acceptable measure, but there is no notion of magnitude associated with the numbers or symbols [Fenton, 1996]. With nominal scales, no judgment is inferred about the severity of the measurement.

6.4 Metric Taxonomy Development

“What is not measurable make measurable,” sited by Galileo [Fenton1996]?”

6.4.1 Objective Oriented Metrics

Before developing the metric taxonomy, we first introduce a concept of objective oriented metrics. Utility is in the eye of beholder [Fenton, 1997] and a particular metric is only useful if it helps the user recognize system or process improvement. Goal-Question-Metric Method (GQM) [Fenton, 1997] is an effective approach in developing metrics for specific goals within an organization. The question portion of GQM refers to the accomplishment of the sub-objectives in order to determine if the top goal is met. The metrics address the question, “what is being measured?” The method is similar to value hierarchy structure development and is used extensively by AT&T [Fenton, 1997]. GQM fails at developing metric scales, objectivity or feasibility. The metric taxonomy presented in this thesis addresses the above failures of GQM and uses objectives instead of goals.

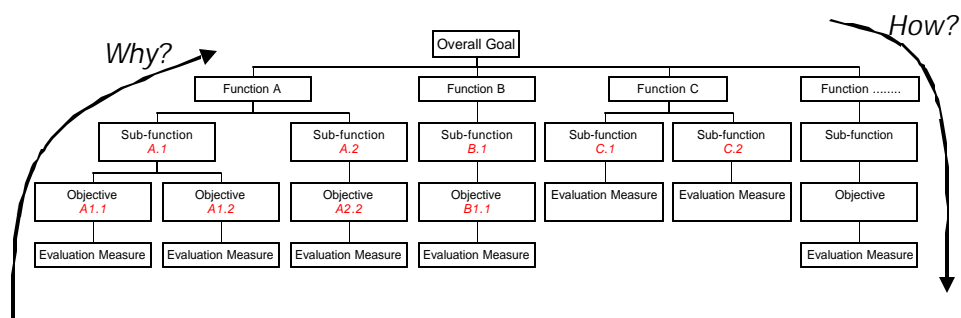


Figure 15: Generic Objective Value Hierarchy Structure [Willis, 2000]

A value hierarchy structure (Figure 15) is developed to add value and meaning to IA metrics. The top of the structure represents the top-level objective (goal) and the next layer represents major critical functions. If possible there is further development of the structure into sub-functions and the lowest level objectives require an evaluation measure or metric. The value hierarchy structure or goals tree as it is referred to quite often, asks the question, “why” ascending the tree and “how” descending the tree.

6.4.2 Metric Taxonomy

There is a major concern within all organizations on how to develop appropriate metrics to evaluate IA policies and manage critical resources. In order to generate IA metrics, Skroch [1999] believes that the following questions must be answered comprehensively and systematically.

- What do you want to measure?
- How are the metrics manifested?
- How do you measure them?
- How can you use them?

With these questions, the use of the Hierarchy Structure Method (presented earlier in this chapter) and literary research, a metric taxonomy was designed and is addressed in this section. Information assurance metrics characterize the “trust” and

“credibility” to that filtered subtopic alone. Steps one through five allow organizations to determine the best set of useful and meaningful IA metrics for a specific set of risk scenarios by selecting the appropriate organizational objectives. The metric taxonomy (Figure 16, Page 68) allows for an input (a measurement requirement) and output (evaluate the trust and credibility of the system) functions to determine the overall effectiveness of the desired IA system. In general, metrics answer questions about effectiveness, risk, system capability, classification and number, and assist decisionmakers in selecting an appropriate policy and managing a policy or system through its lifecycle.

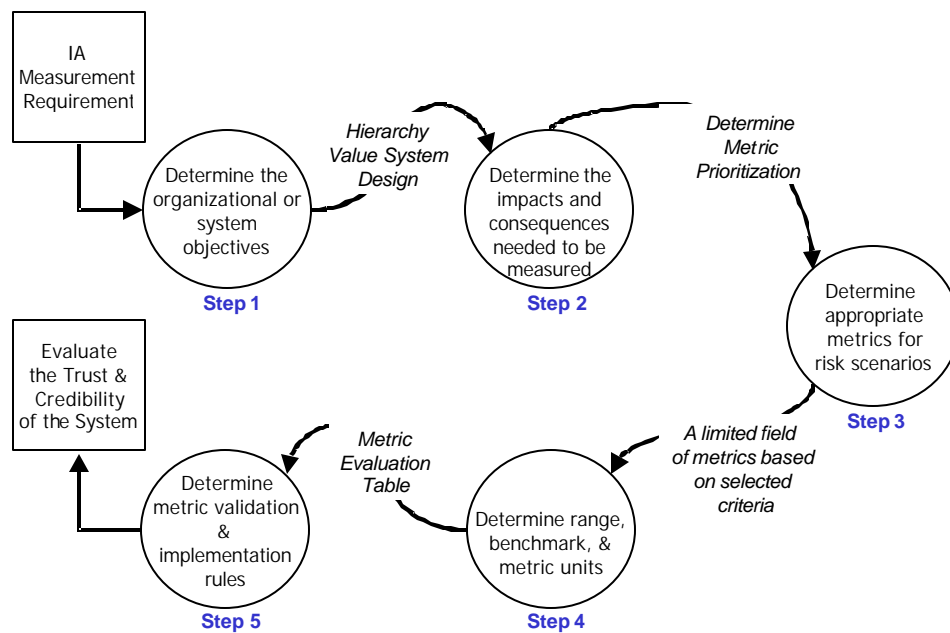


Figure 16: Information Assurance Metric Generation Framework

In Figure 16, each circle represents a step with the taxonomy and each is described in the following sections. The expressions between the circles (e.g., Metric Evaluation Table) represent the results after the previous step is completed. Chapter 7

illustrates the IA metric taxonomy in the context of the methodology and the scenario-based example.

6.4.2.1 Step 1 (Determine the Organizational or Systems Objectives)

The initial step in the metric taxonomy is to determine the overall needs for measuring the system by developing an objective value hierarchy structure. This includes formulating a definition for each objective and defining appropriate sub-objectives. This section addresses the major objectives associated with IA metrics in order to develop a common language and environment. Through literary research and expert evidence, 19 information assurance objectives are listed in Table 4 (Page 71). The list corresponds to objectives that are highly coupled with “trustworthiness” and “credibility.” The list is not inclusive and organizations may want to define, use and measure others in the context of the taxonomy. The justification for using 19 objectives is:

1. The objectives represent the main effort in defining and measuring the efficacy of an IA system, and
2. The metrics are ultimately related to trust through relationships, comparisons and values.

Several iterations were used to build the value hierarchy structure in Figure 17 (Page 72). In the figure *trustworthy* and *credibility* systems are the overall goal an IA environment and represent the top-level objective. Each objective or sub-objective is represented by several IA metrics useful in adding value to an organization’s operations and policy selections. The top-level objectives (i.e., Risk (A.1), Availability (B.1), Cost (C.1), and Survivability (D.1)) have several sub-objectives beneath them, which are used to further define the organization’s critical objectives. It may be necessary to prune or rearrange Figure 17 into a structure that meets organizational needs and desires Figure

18, Page 72). Sub-objectives are not always necessary but metrics are identified, defined and mapped for the lowest level objectives, e.g., in Figure 17, the objective uncertainty (A.1.1) has metrics but risk itself would not. It also may be easier to define organizational objectives with only six objectives and no sub-objectives. Reading the figure from top to bottom helps to answer the question “how is the objective being measured,” and reading the figure from bottom to top helps to answer the question “why are we measuring the objective.”

Defined Objective	Meaning
<i>Availability</i>	The Assurance that information and services are there for the user when required [Cramer, 1997]. The probability that a system performs a specified function under given condition at a prescribed time [McCormick, 1981].
<i>Cost</i>	Typically, the amount of dollars, manpower or time used for a specific service, process or system and the assurances for those entities. Within the IA spectrum, cost can be measured in: 1) effort of design, implementation, maintenance, and operations of a product or service, and 2) value of information lost or gained.
<i>Expected Damage</i>	The average damage expressed in cost, manpower or resources given by the combination of hazard and vulnerability.
<i>Extreme Events</i>	An event or events with a low probability of occurrence and a high impact to an organization or project.
<i>Information Loss</i>	The decrease in amount, magnitude, or degree of information between two systems or users.
<i>Integrity</i>	The assurance that information and systems are not altered or corrupted [Cramer, 1997].
<i>Maintainability</i>	The ability to undergo repairs and modifications during normal and adverse operations [Randell, 1992].
<i>Operability</i>	A process is operable if the available set of inputs is capable of satisfying desired steady-state and dynamic performance requirements defined at the design stage, in presence of anticipated set of disturbances, without violating any process, equipment, or machinery constraints [Vinson, 1996].
<i>Redundancy</i>	Redundancy refers to the ability of extra components of a system to assume the functions after failure [Haimes, 2001c].
<i>Reliability</i>	Continuity of correct service; failure free operation in a specified environment [Storey, 1996]. The probability that a specified fault event has not occurred in a system for a given period of time t and under specified operating conditions [McCormick, 1981].
<i>Return on Investment (ROI)</i> [Putnam, 1992]	The practice of recapturing funds advanced to improve process productivity over the period funds are in use for this purpose [Putnam, 1992].
<i>Risk</i>	A measure of the probability and severity of adverse effects [Lowrance, 1976]
<i>Security</i>	Measures taken to decrease the likelihood and impacts of threats to information system, which include: attacks, failures, and accidents.
<i>Situational Awareness</i>	The ability to identify, process, and comprehend the critical elements of information about what is happening to the team with regards to the mission.
<i>Surety</i>	Surety is defined as the measure of the acceptable system performance under an unusual loading [Ezell, 1998].
<i>Survivability</i>	The capability of a system to achieve its mission objectives in a timely manner in the face of accidents, failures, and attacks [Longstaff and Haimes, 1999]
<i>Uncertainty</i>	The lack of knowledge or sureness about the probabilities, and consequences of the risks inherent to the system.

Table 4: IA Metric Value Hierarchy Objective Characteristics

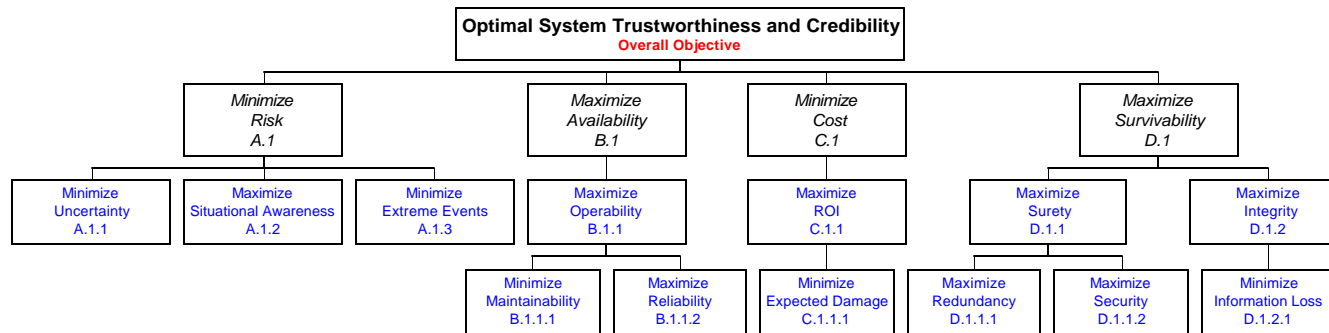


Figure 17: Information Assurance Metric Value Hierarchy Structure (Example 1: Overall)

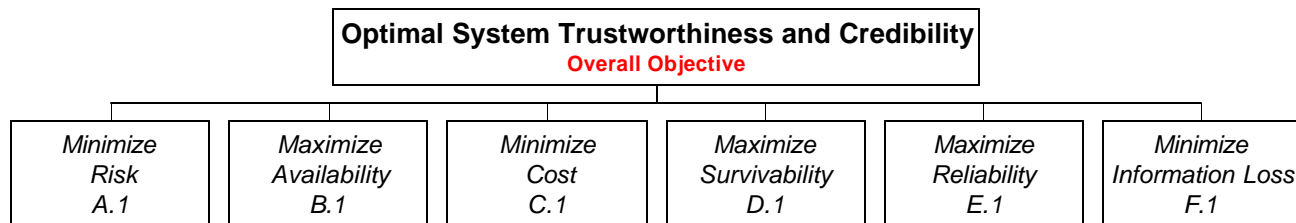


Figure 18: Information Assurance Metric Value Hierarchy Structure (Example 2: Condensed)

6.4.2.2 Step 2 (Determine Impacts and Consequences needed to be Measured)

The second step is to determine the impacts and consequences needed measuring within the system. This second step asks, “what do you want to measure (e.g., loss of life, mission failure, loss of trust),” and “how are these impacts represented (e.g., loss of capability, modification of information, diminished operations [Skroch, 1999])?” Another way of looking at this step is to ask, “what happens if we do not measure the organizational top-level objectives (e.g., maximize availability or minimize risk)?” Answering these questions helps the organization understand the impacts and consequences of measuring the filtered risk scenarios.

6.4.2.3 Step 3 (Determine the Appropriate Metrics)

In the third step, the analyst determines the appropriate metrics, their utility, type and function within the system. This third step asks, “how do you measure a specific risk scenario (e.g., virus, insider, weather) in the context of the organization’s objectives?” The concept to be measured must be clearly defined by mathematical or empirical relational sets [Jacquet, 1997]. Each bottom level objective in the value hierarchy structure is mapped to specific metrics that is used to measure that objective (e.g., survivability or risk).

6.4.2.4 Step 4 (Determine Range, Benchmark, and Metric Units)

In the fourth step, the analyst determines any benchmarks, ranges, and measurement unit for each metric through expert evidence or literary research and forms a metric evaluation table. A numerical assignment rule is described through descriptive text or mathematical expressions. The first type of description is used when the

measurement method is applied. The second type is required in the analysis of mathematical properties.

6.4.2.5 Step 5 (Determine Validation and Implementation Rules)

In the last step, the analyst examines validation and implementation rules for the metrics and asks, “how can you use them,” and “how are you going to get results from the metrics?”

6.5 *Information Assurance Metrics (Definitions and Representation)*

Table 36 (Appendix C) represents an alphabetical list of IA metrics, which were developed or expanded based on literary research and expert evidence. The table forms a “grab bag” of metrics that organizations can use to:

1. Measure the consequences and impacts of risk scenarios.
2. Measure the trust associated with an IA system through relationships, comparisons and values.
3. Measure the usefulness of current and future policies, and operations.
4. Measure risk assessment and management identification and mitigation policies and procedures.
5. Measure the value of a system based on quantitative or qualitative means.

6.6 *Information Assurance Metric Characteristics and Value*

The section identifies several IA metrics useful in obtaining optimal trustworthy and credible IA systems. The results of this section help individuals understand IA metrics by assigning utility and value to the metrics in order to measure specific risk scenarios. Table 37 encapsulates the metric characteristics and is illustrated in Appendix D.

Chapter 7 Description and Demonstration of the IA Methodology

7.1 Methodology Description and Introduction

The IA methodology consists of three phases: *formulation* (Steps A, B, C), *analysis* (Steps D, and E), and *interpretation* (Steps F, and G). This chapter demonstrates the efficacy of the IA methodology by integrating a detailed description of each step in the methodology within a scenario-based example. The example serves as a roadmap or “prototype” for organizations to implement the methodology in real-world IA environments. Specific steps of the methodology, i.e., Hierarchical Holographic Modeling (Chapter 5), IA Metrics (Chapter 6), Fault-tree and Fractile Distribution Analyses (Chapter 8), and IA Case Study Analysis (Chapter 9) are the core topics of the methodology and form the major contributions of this thesis. These topics are presented as separate chapters due to size and scope.

The following scenario-based example serves the purpose of providing guidelines for organizations to execute the steps in the IA methodology. It also acts as a conduit to understanding the complexity, interdependencies and interconnectedness of the issues surrounding IA, and justifies the need to execute systematic and comprehensive risk assessment and management. A US Army Division is offered as the example organization because it represents an entity that has a large personnel base; sub-units may be geographically dispersed making command and control difficult; large and diverse information infrastructures; and reliance on technology, information and personnel to maintain those critical information systems. Each organization possesses its own objectives and goals, and is subject to different organizational IA scenarios. It is important to note the key tasks within the IA methodology because they form the basis

for understanding IA problems and developing the appropriate solutions, regardless of the organizational scenario.

7.2 Information Assurance Scenario

The following scenario is a hypothetical case and illustrates one set of circumstances in which the methodology may be used. XYZ Division is on a two-week new equipment fielding and command post readiness training exercise in which only headquarter staffs are deployed to evaluate new equipment. The new equipment consists of command, control, communications, computers, intelligence, reconnaissance and surveillance system for the division. Some of these systems include *the Advanced Field Artillery Tactical Data System (AFATDS)* modernizes the Army's fire support command, control and coordination system; the *All-Source Analysis System (ASAS)* is the intelligence electronic warfare (IEW) sub-element of the Army battle command system; The *Army Data Distribution System (ADDS)* provides tactical commanders and their staffs with automated, secure, near-real time radio communications systems with data distribution capability between computers and position, location and navigation reporting of their combat elements in support of tactical operations; The *Battlefield Combat Identification System (BCIS)* provides battlefield fratricide incident minimization; The *Forward-Area Air Defense Command and Control (FAADC2) System* provides forward- area air defense weapons with target data to protect friendly aircraft and facilitate management of the air battle [AUSA, 2001]. These systems are part of the Joint Vision 2020 concept in modernizing the military to achieve full-spectrum dominance on the battlefield. The exercise hinges on reliable and available voice and data communications between units. Reliability is the key measurement for the exercise and used in modeling, fault-tree analysis and extreme event analysis. The training exercise consists of all divisional headquarters units, division staff and related higher unit

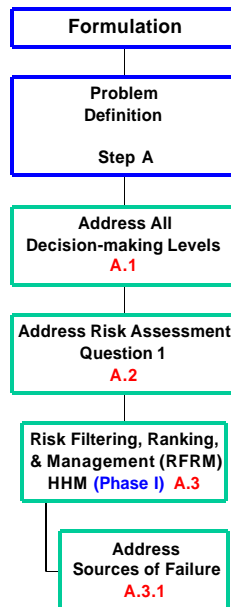
attachments (i.e., Corps Support Groups and Logistic units). One battalion headquarters from the division acted as the opposing force (OPFOR) for the exercise. The new equipment resides in all battalion, brigade and division command posts in order to improve information superiority at crucial points in the battle; suffer fewer chance encounters with the enemy; improve initiative opportunities for small mobile units; ensure reliable information systems and communications between command posts, improve commander decisionmaking capabilities; improve time and accuracy within the division's targeting capabilities; improve information sharing among high tempo and mobile units, and logistic units; reduce interference and jamming; improve information operations, time management and coordination between different staffs. In a month, the division deploys all headquarters and troops to evaluate the command, control and communication procedures between command posts and their troops. The higher headquarters (Corps) plays a bigger part by deploying additional units for the fielding exercise.

Communications for the exercise connects the division into the Internet so their higher headquarters, which is not present for this exercise, could monitor the progress of the training exercise. Leased lines from AT&T were used as the primary means to connect the two headquarters due to distance and limited divisional satellite elements. The division is testing new TTPs for a new tactical command post communications network and integration package.

The innovative package allows command posts, down to the battalion level to seamlessly and reliably share information and intelligence to successfully execute operations and missions within any environment. After the conclusion of the exercise, the division commander gathered with the division staff, division unit representatives and product vendors, and held an After Action Review (AAR) and issued these assessments:

1. The division is scheduled to deploy on another exercise in one month and during the exercise information systems between the command posts experienced diminished reliability and availability. The next exercise has an increase in unit and equipment quantity as well as higher volume of troop movement. There is a concern for the safety of the division and its soldiers and a risk assessment process should be accomplished prior to the next exercise.
2. The higher headquarters plans to offer assistance and resources to conduct the risk assessment. This includes assistance in buying software and hardware or implementing training for operators.
3. The division wants to identify the courses of action (i.e., hardware, software, training, and organizational policies) necessary to fix the IA problems seen on this past exercise. An information assurance project team is formed with key individual from different units and different staff section, which include one person from each division staff (i.e., personnel, intelligence, operations, logistics, signal), two representatives from each brigade (i.e., one officer and one non-commissioned officer), one representative from the Corps operations cell and any contractors or vendors associated with the fielding exercise.
4. A progress briefing is scheduled in two weeks to assess the risk assessment process.
5. The exercise was a partial success but the division commander feels that there are training issues for our operators and he is concerned about our connection to the Internet and the opportunity it plays for Hackers. The commander also feels that human error might have played a large part in the information assurance problems experienced during this exercise.

7.3 Step A: Problem Definition



The first step within the *Formulation* element of the IA Methodology is *Problem Definition*. This encompasses addressing all organizational decisionmaking levels, addressing risk assessment question one and using Hierarchical holographic Modeling to address all sources of risk.

The first and sometimes most difficult step in engineering design or a decision process is defining the problem. Defining scope of the problem focuses the effort toward solving the problem. One should consider the “end in mind” when developing the problem statement. This involves describing the bounds of the problem, and stakeholder objectives. If one is to attempt the

assurance of an information system, then one must study and understand the problem from a whole systems viewpoint [Craft, 1999]. If we fail to identify and understand the problem, we often expend resources in designing, implementing and managing a solution that solved the wrong problem. This step must capture the needs, wants, and desires of the decisionmakers and the goals of the organization. By the end of Step A, the analyst understands the problem and associated challenges, and understands the stakeholders’ needs and desires.

The problem definition step encompasses engineering problem statement and stakeholder analysis. The engineering problem statement is a mutual agreement between the client and analysts, which captures the problem spirit and essence. Steps A.2 and A.3 facilitate redefining the engineering problem statement and identifying any additional challenges that complicate the problem solving process.

The problem definition in this scenario-based example is how to: 1) systematically and comprehensively identify and assess the risk scenarios impacting the organization, 2) generate appropriate policies in order to mitigate or transfer those risk scenarios by applying the necessary resources, and 3) measure the effectiveness of the policies selected by the organization. The IA challenges are centered on four critical areas: modeling, complexity, system uncertainty and metrics.

- *Challenge 1 (Modeling)*: Accurately representing large-scale and complex systems while capturing the best tools and methodologies to simplify and improve these systems.
- *Challenge 2 (Complexity)*: Capturing the interconnectedness and interdependencies of information assurance in information networks.
- *Challenge 3 (System Uncertainty)*: Determining probability distributions and likelihood of information assurance events in information networks. Determining the level of completeness of the HHM and the modeling process.
- *Challenge 4 (Metrics)*: Measuring the effectiveness of a system and its components by relating the metric to trust of the system.

The stakeholder analysis identifies the needs and desires of people who directly affect the problem. Step A.1 facilitates identifying and understanding the people, and their priorities and needs within the stakeholder analysis. In order to model and understand any problem, the perspectives of different stakeholders must be documented. The relationship between goals and stakeholders is documented using a stakeholder-goal priority table [Kontio, 2000]. Table 5 (Page 81) allows a means to document the priorities for a given stakeholder but priorities between stakeholders cannot be derived (a lower number equates to a higher priority for that individual). Kontio [2000] uses goals but within this IA methodology, the term “objective” is used to denote an obtainable and achievable organizational ambition defined by some set of bounds. Interpretation across columns and in the same column within the table is not

useful because the table uses ordinal numbers and is not weighted. Table 5 represents a set of one possible stakeholder-objective priority lists. The numbers are generated to illustrate that decisionmakers and key individuals impact operations and the problem solving process in different ways. The table is extremely useful in risk analysis and management because it allows for better filtering and ranking of risks within Step B of the IA methodology.

Stakeholder Objective	Higher Headquarters Commander	Division Commander	Operations Officer	Division Signal Officer	Vendors & Contractors	Logistic & Budget Officer
A. Minimize cost to fix IA problems	9	7	9	3	3	3
B. Maximize troop safety	1	1	1	1	1	1
C. Maximize equipment safety	2	2	2	4	6	11
D. Maximize product or service timeliness	11	10	11	9	5	6
E. Maximize information superiority	4	8	4	6	10	9
F. Maximize division readiness	3	3	31	5	9	5
G. Maximize division enhancement capability	7	5	10	7	7	8
H. Minimize fielding timeline	8	9	5	8	8	7
I. Meet contract requirements	5	11	8	11	2	4
J. Balance division budget	10	6	7	10	11	2
K. Minimize IA problems	6	4	6	2	4	10

Table 5: Stakeholder-Objective Priority Table

7.3.1 Step A.1: Address All Decision Making Levels

Many real world-world decisions are made not by single individuals but by groups of individuals. Each decisionmaker characterizes and interprets the value of the objectives under consideration differently. Decisionmaking under uncertainty encompasses every fact, dimension and aspect of our lives [Haimen, 1998]. Decisions

made at one level (personal, corporate or government levels) inherently affect people at different phases (planning, operational, design, management or strategic). The goal of this step is to identify all decisionmaking levels in order to decrease the uncertainty about incomplete risk assessment. With the US Army there are three decisionmaking levels: operational (people executing planned orders), planning (people planning future operations and managing current operations), and strategic (typically Corps, and above and managing decisions at a much higher level (i.e., Pentagon and DoD). Each level has different and overlapping IA risk scenarios associated with it.

7.3.2 Step A.2: Address Risk Assessment: Question One

In order to understand risk assessment question one, it is essential to understand the building blocks of risk assessment and management, and the questions it attempts to answer. The products of Step A.2 are a description of those questions and their role in the IA methodology. Preparatory or reactive risk management actions intended to increase confidence in critical infrastructures specifically addressing information infrastructures are a thesis focus. In 1999, CSI and the FBI conducted a survey of 521 organizations and found that although 51% acknowledged financial losses, only 31% could quantify their losses, and a very small amount conducted risk assessment and risk management to mitigate their information security losses [CSI, 1999]. The risk and uncertainty inherent in all systems designed by human beings are frequently magnified by the application of large-scale technology [Haimes, 1998] such as the case with IA. What is the damage that is caused to a military operation if confidential information was lost, damaged or misinterpreted? There are many costs associated for information or system reconstitution such as additional personnel training, and lost revenues for the institution. Risk assessment and management are essential tasks to identify critical assets and potential threats; to identify and assess organizational vulnerabilities within

technology, personnel and infrastructure; to recognize the probabilities associated with the risks, and cost estimates associated with losses. Some questions usually surface when conducting risk assessment and management in safeguarding information and computer networks.

- Where does the organization begin in protecting information and equipment?
- Why should I worry about these details when I have insurance policies to cover my losses?
- How can my “small” organization deal with real threats and vulnerabilities?

Organizations asking these questions want a business case to exist before the organization commits dollars and resources to IA. Making the business case for industry to conduct IA research and risk analysis is currently the sticking point for many organizations and corporations. If it costs an organization \$200,000 to implement IA procedures, which includes the cost for conducting risk analysis and they only lose \$190,000 for doing nothing, the organization is inclined to do nothing. This is only a short-term plan that results in increased asset loss. That can be extremely risky since it rarely pays to do nothing and current estimates have organizations saving dollars, resources and information when using risk assessment, and risk management. Also, this is an investment in longer periods of potential threats and uncertainty.

A key IA issue is what resources (i.e., money, time, people, technology) should be applied to tackle inherent and future issues. Information assurance is a solvable problem with our current arsenal of resources using proactive risk management. Short-term investment in IA challenges will have enormous long-term benefits to include:

- Assuring the US military is successful in any mission on the information battlefield.
- Reducing the long-term costs of IA.

- Reducing the costs of disruptions, lost productivity and information loss in our current information infrastructure.
- Reducing fratricide on the battlefield due to increased military information technology integration; the Warfighters environment is information intense.

Risk assessment is distinguished from risk management from the questions it attempts to answer. In risk assessment, the analyst attempts to answer the following set of questions:

1. What can go wrong?
2. What is the likelihood that it would go wrong?
3. What are the consequences? [Kaplan and Garrick, 1981]

Answering these questions help identify, measure, quantify and evaluate risks and their impacts on the systems. In Steps A.2 and A.3, only question one is considered, where questions two and three are addressed in Step B of the IA methodology. In risk management, the analyst considers a second set of questions, which are answered in step D of the methodology:

1. What can be done and what options are available?
 2. What are the associated trade-offs in terms of all costs, benefits and risks?
 3. What are the impacts of current management decision on future options?
- [Haimes, 1991, 1998]

Risk assessment and risk management must be a part of the decisionmaking process and is an integral part of building the HHM. It is most effective if used during the entire planning process and introduced early. Although risk assessment and risk management are distinctly two different, there is overlap within the process. The entire risk assessment and management process contains [Haimes, 1998] five steps

(answering six questions), which are integrated within the methodology (location shown in parenthesis):

1. Risk identification (Step A)
2. Risk quantification and measurement (Step B)
3. Risk evaluation (Step B)
4. Risk acceptance and avoidance (Step D)
5. Risk management (Step D)

Risk assessment and management bridges the gap and identifies “that to be defended and that which can be defended.” Current countermeasures do not work well against future threats and vulnerabilities but proper risk assessment and management can increase assurance levels by transferring, mitigating or accepting current and future IA risks.

7.3.3 Step A.3: Hierarchical Holographic Modeling

Hierarchical Holographic Modeling effectively identifies most, if not all important and relevant sources of risk [Haimes, 1981, 1998] as discussed in Chapter 5 . This step answers the risk assessment question, “What can go wrong?” Information assurance is a complex system of components performing a myriad of functions, responding to diverse elements and is composed of hundreds, and thousands of entities. Although not all such components are on the critical path of the operability of the overall system, there is a need to identify and understand the multiple perspectives of the functionality associated with IA [Haimes, 1981, 1998]. The HHM attempts to capture the sources of risk associated with the complexity, interconnectedness and interdependency of IA.

In order for organizations to be successful in the area of identifying IA risk scenarios, two main concepts should be followed:

1. Risk identification is accomplished through structured brainstorming techniques to generate ideas [Norton et al., 1998]. It is essential to ensure many diverse people and departments come together to identify the risks (engineers, analysts, management personnel, etc.) associated with the organization and its information systems.
2. Comprehensive and systematic scenario risk identification necessitates the need for organizations to identify interlocking community circles (Figure 19). In this example, the division, a US Army major command has information system within the DII. An organizational structure and mission define many different interlocking circles, which characterize the interdependencies, interconnectedness, and complexity of the problem and the associated risk scenarios. Figure 19 illustrates two interlocking communities used to generate the total HHM and the HHM used in the scenario-based example. The two communities are not inclusive, and are limited only by the imagination of the analyst.

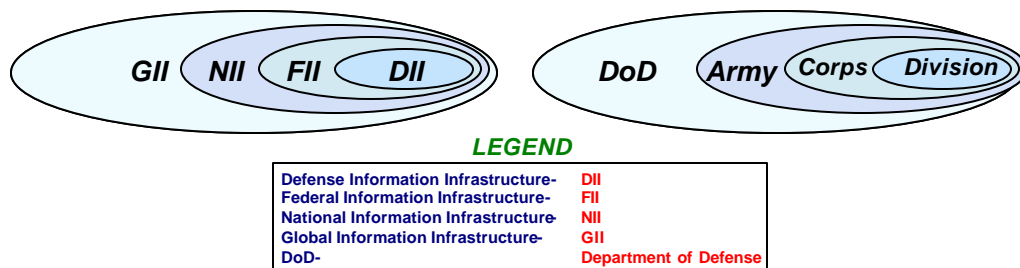


Figure 19: Information Assurance Interlocking Community Complexity

To identify all conceivable risk scenarios that the US Army might encounter within IA, a HHM was developed in Chapter 5 . With the time constraint facing the division, the division IA project team selected a reduced set of head-topics from the complete set in Appendix B. One head-topic from the 10 global topics is selected. Figure 20, Figure 21, and Figure 22 (Pages 88-90) illustrate the potential risk scenarios associated with the head-topics (Table 6). The reduced version of the selected HHM

head-topics is presented to illustrate the IA methodology within the scenario-based example. An organization that builds an HHM based on their particular scenario initial uses all generated head- and sub-topics.

Reference #	Global Topic	Head-Topic
A	Organizational	Organizational Errors
B	People (Human Factors)	Sociological Factors
C	Assets	Asset Recovery
D	Software	Software Based Errors
E	Threats	DII Threats (Who?)
F	Architecture	Computer Layers
G	Information Environment	Telecommunication Aspects
H	Information Operations (IO)	Interoperability
I	Knowledge Management	Encryption Key Management
J	Models and Methodologies	Metrics

Table 6: HHM Global and Sub-Topics Selected for the IA Methodology

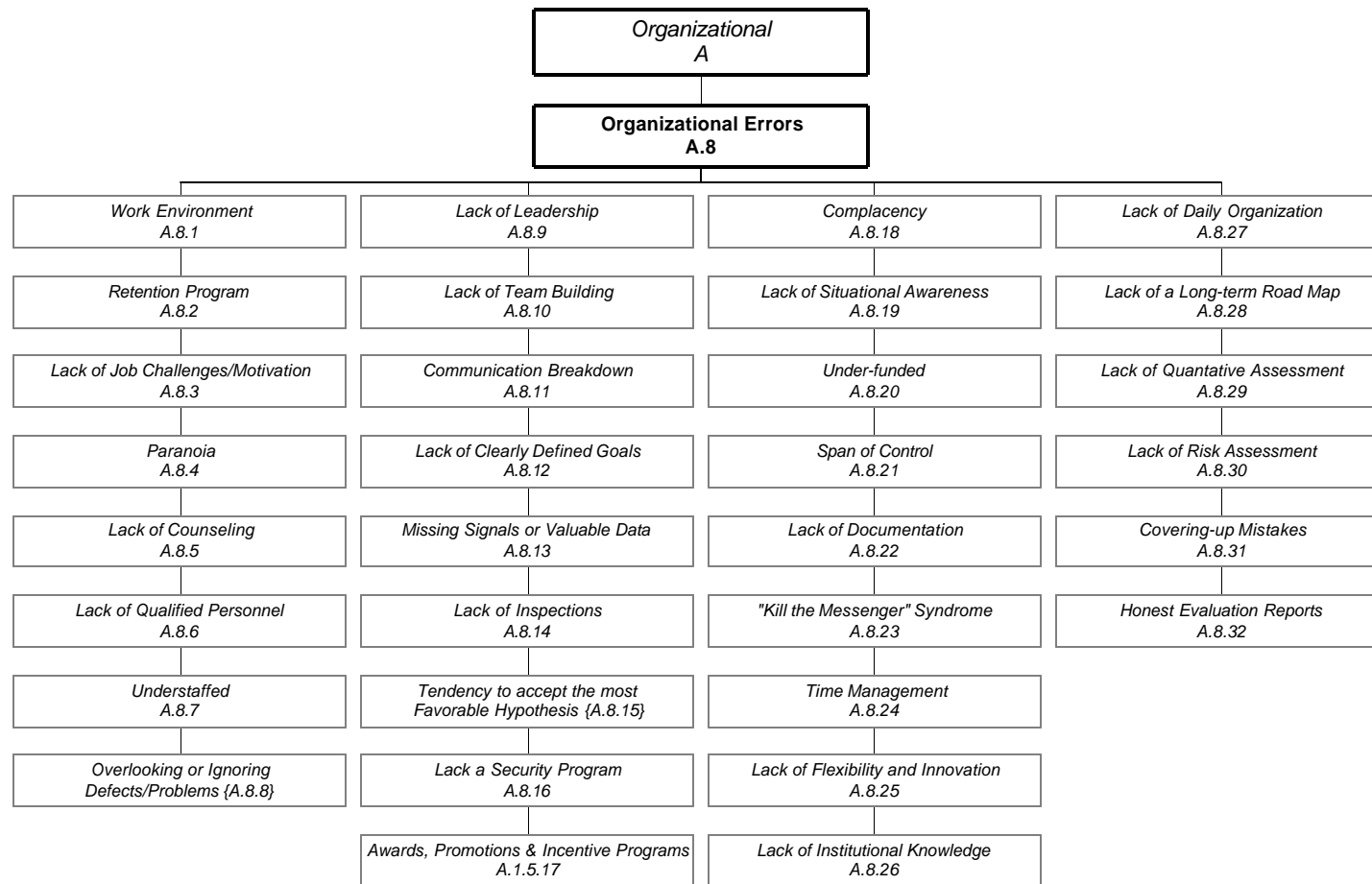


Figure 20: Partial HHM (Head-topic A.8)

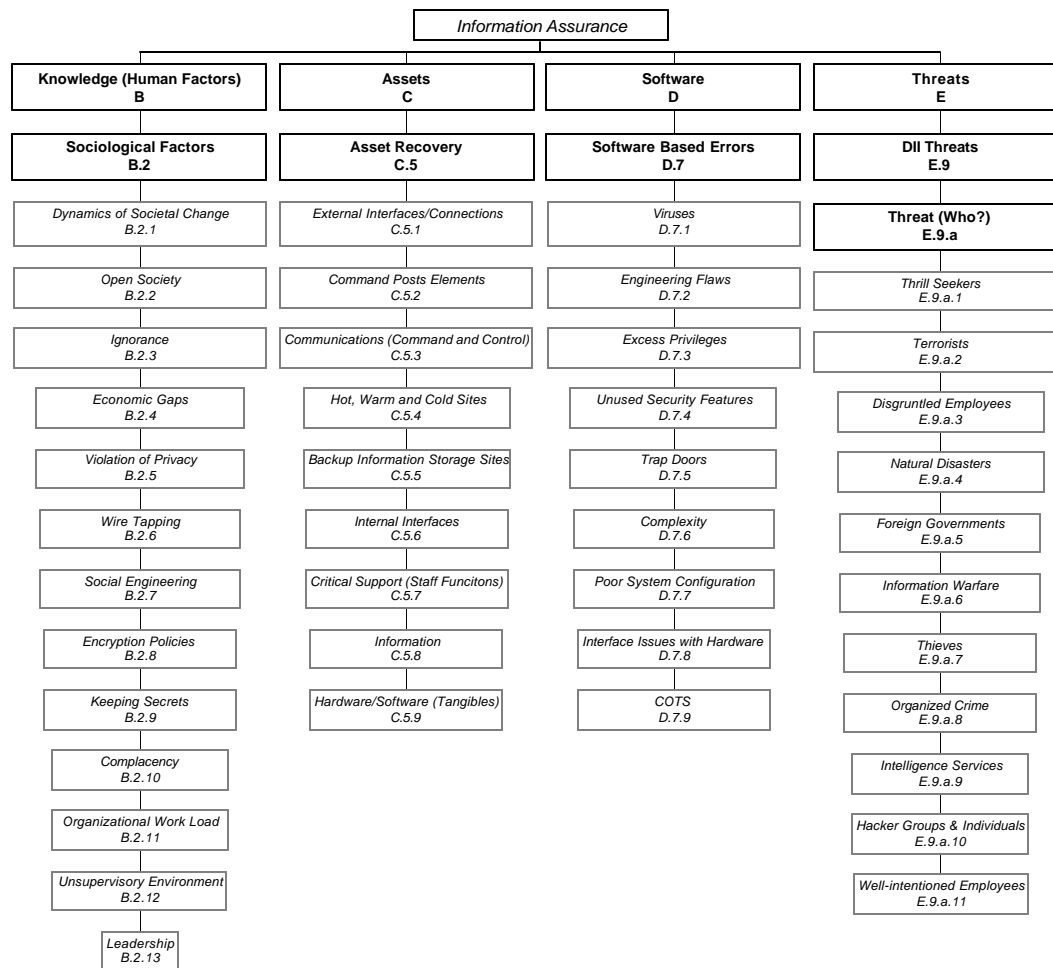


Figure 21: Partial HHM based (Head-topics B.2, C.5, D.7, and E.9)

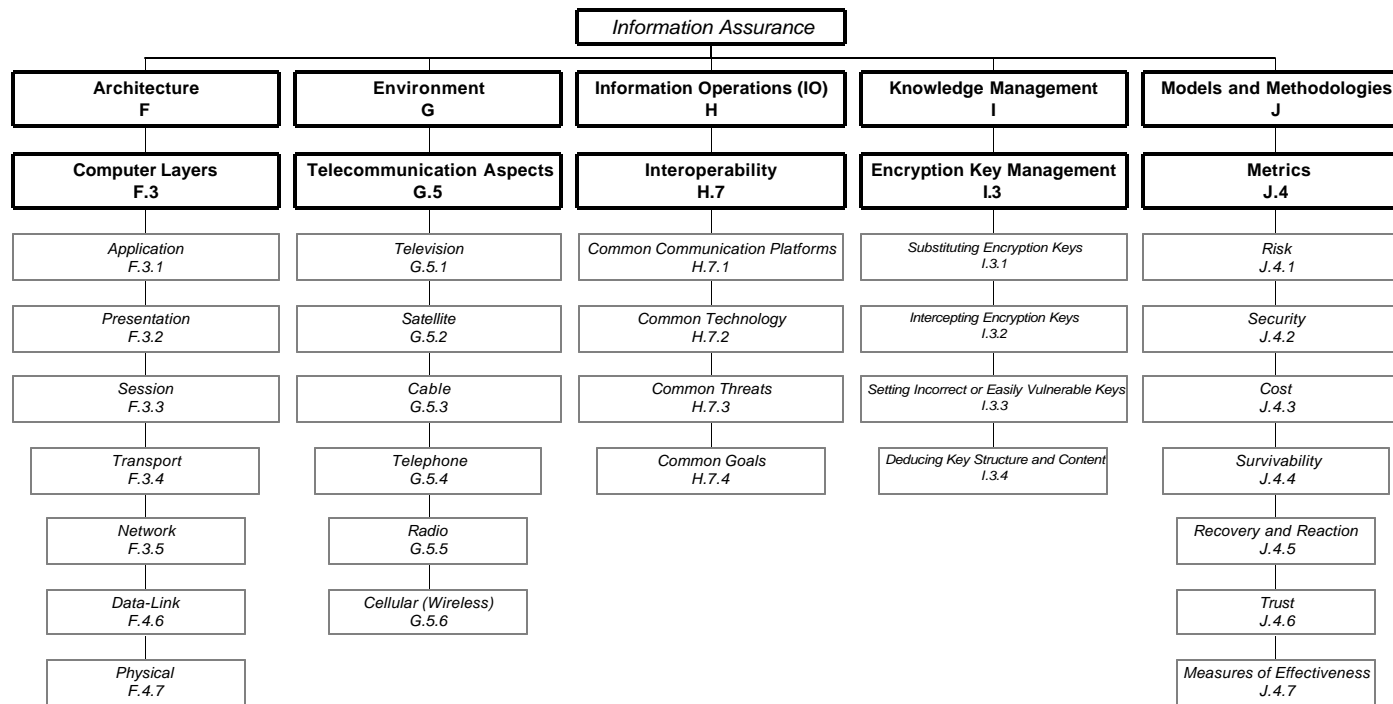


Figure 22: Partial HHM based (Head-topics F.3, G.5, H.7, I.3, and J.7)

7.3.4 Step A.3.1: Addressing Sources of Failure

Accidents are not due to lack of knowledge, but failure to use the knowledge we have as cited in Perrow [1999] by Trevor Kletz. The strategy of identifying all sources of risk revolves around several decompositions and multiple iterations. To effectively deploy the next step within the IA methodology (Risk Filtering, Ranking and Management (RFRM) [Haimes et al., 2001]), one might identify all risks and sources of failures including hardware, software, human and organizational failures (Figure 23). Addressing all possible failures characterizes the holistic risk management approach involving all aspects of the system's planning, designing, constructing, operation, and management [Haimes, 1998]. Including the four sources of failures in risk assessment and management encompasses everyone concerned – senior and junior management as well as lower levels of the organization (i.e., designers, engineers, and blue-collar workers).

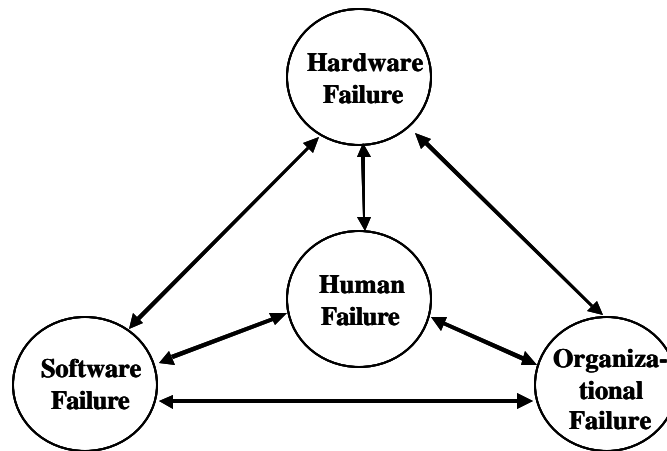


Figure 23: Sources of Failure [Haimes, 1998]

After an incident or accident, many focus on the technology aspects as a failure point but most failures of critical engineering systems are caused by organizational or

human errors. In some studies human error has accounted for 32% of computer network failures (Figure 25, Page 94) [Schweber, 1997] leading to lost information, system downtime and loss of revenue. This focus on technical solutions (hardware and software solutions) is due to the way risk and failures are analyzed in the current information age.

Each source of failure is composed of several dimensions and requires total involvement of each of these dimensions in the risk assessment and management process. The four sources of failure are not necessarily independent and affect each other based on their inter-relationships. Although, it is not always clear in defining the boundaries between hardware and software, and organization and human, the four sources provide a meaningful foundation to build total risk assessment framework.

Table 7 (Page 93) depicts some AT&T examples of failure from each of the sources, their percent of occurrence, their root cause and their interconnected cause.

SOURCES OF FAILURE	PERCENT OCCURRED ⁶	ROOT CAUSE	INTERCONNECTED CAUSE
Hardware	19%	Hardware reconfiguration and redundancy, and recovery procedures	Organizational errors while reconfiguration or recovery procedures are executed. Software errors appear during recovery mode.
Software	14%	Errors in one line of switching code	Software code glitch reacting to a human input
Organizational	49% ⁷	Poor operator equipment maintenance. Lack of leadership and spot-checking.	Human error, mainly complacency, causes hardware and software errors and decreases communication reliability and availability.
Human		Configuration changes, and patch installations of voice and data switches	Errors in software upgrade and changes following software maintenance procedures

Table 7: Sources of Failure in the Public Switched Telephone Network

[Kuhn, 1997]

Figure 24 and Figure 25 (Page 94) represent two pie charts from two different sources depicting the impacts of sources of failure on a system. The figures illustrate the high impact (55% and 32%, respectively) on information and information networks by human error. The figures depict viruses (4% and 7%, respectively) as a minor but consistent risk within information networks. The figures also represent a need to understand the connectedness and interdependent natures of all sources of risk and their impact on information networks.

⁶ Vandalism accounts for 1%; Overloads in this context are considered a hardware and organizational source of failure, and accounts for 6% but is not represented in Table 7; and Acts of nature account for 11%.

⁷ Human and Organizational sources of failure jointly account for 49% together and Kuhn [1997] does not distinguish between the two sources.

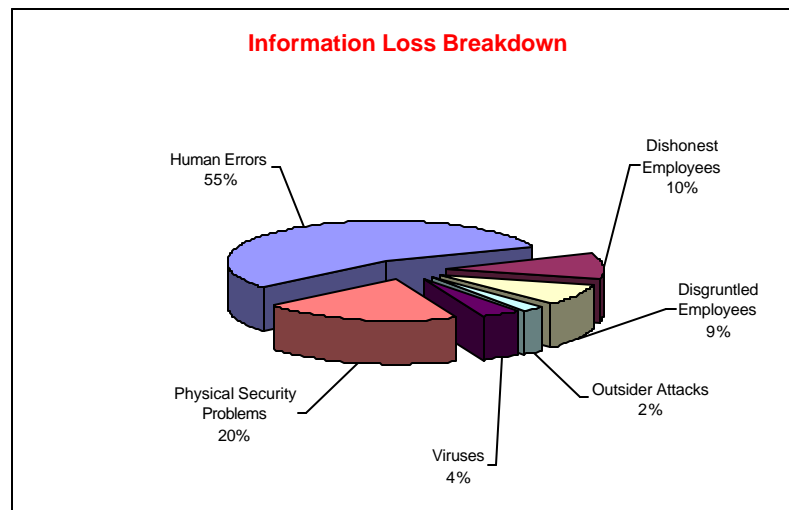


Figure 24: Information Loss Breakdown (Crime/Loss Breakdown)

[Icove et al., 1995]

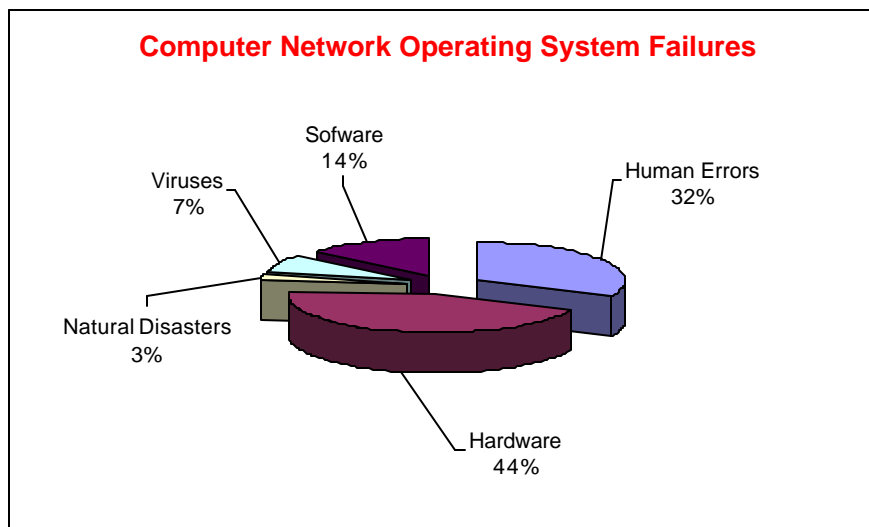
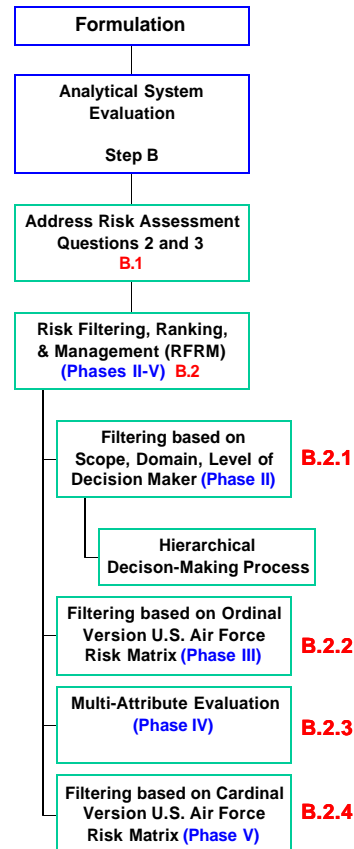


Figure 25: Computer Network Operating System Failures [Schweber, 1997]

7.4 Step B: Analytical System Evaluation

7.4.1 Step B.1: Address Risk Assessment: Questions Two and Three



This step answers the risk assessment questions, “What is the likelihood and what are the consequences?” It is impractical to apply risk quantitative risk analysis to thousands of sources of risk. Eight major phases within the RFRM are used to reduce the number of entries in the HHM to provide priorities in the scenario analysis. Risk ranking and filtering is necessary when hundreds or thousands of subtopics are identified through the initial HHM process (Step A.3), which impact the total IA system. The primary purpose of this step is to reduce the HHM to a manageable level. This manageable level varies but for complex systems, the number is around 10 by the use of expert evidence (domain knowledge), common sense or quantitative data. These top 10 are

used to understand the components that have the largest impact on the total system.

Information assurance consists of several complex challenges that span across several disciplines (social science, engineering, design, management, etc.). The RFRM method is essential to focusing efforts and resources to critical sources of risks that affect specific levels of an organization. The key aspects of the RFRM method are [Haimes, 1998]:

- A quantification of risk by measurable attributes.

- A graphical risk “fingerprint” is used to distinguish among critical items.
- A telescoping filter approach to reducing the critical item list to the most critical number of sources of risk often referred to as the “top number”.
- Once the risk components are filtered to the top 50, ranking is then used to further reduce the number to 10-20.
- A “bookkeeping” method is used to track the risk scenarios throughout the methodology. Bookkeeping methods are only bound by the users imagination and there are several methods of bookkeeping within the RFRM process but only one is discussed in this thesis (i.e., table tabulation).

7.4.2 Step B.2: Risk Filtering, Ranking and Management (RFRM)

7.4.2.1 Step B.2.1: Filtering Based on Level of Decisionmaking, Organizational Scope, and Temporal Domain

The total number of head-topics and subtopics are overwhelming for IA for any decisionmaker. Not all HHM topics are of immediate and simultaneous concern to all decisionmaking levels at all times. The US Army decisionmaking levels, myriad of environments (scopes) and temporal domains were the basis for the HHM. This step reflects the judgment of decisionmaker of whether a HHM topic is incorporated for further analysis, and reduces the thousand of IA risk sources to around 50-100 for a decisionmaking level, scope and temporal domain. Table 8 (Page 97) depicts the decisionmaking levels, scope, and temporal domains. The sources of risk within the HHM are filtered based on the interests and responsibilities of the individual risk manager, risk analyst or decisionmaker. For example, a decisionmaker in the Pentagon has different needs and visions from decisionmakers in a Division or an operations section within a battalion or a civilian contractor. Each organization chooses different considerations for identifying and filtering the risks associated with their organization based on their mission, composition, and goals.

The appropriate risk filtering considerations are highlighted in Table 8, and deemed significant or of immediate concern based on the organization. The risk scenarios survive based on these considerations, which are highlighted in Table 9 (Page 98). This step narrows the amount of risk scenarios from 92 to 50. The HHM affords duplication in the risk scenario identification process in different head-topics. In this case, only one topic from the “complacency” (A.8.18 and B.2.10) and “leadership” (A.8.1 and B.2.13) sub-topics are carried over to the next step.

Decisionmaking Level	Scope	Temporal Domain
Strategic	Training	First 48 hours
Planning	Deployment	Short-term (days)
Operational	Operations in Peace-time	Intermediate-term (months)
	Operations after deployment	Long-term (years)
	Information Operations	
	Redeployment	
	Equipment Fielding	

Table 8: Step B.2.1 Risk Filtering Considerations

#	HHM Sub-Topic	#	HHM Sub-Topic	#	HHM Sub-Topic
A.8.1	Work Environment	B.2.5	Violation of Privacy	F.4.1	Application
A.8.2	Retention Program	B.2.6	Wire Tapping	F.4.2	Presentation
A.8.3	Lack of Job Challenges/Motivation	B.2.7	Social Engineering	F.4.3	Session
A.8.4	Paranoia	B.2.8	Encryption Policies	F.4.4	Transport
A.8.5	Lack of Counseling	B.2.9	Keeping Secrets	F.4.5	Network
A.8.6	Qualified Personnel	B.2.10	Complacency	F.4.6	Data-link
A.8.7	Understaffed	B.2.11	Organizational Work Load	F.4.7	Physical
A.8.1	Overlooking or Ignoring Defects/Problems	B.2.12	Un-supervisory Environment	G.5.1	Television
A.8.9	Lack of Leadership	B.2.13	Leadership	G.5.2	Satellite
A.8.10	Lack of Team Building	C.5.1	External Interfaces/Connections	G.5.3	Cable
A.8.11	Communication Breakdown	C.5.2	Command Post Elements	G.5.4	Telephone
A.8.12	Lack of Clearly Defined Goals	C.5.3	Command and Control Communications	G.5.5	Radio
A.8.13	Missing Signals or Valuable Data	C.5.4	Hot, Warm and Cold Sites	G.5.6	Cellular (Wireless)
A.8.14	Lack of Inspections	C.5.5	Backup Information Storage Sites	H.7.1	Common Communication Platforms
A.8.15	Tendency to Accept the Most Favorable	C.5.6	Internal Interfaces	H.7.2	Common Technology
A.8.16	Lack of Security Program	C.5.7	Critical Support (Staff Functions)	H.7.3	Common Threats
A.8.17	Awards, Promotions and Incentive Programs	C.5.8	Information	H.7.4	Common Goals
A.8.18	Complacency	C.5.9	Hardware/Software (Tangibles)	I.3.1	Substituting Encryption Keys
A.8.19	Lack of Situational Awareness	D.7.1	Viruses	I.3.2	Intercepting Encryption Keys
A.8.20	Under-funded	D.7.2	Engineering Flaws	I.3.3	Setting Incorrect or Easily Vulnerable Keys
A.8.21	Span of Control	D.7.3	Excess Privileges	I.3.4	Deducing Key Structure and Content
A.8.22	Lack of Documentation	D.7.4	Unused Security Features	J.4.1	Risk
A.8.23	"Kill the Messenger" Syndrome	D.7.5	Trap Doors	J.4.2	Security
A.8.24	Time Management	D.7.6	Complexity	J.4.3	Cost
A.8.25	Lack of Flexibility and Innovation	D.7.7	Poor System Configuration	J.4.4	Survivability
A.8.26	Lack of Institutional Knowledge	D.7.8	Interface Issues with Hardware	J.4.5	Recovery and Reaction
A.8.27	Lack of Daily Organization	D.7.9	COTS	J.4.6	Trust
A.8.28	Lack of Long-term Road Map	E.9.a.1	Thrill Seekers	J.4.7	Measures of Effectiveness
A.8.29	Lack of Quantitative Assessment	E.9.a.2	Terrorists		
A.8.30	Lack of Risk Assessment	E.9.a.3	Disgruntled Employees		
A.8.31	Covering-up Mistakes	E.9.a.4	Natural Disasters		
A.8.32	Honest Evaluation Reports	E.9.a.5	Foreign Governments		
B.2.1	Dynamics of Societal Change	E.9.a.6	Information Warfare		
B.2.2	Open Society	E.9.a.7	Thieves		
B.2.3	Ignorance	E.9.a.8	Organized Crime		
B.2.4	Economic Gaps	E.9.a.9	Intelligence Services		
		E.9.a.10	Hacker Groups and Individuals		
		E.9.a.11	Well-intentioned Employees		

Table 9: Initial HHM Tracking
Table

7.4.2.2 Hierarchy Decisionmaking Process

Information assurance is a large multiple-objective decisionmaking problem. The decisionmaker's decisions can affect all levels of an organization as benefits, risks, and costs, etc. Decision problems fall into two broad categories: decisionmaking under uncertainty and under risk. Organizations are hierarchical in nature and can represent vertical, horizontal, external, and geographic structures [Ashkenas, 1995]. A decisionmaker is an individual or a group of individuals who directly or indirectly influence value judgments on a list of alternatives, which affects the final outcome. Information assurance relates to trade-offs that affect a decisionmaker and their decisions. It is essential to identify, and understand the complexity of decisionmaking within IA. A US Army division is a complex and highly dynamic organization. Although decisions are not made in a vacuum or in a stovepipe, it was essential during the previous step to select those decisionmaking risk-filtering considerations (Table 8) to filter out the risk scenarios that are not immediate and detrimental risks to the organization and the decisionmakers.

7.4.2.3 Step B.2.2: Filtering and Ranking Using the Ordinal Version of the US Air Force Risk Matrix

This step unites the joint contributions of two different types of information – the likelihood of “what can go wrong,” and the associated consequences, which are estimated using expert or available evidence. In this step, one develops an ordinal matrix (Figure 26, Page 102) in order to reduce the risk scenarios to about 20. The matrix was built by the US Air Force [1988] and the McDonnell Douglas Corporation [Haimes et al., 2001c] and is a two dimensional table represented by first dividing the likelihood of a risk source into five discrete ranges (along the top) and then categorizing

the output severity into four- or five-level scales (along the side). The cells of the matrix are assigned relative levels of risk severity (i.e., low, moderate, high, extremely high). As an example, a risk scenario that occasional occurs and has an impact on “loss of mission” has a high level of severity. The impact column is flexible to meet the specific goals and missions of the organization. In some scenarios, it may be necessary to assign “loss of information”, “loss of capability after a mission” or “not achieving the set objectives of a mission” to the “A” row. The likelihood column is equally flexible by using other representations, e.g., moderate, remote, improbable, incredible, and impossible [Leveson, 1995].

The division IA project team is concerned about Extremely High- and High-risk severity levels. The team continues to filter the risk scenarios based on an assessment of the risk scenarios and determines a set threshold depicted by the stepped line in Figure 26. Figure 27 (Page 103) describes each risk severity interpretation used throughout the IA methodology. Risk scenarios falling above the stepped line survive to the next step (B.2.3) and the scenarios falling below the stepped line (i.e., low and moderate severity boxes) are filtered because they do not pass a predetermined risk threshold. The team keeps track of the filtered risk scenarios (those falling below the set threshold) to facilitate the risk management process within Steps D and E.

They depicted the risk scenarios that survive for the next step as highlighted cells within Table 10 (Page 104). The data in the table is generated to illustrate the methodology and reduces the number of risk scenarios from 50 to 21. Although the data is fictitious, organizations obtain data used in this section and throughout the methodology through expert evidence and statistical data within the organization as well as conducting simulation testing. The following notation for Table 10 is used to represent the likelihood, the likely effect and the risk severity columns. The letters U, S, O, L and F represent the likelihood column based on Figure 26 (e.g., U denotes *Unlikely*

and F denotes *Frequently*). The letters A, B, C, D, and E represent the impact column based on Figure 26 (e.g., A denotes *Loss of Life/Asset*). The letters EH, H, M and L represent the risk severity column based on Figure 27 (e.g., EH denotes *Extremely High* and L denotes *Low*).

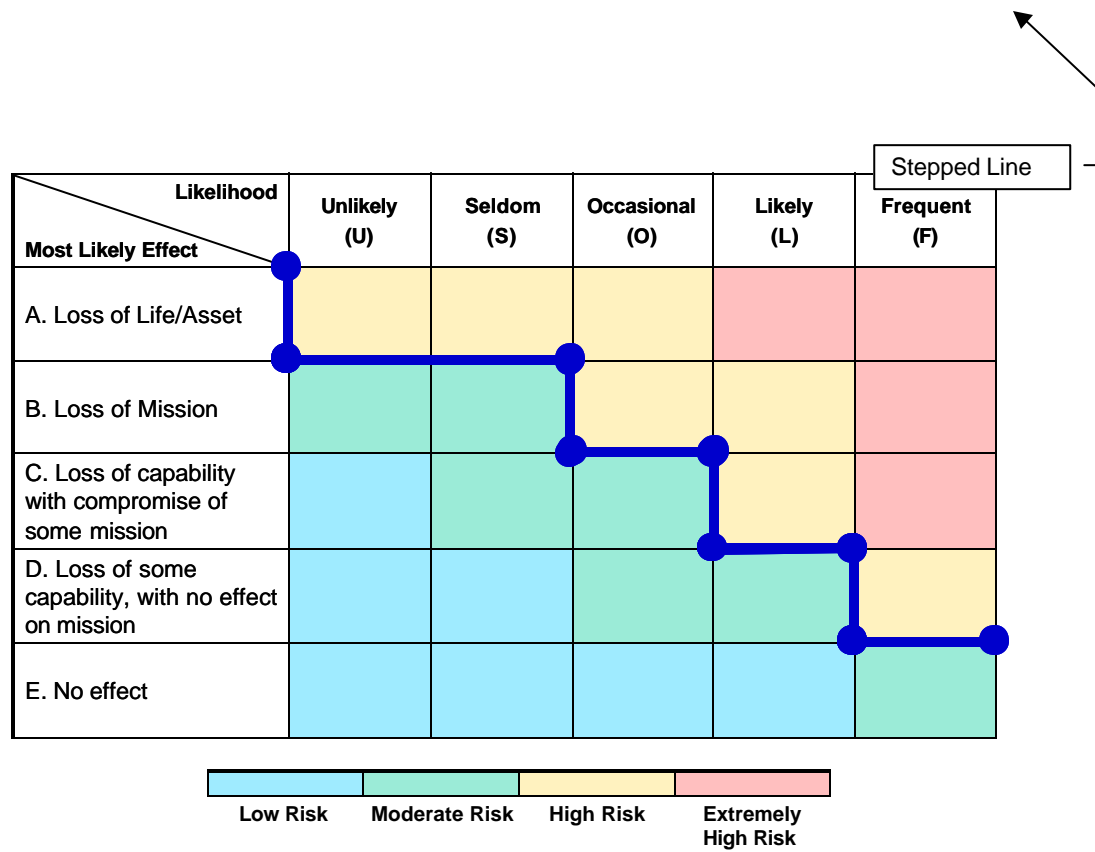


Figure 26: Risk matrix with natural language for Step B.2.2

[Haimes et al., 2001c]

<i>Shades</i>	<i>Risk Severity</i>	<i>Notation</i>	<i>Interpretation</i>
	Extremely High	EH	The risk scenario has catastrophic potential with loss of ability to accomplish mission. Resources should be committed to mitigate risks.
	High	H	The risk scenario may have catastrophic potential while significantly degrading mission capabilities. Resources may need to be committed to mitigate risks.
	Moderate	M	The risk scenarios are unlikely to cause damage while degrading mission capabilities. Resources are not committed to mitigate risks at this time.
	Low	L	The risk scenarios are very unlikely to cause damage with little or no impact to mission capabilities. Resources are not committed to mitigate risks at this time.

Figure 27: Color Assessment and Interpretation Table

Reference #	Subtopic	Likelihood	Impact	Risk	Severity
A.8.2	Retention Program	O	C	M	
A.8.3	Lack of Job Challenges/Motivation	S	D	L	
A.8.6	Qualified Personal	L	B	H	
A.8.7	Understaffed	O	B	H	
A.8.1	Overlooking or Ignoring Defects/Problems	O	B	H	
A.8.9	Lack of Leadership	L	A	EH	
A.8.10	Lack of Team Building	U	B	M	
A.8.11	Communication Breakdown	O	A	H	
A.8.12	Lack of Clearly Defined Goals	S	C	M	
A.8.14	Lack of Inspections	S	B	H	
A.8.18	Complacency	O	A	H	
A.8.19	Lack of Situational Awareness	F	A	EH	
A.8.21	Span of Control	U	C	L	
A.8.24	Time Management	O	C	M	
A.8.25	Lack of Flexibility and Innovation	S	C	M	
A.8.26	Lack of Institutional Knowledge	L	B	H	
A.8.30	Lack of Risk Assessment	L	A	EH	
B.2.11	Organizational Work Load	O	C	M	
B.2.12	Un-supervisory Environment	L	B	H	
C.5.1	External Interfaces/Connections	S	C	M	
C.5.2	Command Post Elements	O	B	H	
C.5.3	Command and Control Communications	L	B	H	
C.5.6	Internal Interfaces	U	D	L	
C.5.7	Critical Support (Staff Functions)	S	B	M	
C.5.8	Information	L	A	EH	
C.5.9	Hardware/Software (Tangibles)	L	C	H	
D.7.1	Viruses	L	C	H	
D.7.2	Engineering Flaws	U	B	M	
D.7.3	Excess Privileges	U	D	L	

Reference #	Subtopic	Likelihood	Impact	Risk	Severity
D.7.4	Unused Security Features	S	C	M	
D.7.5	Trap Doors	U	D	L	
D.7.6	Complexity	S	B	M	
D.7.7	Poor System Configuration	S	B	M	
D.7.8	Interface Issues with Hardware	S	C	M	
D.7.9	COTS	L	C	H	
E.9.a.1	Thrill Seekers	S	C	M	
E.9.a.10	Hacker Groups and Individuals	O	C	M	
F.4.4	Transport	U	E	L	
F.4.5	Network	O	C	M	
G.5.2	Satellite	O	B	H	
G.5.3	Cable	U	D	L	
G.5.5	Radio	O	B	H	
G.5.6	Cellular (Wireless)	S	D	L	
H.7.1	Common Communication Platforms	U	C	L	
H.7.2	Common Technology	O	B	H	
I.3.3	Setting Incorrect or Easily Vulnerable Keys	S	D	L	
J.4.1	Risk	O	C	M	
J.4.2	Security	O	C	M	
J.4.4	Survivability	O	C	M	
J.4.6	Trust	O	A	H	

Table 10: Risk Severity for Risk Scenarios in Step B.2.2

7.4.2.4 Step B.2.3: Multi-Attribute Evaluation

The main goals of this step are to avoid eliminating important subtopics and assist subtopic reduction by quantitative risk analysis in the next step (B.2.4). The information in this step is used as source material to accurately represent the likelihood of each risk scenario in Step B.2.4. In the preceding step (Step B.2.2), qualitative assessments of likelihood and severity are applied to filter a set of scenarios in a matrix [Haimes et al., 2001c]. In this step (Step B.2.3), four attributes are grouped, into 19 categories to illustrate the ability of each remaining scenario to defeat the defensive properties of the system attributes. The attributes include redundancy, resilience, robustness and assurance are grouped in Figure 28. These attributes reflect the seriousness of the threat that a scenario poses to IA as a system. The risk scenarios are rated against natural-language scale levels (high (H), medium (M) and low (L)) defined for each of the 19 sub-categories. The judgment of the severity of the scenario determines whether the scenario should remain for further consideration or should be filtered out [Haimes et al., 2001c]. Figure 28 (Page 108) identifies the sub-categories under each attribute and Table 13 (Page 111) displays the rated scale levels for each sub-category under an attribute. An attribute is definable for each risk scenario or it is “not applicable (NA)” and discarded for that set of risk scenarios. For a set of risk scenarios, several important attributes are discarded and therefore, critical information is lost. Although not within the scope of this thesis, minimizing lost information is a key concern and critical improvement in future research.

The project team wants to reduce the risk scenarios to a more manageable level in the next step in order to apply quantitative risk analysis to those remaining scenarios. Table 11 (Page 107) lists the remaining 21 subtopics (risk scenarios), and exemplifies a more specific situation description. The division specifies “failure of the exercise” as loss

of soldier's life, unresolved IA problems for more than 24 hours, loss of radio communication with a field unit for more than one hour, and loss of a data network for more than four hours.

Subtopic	Risk Scenario Description
Qualified Personal	Failure of the exercise is based on a lack of qualified personnel on any C4ISR system or in any command post. Qualified personnel provide a level of adequate knowledge, service and effort toward an objective.
Understaffed	Failure of the exercise is based on a lack of sufficient personnel to execute any mission during the exercise.
Overlooking or Ignoring Defects/Problems	Failure of the exercise for overlooking or ignoring defects and problems causing equipment related failures.
Lack of Leadership	Failure of the exercise related to lack of sufficient leadership present during crucial times.
Communication Breakdown	Loss of communications and the ability to share information between staffs, units and individuals during the exercise.
Lack of Inspections	Failure of the exercise is based on lack of conducting proper inspections during the exercise.
Complacency	Failure of the exercise is based on unit and individual complacency.
Lack of Situational Awareness	Failure of the exercise is based on lack of situational awareness causing loss of the ability to mitigate risks and knowledge about a unit's environment.
Lack of Institutional Knowledge	Failure of the exercise is based on lack of institutional knowledge in command posts and field units during the exercise.
Lack of Risk Assessment	Failure of the exercise is based on conducting improper risk assessments or failing to execute a risk assessment.
Un-supervisory Environment	Failure of the exercise is based on un-supervisory critical events.
Command Post Elements	Failure of the exercise is based on the compromise of any brigade and above level command post or logistics center by a software virus, hacker, network failure or other IA incident causing situational awareness and mission success.
Command and Control (C ²) Communications	Failure of the exercise is based on compromise of a brigade and above level C ² voice or data links for more than one hour.
Information	Failure of the exercise is based on loss, availability or degradation of division information networks.
Hardware/Software (Tangibles)	Failure of the exercise is based on critical hardware or software entities (i.e., voice and data switches, satellite units, relays, and retransmission units).
Viruses	Failure of the exercise is based on software viruses.
COTS	Failure of the exercise based on commercial-off-the-shelf software failures.
Satellite	Failure of the exercise is based on loss of satellite communications for a field unit of more than 4 hours.
Radio	Failure of the exercise is based on loss of a division radio network (voice or data) for a field unit of more than 2 hours. This includes loss of a retransmission station for more than 2 hours.
Common Technology	Failure of the exercise is based on common technology problems (i.e., interface issues with higher headquarters or supporting units).
Trust	Failure of the exercise is based on lack of information network trust and lack of ability to measure that trust.

Table 11: Risk Scenario Descriptions

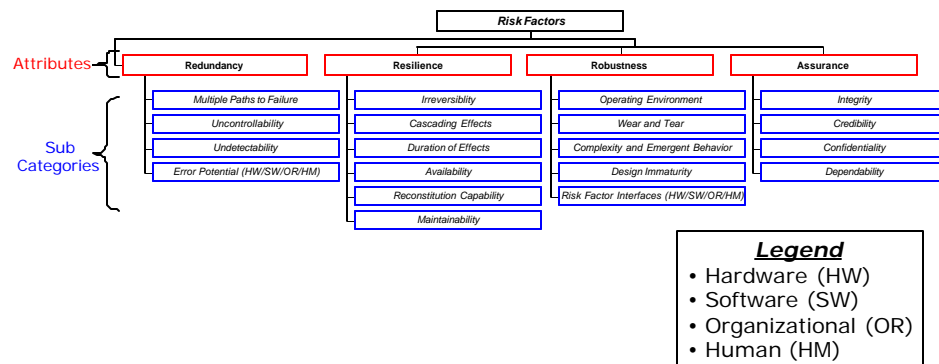


Figure 28: Attributes and Sub-categories for Filtering Scenarios

Classification of the attributes (redundancy, resilience, robustness (called the 3 R's) [Haimes et al., 2001c] and assurance were chosen as the defenses of the IA system in Step B.2.3. The 3 Rs are well known in large-scale systems (i.e. water-resources, space, information and infrastructure systems) and the assurance attribute comprehensively covers specific risk factors associated with IA. Redundancy refers to the ability of extra components of a system to assume the functions after failure [Haimes et al., 2001c]. Resilience is the ability of a system to repair and bounce back following an emergency. Robustness refers to the ability of a system to perform its intended function over the expected useful lifetime in the presence of external stresses or noise. Assurance refers to a system or the information contained within the system to provide trust and credibility to the user. The sub-categories are defined alphabetically in Table 12 (Page 110) and attribute scales are presented in Table 13 (Page 111) from the major defensive attributes of the system.

Availability, confidentiality, dependability, design immaturity, integrity, maintainability, multiple paths to failure, reconstitution capability, risk factor interfaces, uncontrollability and undetectability are discarded attributes based on the set of risk scenarios. Based on this step, the organization rated the risk scenarios against seven attributes represented in Table 14 (Page 112). This step assists the project team in the

reduction process in Step B.2.4 by putting a magnifying glass on the probabilities of the risk scenarios.

<i>Availability</i> : Indicates a scenario for which the system provides correct service during normal and adverse operations.
<i>Cascading Effects</i> : Indicates a scenario for which the effects of an adverse condition readily propagate to other systems or subsystems.
<i>Complexity and Emergent Behavior</i> : Indicates a scenario in which there is a potential for system-level behaviors that are not anticipated simply from knowledge of components and the laws of their interactions [Haimes et al., 2001c].
<i>Confidentiality</i> : Refers to a scenario in which the system has the ability to ensure information is disclosed only to authorized entities.
<i>Credibility</i> : Indicates a scenario in which the system provides a level of confidence about itself and its information.
<i>Dependability</i> : Indicates a scenario that has the ability to deliver service that is justifiably trusted.
<i>Design Immaturity</i> : Indicates a scenario that lack of system experimentation, design experimentation or insufficient concept understanding leads to adverse conditions.
<i>Duration of Effects</i> : Indicates a scenario for which the duration of adverse consequences is long.
<i>Error Potential</i> : Refers to a scenario in which the system has the ability to produce faults, failures or errors by hardware, software, organizational practices or human interaction.
<i>Integrity</i> : Indicates a scenario in which all sub-components work together to accomplish the system mission.
<i>Irreversibility</i> : Indicates a scenario in which the adverse condition cannot be returned to the initial, operational condition [Haimes et al., 2001c].
<i>Maintainability</i> : Refers to a scenario in which the system has the ability to undergo repairs and modifications during normal and adverse operations.
<i>Multiple Paths to Failure</i> : Indicates a scenario in which multiple and unknown methods lead to damage to the system.
<i>Operating Environment</i> : Indicates a scenario that results from external stresses [Haimes et al., 2001c].
<i>Reconstitution Capability</i> : Indicates a scenario in which the system has the ability to rebuild the information lost or damaged after an IA incident.
<i>Risk Factor Interfaces</i> : Indicates a scenario that is sensitive to interfaces among diverse sub-systems (i.e., hardware, software, organizational or human).
<i>Uncontrollability</i> : Indicates a scenario in which there is no need to regulate or adjust the system to prevent damage to the system.
<i>Undetectability</i> : Refers to the likelihood that the system does not recognize the initial events of a scenario before damage occurs to the system.
<i>Wear and Tear</i> : Indicates a scenario that results in degrading effects or performance of the system.

Table 12: Defensive Attributes of the System

	High	Medium	Low	Not Applicable
Availability	Unknown or a below 90% availability rate	Medium availability rate (between 90% and 99%)	High availability rate (above 99%)	Not applicable
Cascading Effects	Unknown or many cascading effects	Few cascading effects	No cascading effects	Not applicable
Complexity and Emergent Behavior	Unknown or high degree of complexity	Medium degree of complexity	Low degree of complexity	Not applicable
Confidentiality	Inflexible	Semi-flexible	Flexible	Not applicable
Credibility	Unknown	Partially known	Well-known	Not applicable
Dependability	Unknown or low potential	Medium potential	High potential	Not applicable
Design Immaturity	Unknown or high immature design	Immature design	Mature design	Not applicable
Duration of Effects	Unknown or long duration	Medium duration	Short duration	Not applicable
Error Potential	Unknown or catastrophic	Moderate	Low	Not applicable
Integrity	Always questioned	Partially questioned	Never questioned	Not applicable
Irreversibility	Unknown or no reversibility	Partial reversibility	Reversible	Not applicable
Maintainability	Unknown or requires constant maintenance.	Moderate maintenance or maintenance is difficult to execute	Minimal maintenance or maintenance is easy to execute.	Not applicable
Multiple Paths to Failure	Unknown or many paths to failure	Few paths to failure	Single path to failure	Not applicable
Operating Environment	Unknown sensitivity or very sensitive to operation environment	Sensitive to operating environment	Not sensitive to operating environment	Not applicable
Reconstitution Capability	Not understood or not well defined. Not easily adapted and executed	Either understood or not well defined. Partially adaptable and some set up time required to execute	Understood, well defined and easily adapted and executed	Not applicable
Risk Factor Interfaces	Unknown sensitivity or very sensitive to interfaces	Sensitivity to interfaces	No sensitivity to interfaces	Not applicable
Uncontrollability	Unknown or uncontrollable	Imperfect control	Easily controlled	Not applicable
Undetectability	Unknown or undetectable	Late detection	Early detection	Not applicable
Wear and Tear	Unknown or much wear and tear	Some wear and tear	No wear and tear	Not applicable

Table 13: Scale levels for the criteria [Haimes et al., 2001c]

Attributes	Cascading Effects	Complexity & Emergent Behavior	Duration of Effects	Error Potential	Irreversibility	Operating Environment	Wear and Tear
Risk Scenarios							
Qualified Personnel	H	M	M	H	M	M	M
Understaffed	M	L	M	M	L	H	H
Overlooking or Ignoring Defects/Problems	H	M	H	H	L	H	M
Lack of Leadership	H	H	H	H	M	H	H
Communication Breakdown	L	M	M	H	L	H	H
Lack of Inspections	M	M	M	H	L	M	M
Complacency	M	H	M	M	H	H	H
Lack of Situational Awareness	H	H	H	H	M	H	M
Lack of Institutional Knowledge	M	M	H	H	M	H	M
Lack of Risk Assessment	M	M	M	H	M	L	L
Un-supervisory Environment	M	M	L	M	M	M	M
Command Post Elements	M	H	M	H	M	H	H
Command and Control Communications	H	H	M	H	M	M	H
Information	H	M	M	H	H	M	L
Hardware/Software (Tangibles)	H	H	M	M	H	M	H
Viruses	H	H	H	M	L	H	H
COTS	H	H	M	M	H	M	M
Satellite	L	H	M	M	L	M	M
Radio	H	M	M	H	M	H	H
Common Technology	M	M	M	L	L	L	M
Reliability	M	M	H	H	M	M	M
Availability	M	M	H	H	M	M	M
Data Integrity	M	M	H	H	M	M	H
Dependability	L	M	L	M	M	M	M

Table 14: Rating Risk Scenarios Against the Seven Attributes

7.4.2.5 Step B.2.4: Filtering and Ranking Using the Cardinal Version of the US Air Force Risk Matrix

This step reduces the number of entries in the IA HHM from approximately 20 to 10. In previous steps, qualitative methods were used to filter risk scenarios. In this step, quantitative and specifically estimating the absolute likelihood of a scenario is used, when possible. The use of ranges of likelihood has advantages and averts linguistic confusion when interpreting natural language expressions such as “high”, “low”, etc. Numerical approaches makes matrix mapping tractable and easily modifiable. Figure 29 (Page 114) depicts the cardinal version (probabilities along the top axis) of the risk matrix first deployed in Step B.2.2. The probabilities are only a guideline and are adjustable to meet an organization’s needs. Deciding on the probabilities along the top axis can be difficult and is based on an organizations ability to gather data on the filtered risk scenarios. Data mining using statistical and historical data, expert evidence and simulation results are several ways of generating probability data on risk scenarios. The IA project team sets the same threshold as in Step B.2.2 to filter all risk scenarios below the high risk severity level, and denotes the threshold by the stepped line in Figure 29.

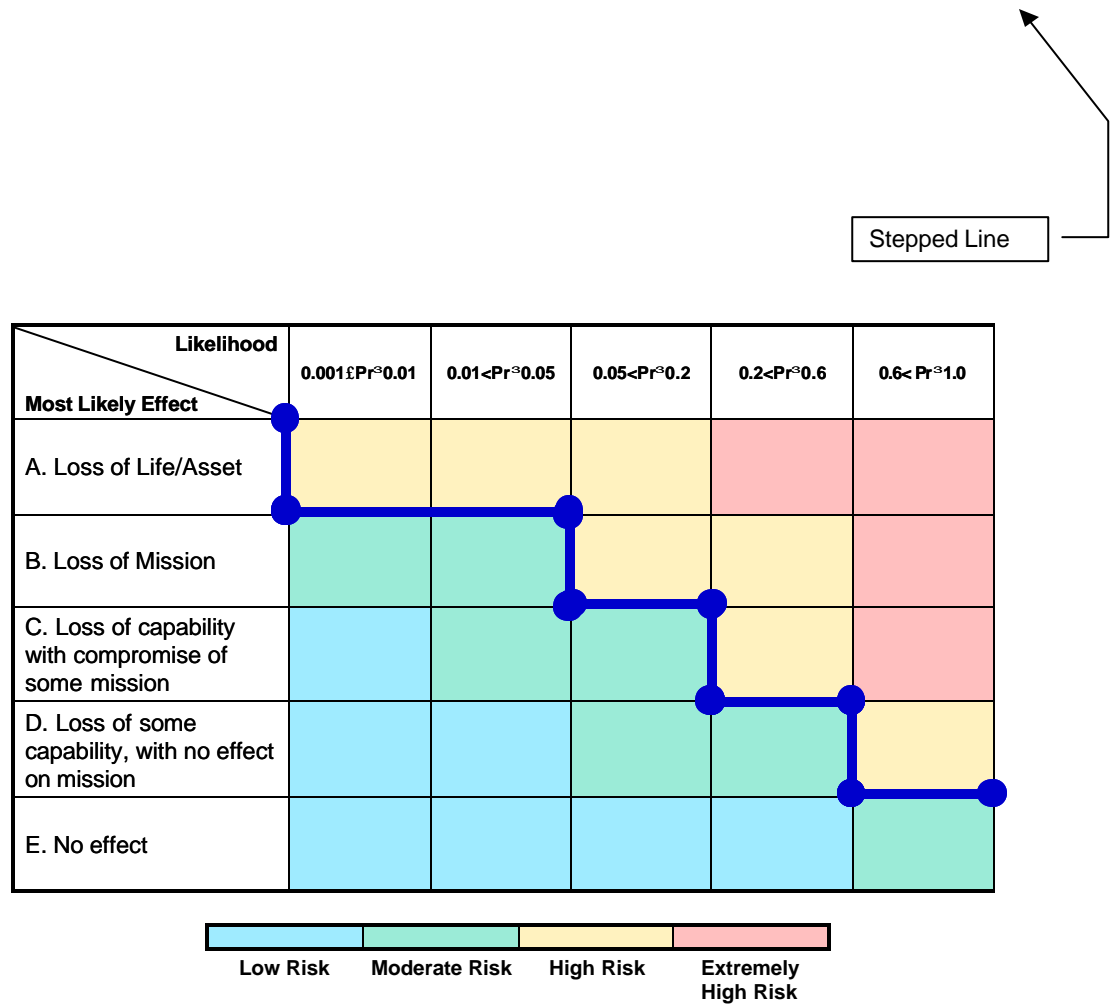


Figure 29: Cardinal risk matrix version [Haimes et al., 2001c]

The following notation for Table 15 (Page 116) is used to represent the impact and risk severity columns. The data within the table is fictitiously generated to illustrate the methodology. The letters A, B, C, D, and E represent the impact (e.g., A denotes Loss of Life/Asset) and the letters EH, H, M and L represent the risk severity column (e.g., EH denotes Extremely High and L denotes Low) based on Figure 29. The project team identifies the seven manageable sets of risks in Table 15 (Page 116) depicted by highlighted cells.

Sub-topic	Likelihood of Failure	Impact	Risk Severity
Qualified Personal	0.20	A	H
Understaffed	0.01	B	M
Overlooking or Ignoring Defects/Problems	0.20	C	M
Lack of Leadership	0.15	C	M
Communication Breakdown	0.10	C	M
Lack of Inspections	0.01	B	M
Complacency	0.05	B	M
Lack of Situational Awareness	0.50	A	EH
Lack of Institutional Knowledge	0.25	C	M
Lack of Risk Assessment	0.10	B	M
Un-supervisory Environment	0.15	C	M
Command Post Elements	0.05	B	H
Command and Control Communications	0.80	B	EH
Information	0.05	B	M
Hardware/Software (Tangibles)	0.45	D	M
Viruses	0.07	B	H
COTS	0.75	C	EH
Satellite	0.55	D	M
Radio	0.45	B	EH
Common Technology	0.15	D	L
Reliability	0.01	B	M
Availability	0.01	B	M
Data Integrity	0.005	B	L
Dependability	0.001	B	L

Table 15: Results from Step B.2.4

Examples of the assessments that the project team completed as part of their in-depth analysis of the likelihood impact estimates are list below. Only the extremely high-risk severity scenarios are listed for brevity purposes.

- *Qualified Personnel*: Likelihood of failure = 0.20; Most Likely Effect = A (Loss of Life), Risk Severity = High.
 - The failure of any unit or command post lacking qualified personnel may cause the failure of a mission or exercise goal. The division is adding several technology-based systems to its arsenal to aid in seeing, hearing, and visualizing the battle. The technology-based systems require qualified individuals to run, maintain, and manage critical organizational systems.
- *Lack of Situational Awareness*: Likelihood of failure = 0.50; Most Likely Effect = A (Loss of Life/Asset), Risk Severity = Extremely High.
 - The failure of any unit or command post lacking situational awareness at critical times during the exercise might produce a circumstance where loss of life or assets occurs. Situational awareness is defined as individuals or elements having definite knowledge of their environment and the battle command environment. In a military operation or exercise, lack of situational awareness has let to fratricide, loss of equipment and life, and loss of mission objectives. Situational awareness is a key component of total spectrum dominance and achieving information superiority.
- *Command Posts Elements*: Likelihood of failure = 0.005; Most Likely Effect = B (Loss of Mission), Risk Severity = High.
 - Command post elements at all levels of the military play important roles in collecting, storing, retrieving, transmit and present information for

command and control purposes. An integrated and skilled command post gathers the information necessary to allow decisionmakers to allocate resources, firepower, and maneuver forces to defeat the enemy or accomplish unit objectives. Protecting command posts represent critical nodes that move information around the battlefield and are key components to the success of any military operation. The failure of any a division command post may cause the failure of a mission or exercise goal. Protecting those critical elements during the exercise from human error, system failure or enemy degradation is essential in full spectrum dominance.

- *Command and Control Communications:* Likelihood of failure = 0.80; Most Likely Effect = B (Loss of Mission), Risk Severity = Extremely High.
 - Communications is used extensively during any military operation to control forces, and resources while ensuring the safety of forces and tracking the exercise objectives. Reliable and available command and control communications is essential during this exercise. The failure of a command and control system may cause the failure of a mission or exercise goal. The exercise hinges on communications and connectivity between systems and units.
- *Viruses:* Likelihood of failure = 0.07; Most Likely Effect = B (Loss of Mission), Risk Severity = Extremely High.
 - The exercise uses many computers within several command posts integrated to the Internet for reach back purposes. Data, information and intelligence are passed from one computer system to another automatically or manually. Some of the systems are connected to the

Internet and inadvertent virus downloads may cause system loss or degradation, and affect information flow among the division elements.

- *Commercial-off-the-shelf Software (COTS)*: Likelihood of failure = 0.75; Most Likely Effect = C (Loss of Capability and compromise to some mission), Risk Severity = Extremely High.
 - Many of the commercial-off-the-shelf software products are used to store, transfer and modify data, maintain information networks, and communicate between elements in a tactical and non-tactical environment. The security of the telecommunications system (i.e., telephone system and the Internet) largely depends on the integrity and reliability of COTS technologies that constitutes and supports these systems. The division's tactical communications network has COTS products that can hinder or degrade operations if the software fails.
- *Radio*: Likelihood of failure = 0.45; Most Likely Effect = B (Loss of Mission), Risk Severity = Extremely High.
 - The main communications technology within a division is its radio systems. The radio system affords the division the capability of secure line of site communications with real-time applications. Although many radio nets are overlapping, the loss of one or more radio nets based on operator error, compromise, hardware failure, key security error or failure may hinder or degrade the mission and operations within the division.

7.5 Step C: System Modeling and Analysis

Modeling enables predicting or estimating the variables and elements affecting IA risk scenarios, and their interaction with each other. There is an art and science to model building, which uses theories, philosophies, tools and methodologies to define the

model. It is almost always cheaper and faster to work with a model than to directly study the dynamics of a large-scale system. A model assists analysts in understanding the complexity of the problem by graphically representing the problem. It is essential to identify, construct and interpret the models accurately to reflect the characteristics of the real system. After the reduction and filtering process of the HHM, a model in the form of an Input-Output model for the entire risk scenario subset and an influence or event tree diagram for each individual scenario are constructed to identify the functional relationships among the system components and its environment. The analyst decides which model diagram is most useful to the IA process and methodology, and it may be necessary to model a risk scenario with both influence and event tree diagrams. Sometimes it is impractical to use quantifiable risk analysis on certain risk scenarios, therefore, qualitative means are used.

The I-O model is a starting point for the development of modeling diagrams as the least mature of the other modeling techniques (Figure 30, Page 121). An influence diagram (illustrates interconnectedness or interdependencies) or an event tree diagram (illustrates actions leading to an event) is developed for each risk scenario. The end result of the modeling process is a fault-tree configuration for each policy (design) option, if appropriate. Fault-tree analysis is well known and used and justified as a modeling technique. This process leads to more precise analysis of extreme events through expert evidence or Fractile distribution method (Step D.4).

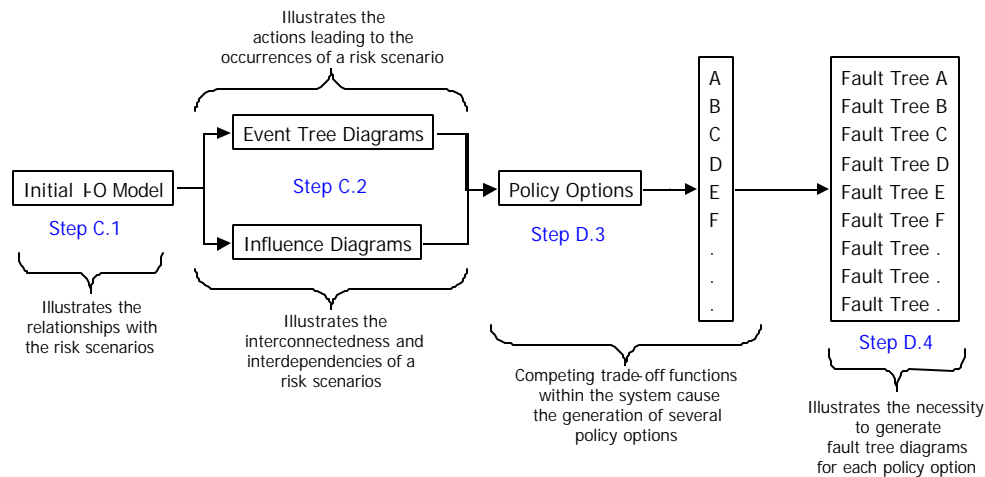
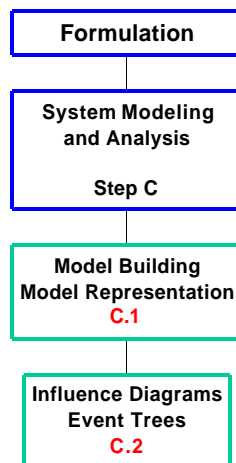


Figure 30: Modeling Diagram Roadmap

7.5.1 Step C.1 Model Building and Model Representation (Input-Output Modeling)



In order to analyze the relationship of the variables, it is necessary to determine an appropriate mathematical model and system representation after Step B is complete. Mathematical model formulation has a set of equations that describe and represent the real system [Haimes, 1998]. Although no single modeling technique would totally encompass the complexities, and interconnectedness of information systems, it is important to identify the interrelationships between the variables.

An Input-Output (I-O) [Willis, 2000] model is used to understand the variables, and their complexities. Mathematical relationships, constraints, and assumptions within the I-O model are important but not developed in this chapter. Critical assumptions and constraints are also identified within the I-O model construction. *Constraints* are restrictions or limitations within the system such as

resources, physical, economic, institutional, or legal limitations. *Assumptions* are facts or statements (e.g., proposition, axiom, postulate, notion), which is understood and taken for granted. The I-O model is also useful in developing other modeling techniques (e.g., influence diagrams and event tree diagrams) discussed in Step C.2. Figure 31 (Page 124) illustrates an I-O model for the set of filtered risk scenarios. The model centers on trust and credibility as characterized by its state variables. The states of the system must have some measurable attribute and the project team identified four states of the system: trust, maintainability, surety and human effort.

- *Trust* is defined as the confidence in or reliance on some quality or attribute of a system or piece of information is measured in the form of reliability. *Reliability* is the conditional probability that the system will perform correctly throughout the interval $[t_0, t]$ [Johnson, 1989].
- *Maintainability* is defined as a measure of the ease with which a system can be repaired, once it has failed [Johnson, 1989] is measured in the form of availability. *Availability* is the probability that a system is operating correctly and is available to perform its functions at the instant of time t [Johnson, 1989].
- *Surety* is defined as the measure of the acceptable system performance under an unusual loading [Ezell, 1998]. *Survivability* is the capability of a system to achieve its mission objectives in a timely manner in the face of accidents, failures, and attacks [Longstaff and Haimes, 1999].
- *Human Effort* is defined as the effective force or exertion against any possible resistance to accomplish a particular goal or objective. *Mean time to human error* is the expected mean time of a human error occurrence related to the human performance reliability function [Dhillon, 1999]. The equation is expressed in the Chapter 6 , Information Assurance Metrics.

There are five variables that are used in this I-O model formulation [Haimes, 1998].

1. *Decision Variables* (**x**) are measures controlled by the decisionmaker such as policy and legislation, organizational environment, education, resources, etc.
2. *Input Variables* (**u**) are materials entering the system but may not be controllable by the decisionmaker such as organizational structure and size, and information system configurations.
3. *Random Variables* (**r**) are events that happen with some associated probability and are described by an associated probability distribution (discrete random variable) or probability density function (continuous random variable).
4. *State Variables* (**s**) represent the quantity and quality level of a system in time. State variables may fluctuate within a system over time.
5. *Output Variables* (**y**) are closely related to the state of the system, the decision and random variables [Haimes, 1998] and often are written as functions of state variables.

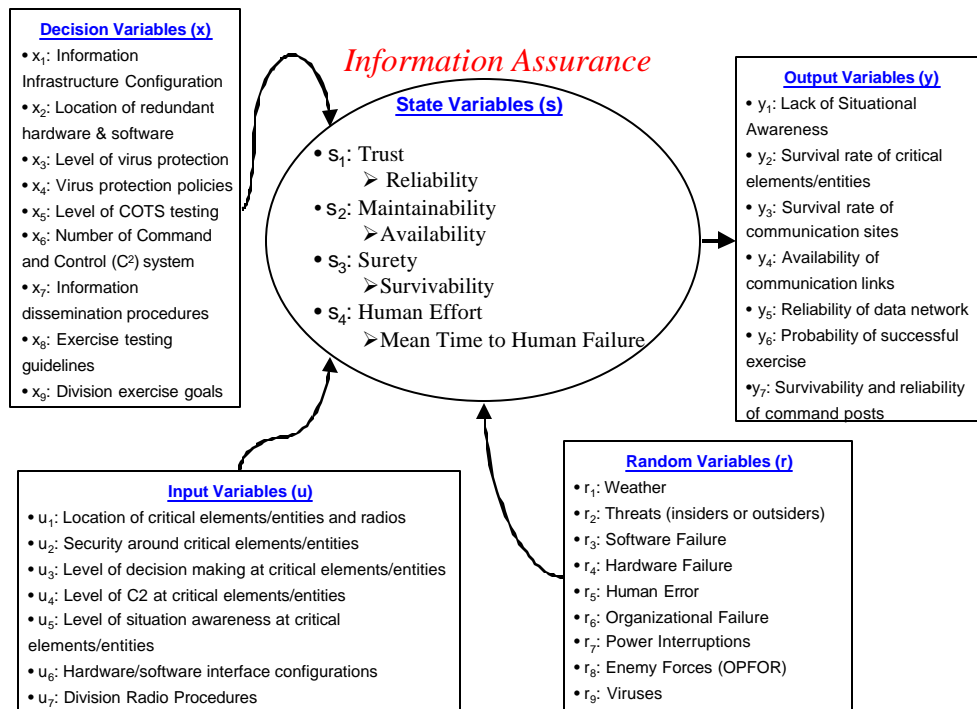


Figure 31: Information Assurance I-O Model

7.5.2 Step C.2: Influence Diagrams and Event Trees Diagrams

In this chapter, only the risk scenarios qualified personnel and radio communications are used to illustrate the remaining tasks within the methodology. The risk scenario *qualified personnel* is modeled with an influence and event tree diagram, where *radio communications* is modeled with only an event tree diagram.

7.5.2.1 Influence Diagrams

One of the most basic, logical and intuitive of modeling building is the influence diagram [Haimes, 1998]. Influence diagrams are unlike the HHM and mathematical model building, although both can assist in identifying the components of the diagram. Organizations need to generate mitigation policies based on the nodes with the most

interaction or correlation and therefore, have the most effect upon the organization in terms of risk, cost and effectiveness. Influence diagrams have the following attributes:

1. Influence diagrams represent casual relationships of a large number of variables.
2. The diagrams use conventional symbols i.e., decision nodes and chance nodes, to capture system randomness.
3. Involves brainstorming as the principle data-gathering tool.
4. Forms a reliable model for decisionmakers and analysts to use for planning and managing the cost, benefits and risks associated with a specific system.
5. Correlation among components can be represented through data or scenario analysis within the diagram. Generally, high correlation is depicted by plus signs (+) and low correlation depicted by negative signs (-) within the diagram.

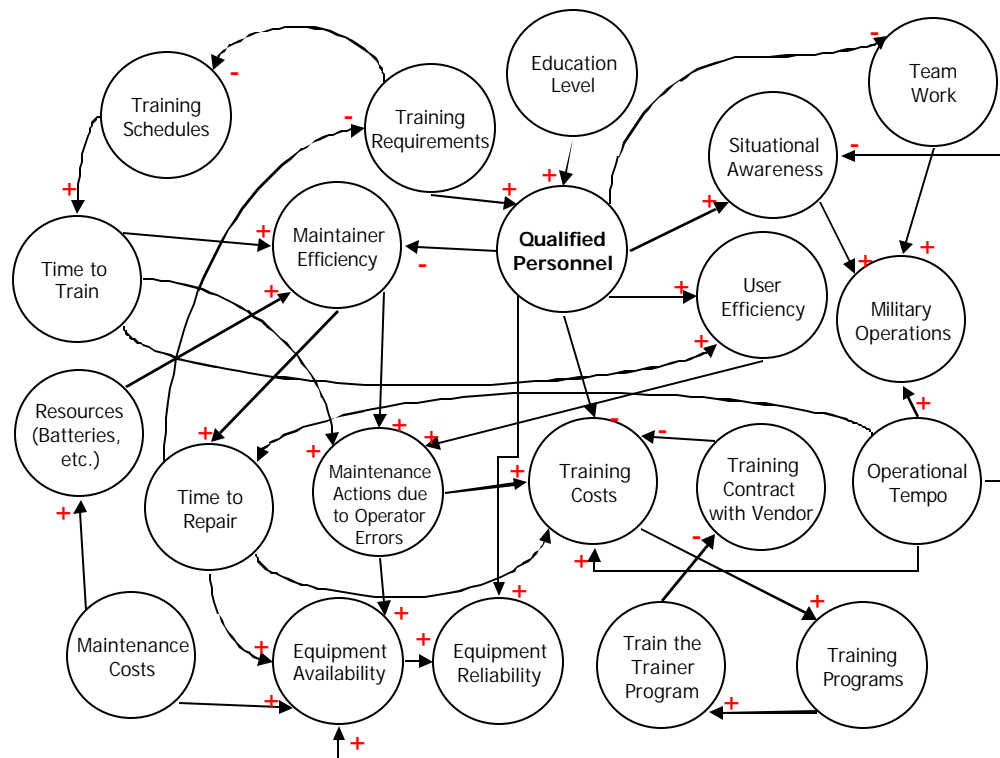


Figure 32: Qualified Personnel Influence Diagram

The division project team represents the risk scenario, *qualified personnel* and isolates several key components from the diagram (Figure 32). *Maintenance Actions due to Operator Errors* play a significant role in the diagram by having five connections with other nodes. These connectors represent a high correlation and interdependency between events. *Equipment availability, operation tempo, time to train, time to repair, and training cost* represent similar correlations and interdependencies. These critical nodes have a major effect on having qualified personnel within the organization. Policy generation should focus on these nodes in order to mitigate or transfer risks within the organization and on future operations. Another component of this influence diagram is the interconnectedness with another filtered risk scenario, i.e., situational awareness in Figure 33 (Page 127). The division IA project team identifies the relationship and develops a situational awareness influence diagram to capture any additional interdependencies.

The consequences are conditioned on the occurrence of the initiating event and subsequent mitigating events (e.g., denial of service attack through a firewall or intrusion detection platform, or human error through sensors, detectors, and fault alarms). In event tree, each event is defined by the success of the event with probability p and failure of the event with probability $1-p$. The objective of the event tree development is to define a comprehensive set of initiative event sequences that encompasses the effects of all realistic and physically realizable potential failures involving the system [Tulsiani, 1989]. Figure 34 and Figure 35 represent event trees for the risk scenarios *radio communication* and *qualified personnel*, respectively. In Figure 34 (Page 129), the event tree reads as follows: given the division radio network falls below the set threshold (98%), does improper COMSEC cause the event? The answer is YES with probability p_1 and NO with probability p_2 ($p_2=1-p_1$). The probability of each event is displayed conditional on the occurrence of events that precede it in the tree [Tulsiani, 1989]. The total event tree represents paths of mitigating events and may represent a success or failure scenarios. Event tree diagrams like fault-tree diagrams are qualitative tools that are evaluated quantitatively [Tulsiani, 1989]. Organizations need to generate mitigation policies based on the events with the highest occurrence probability and therefore, have the most effect upon the organization in terms of risk, cost and effectiveness.

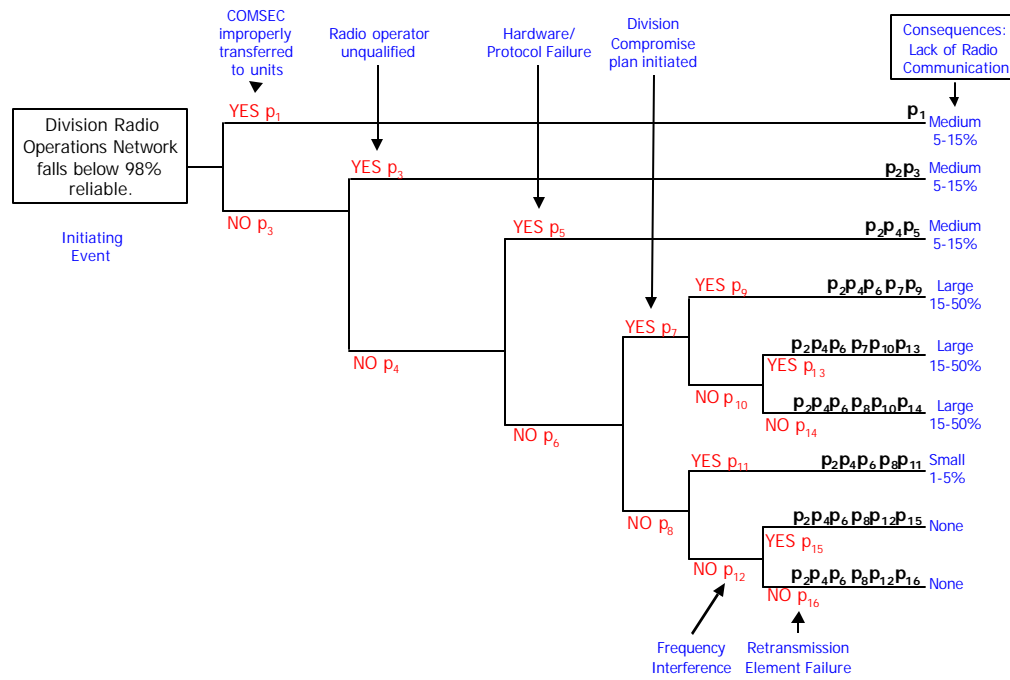


Figure 34: Radio Communications Event Tree Diagram

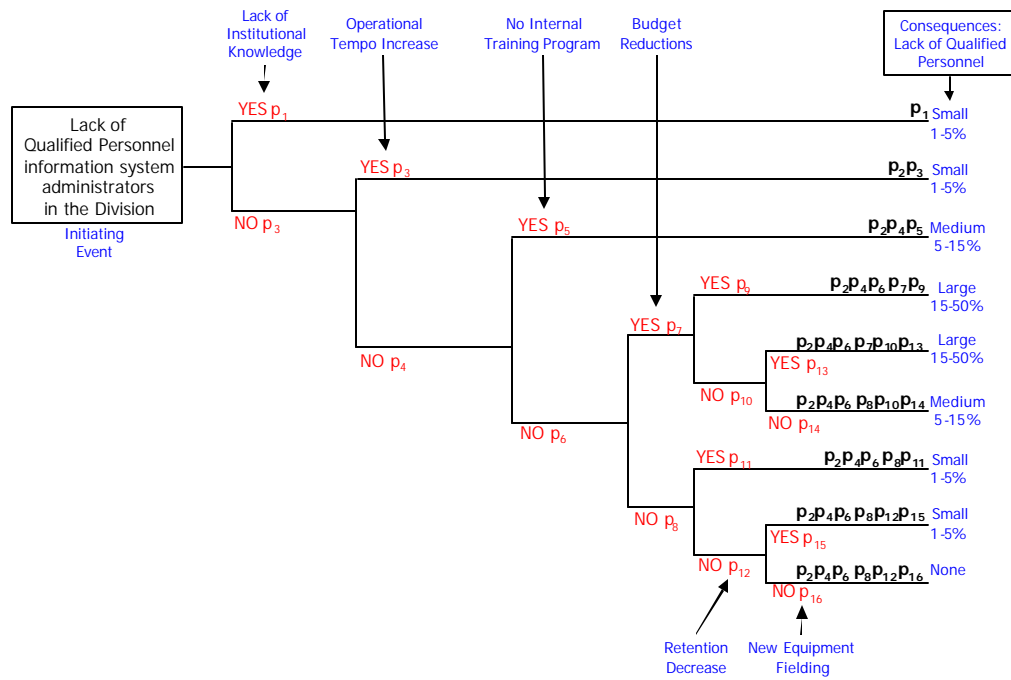
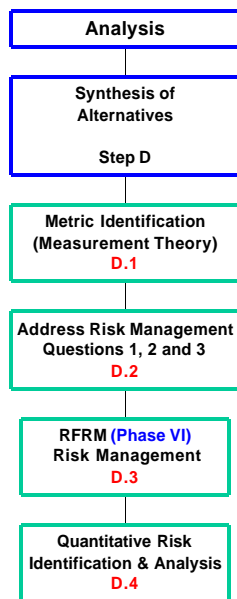


Figure 35: Qualified Personnel Event Tree Diagram

7.6 Step D: Synthesis of Alternatives

7.6.1 Step D.1: Metric Identification



In this step, after the head-topics and subtopic of the HHM are decomposed and 10-20 topics remain, appropriate metrics are developed (e.g., measures of effectiveness, risk, cost) to each topic to gauge the usefulness of the model and policies (Figure 36, Page 132). After the risk scenarios are filtered, each scenario is mapped into a matrix, which describes the metric by type (quantify, qualify or temporal) and by what metric scale (nominal, interval, ordinal, and ratio), which are described in Chapter 6 . The HHM topics are decomposed for the purpose of quantitatively or qualitatively characterizing the knowledge sought by decisionmakers with different needs. As an example, if the subtopic “insiders” from the head-topic “threats” remains after decomposition, a metric is derived that represents the characterization of that subtopic.

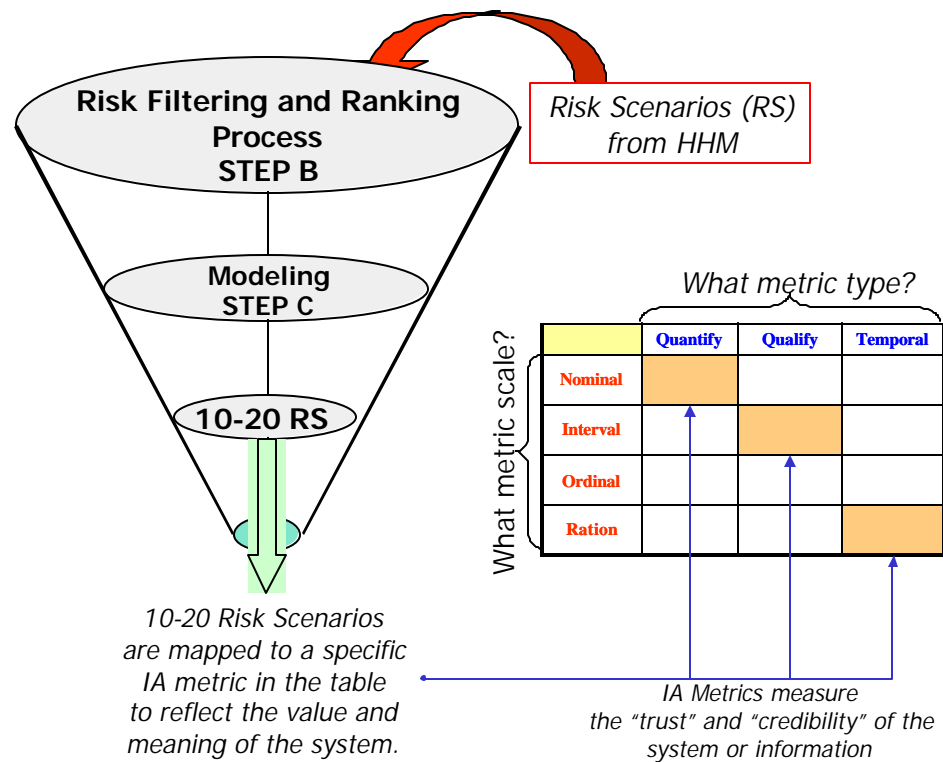


Figure 36: Filtered Risk Scenario Metric Representation

Metrics are needed to establish scales (bounds) and benchmarks for evaluating, designing, installing, operating and maintaining the appropriate level of assurance for specific risk scenarios. The overall goal is a single IA measurement for a specific risk scenario to compare across systems while being useful to the decisionmaker. IA metrics for the seven risk scenarios (subtopics from the HHM) are formulated by using the five-step metric taxonomy developed in Chapter 6 .

7.6.1.1 STEP 1 (Determine the organizational or system objectives)

Figure 37 (Page 133) depicts some organizational objectives generated for the upcoming exercise. The project team chose to measure the next fielding exercise with four base objectives (i.e., risk, availability, information loss and cost). Risk, availability,

and information loss are decomposed further into sub-objectives to help measure the top-level objectives.

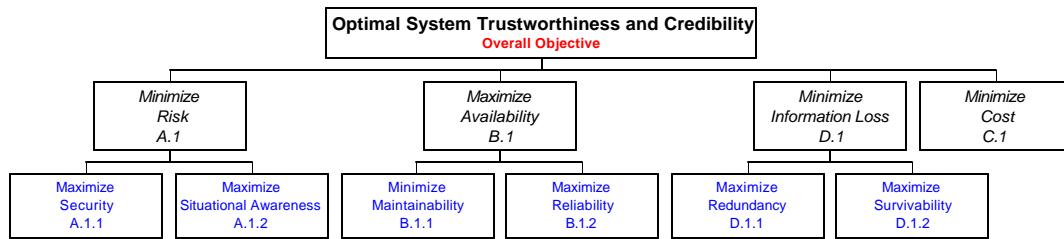


Figure 37: IA Division Project Team Exercise Metric Value Hierarchy Structure

7.6.1.2 STEP 2 (Determine the impacts and consequences needed to be measured)

The end result of this step is the development of three tables. The first table, Table 16 (Page 134) represents five consequences of information assurance for the division established by the project group and their interpretations. The second table, Table 17 represents the interpretation of the impacts that is used in the last table. The last table is a fusion of the first two tables. Table 18 (Page 135) illustrates a mapping of consequences and objectives and their relative impacts on the mission, which is used by organizations as a priority list for metric implementation or data gathering. Table 18 is based on the objective that the metric is attempting to measure and not the metric itself.

Consequence	Interpretation
<i>Loss of Decisionmaking Capability</i>	Loss of the commander's or unit leaders ability to execute decisive decisions on the battlefield. The loss hinders such capabilities as initiative, ability to fight in a "deliberate" setting and the ability to make and communicate sound decisions faster than the enemy [Lamm, L., 2001].
<i>Loss of Equipment</i>	Equipment such as vehicles, tanks, and other weaponry are either destroyed or degraded due to information assurance issues.
<i>Loss of Life</i>	A U.S. Soldiers dies from enemy contact, lack of situational awareness or fratricide.
<i>Loss of Information</i>	Information and knowledge about the battlespace are critical to assist leaders to make timely battlefield decisions. The loss of information assurance hinders such capabilities as superiority, initiative, ability to fight in a "deliberate" setting, the ability to make and communicate sound decisions faster than the enemy and increases the probability of chance encounters with the enemy [Lamm, L., 2001]
<i>Loss of System/Information Trust</i>	Leaders and elements have lost partial or total trust in a system or systems. The lost of trust is affecting situational awareness and dominant battlespace knowledge.

Table 16: Metric Impact and Consequences [Lamm, L., 2001]

<i>Impact</i>	<i>Interpretation</i>
Extremely High	Loss of ability to accomplish mission.
High	Significantly degrades mission capability.
Medium	Degrades mission capability.
Low	Little or no impact to mission capability.

Table 17: Metric Impact Interpretation [Lamm, L., 2001]

Metric <i>Mission Impact</i> Consequence	Minimize Risk	Maximize Availability	Minimize Information Loss	Minimize Cost/Effort
<i>Loss of Decisionmaking Capability</i>	Extremely High	High	Extremely High	Medium
<i>Loss of Equipment</i>	High	High	High	Low
<i>Loss of Life</i>	Extremely High	Medium	Extremely High	High
<i>Loss of Information</i>	High	Extremely High	Extremely High	Medium
<i>Loss of System/Information Trust</i>	Medium	Extremely High	Extremely High	Low

Table 18: Objective-Consequence Mapping Table for Mission Impacts

7.6.1.3 STEP 3 (Determine the appropriate metrics for the filtered risk scenarios)

The lowest level objectives are mapped to metrics that are used to measure the effectiveness of the system or compare the system to other systems. In this case, the project team has some measurements from the last exercise and gauges the usefulness of policies, systems and procedures generated by the organization. Table 19 (Page 136) depicts the filtered subtopics mapped to a specific IA metric with its type and units.

7.6.1.4 STEP 4 (Determine range, benchmark, and metric units)

Metric units are represented in Table 19. Benchmark and ranges for each metric are not within the scope of this thesis and are not represented in this chapter or step. A metric unit depicting none represents a qualitative metric.

7.6.1.5 STEP 5 (Determine metric validation and implementation rules)

The division project team has issued guidance on what measurement data is needed prior to the exercise and on a daily basis throughout the exercise. Metrics like *mean effort to repair a system* and *number of qualified radio operators* are known prior to an operation, others like *mean time to reach target* and *redundancy ratio* are calculated continually throughout an operation or lifecycle. Metric validation and implementation rules consist of steps necessary to successfully and accurately measure specific metrics (e.g., what element or person is collecting the metric data, when is the metric data collected, and how is the metric data collected).

Risk Sub-topic	IA Metrics	Metric Type	Metric Units
<i>Qualified Personal</i>	Personnel Turnover Rate	Quantify	Percent
	Standard Stability Measurement	Qualify	None
	Mean time to Human Error	Quantify	Seconds/Minutes
<i>Lack of Situational Awareness</i>	Expected Effect on Adversary Decisionmaking Abilities	Qualify	None
	Potential Effect (Type I Error)	Quantify	None
<i>Command Post Elements</i>	Detectability	Quantify	None
	Redundancy Ratio	Quantify	None
	Mean Effort to Reach Target	Temporal	Days
	Buffering Effect	Quantify	None
<i>Command and Control Communications</i>	Duration of the Effects	Temporal	Seconds/Minutes
	Number of Dissimilar Systems	Quantify	Systems
	Hardness	Qualify	None
	System Design Adequacy	Quantify	None
	Mean Time to Repair	Temporal	Seconds/Minutes
	Likelihood of Gaining Access to a Sub-system or the Total System	Quantify	None
<i>Viruses</i>	Number of Eradicated Viruses	Quantify	Viruses
<i>COTS</i>	Lifecycle Costs	Quantify	Dollars
	System Spoilage	Qualify	Percent
	Software Capability Maturity	Qualify	None
	Defect Density Measure	Qualify	Defects/LOC
<i>Radio</i>	System Flexibility	Qualify	None
	Mission Time	Temporal	Seconds/Minutes
	Repair Rate Function	Quantify	Systems/unit time

Table 19: Subtopic IA Metric Mapping

7.6.2 Step D.2: Address Risk Management Questions

In this step, we answer the three-risk management question discussed in Step A.2 (Page 84) and related questions depicted in Table 20 (Page 138). These questions provide the framework for risk management and serve as the stopping criteria for this section. Risk management asks, “what can be done and what options are available”, “what are the associated trade-offs in terms of cost, benefits, and risks”, and “what are the impacts of these decisions.” Each of these questions introduces related questions (Table 20) associated with risk management that guides the decisionmaker and analyst through the process of generating policy options.

Questions	Additional questions
<i>What can be done and what options are available?</i>	What Design modifications or operational changes could reduce the risk associated with these scenarios?
	How much would it cost to implement these options?
	What is the risk reduction from the identified scenarios?
	Would these options create new risk scenarios?
<i>What are the associated trade-offs in terms of cost, benefits, and risks?</i>	Which policy options are in direct conflict within a specific technology, resources or cost?
	Which policies can be grouped together by category (i.e., cost, resource, technology, etc.)
	Are all the goals or policies critical?
	Can we learn from other projects?
<i>What are the impacts of current management decision on future options?</i>	What are the vulnerabilities of the current decisions (perceived or real)?
	What future paradigms shifts will affect future options (i.e., technology, policy, etc.)?
	What known limitations will effect future options (i.e., technology (processing speed), policy (time), etc.)?
	Are all the expectations realistic?

Table 20: Risk Management Questions and Sub-questions

7.6.3 Step D.3: Risk Management

Risk management is the optimal balance between uncertain benefits and uncertain costs. The premise that risk management must be an integral part of the overall decisionmaking process necessitates following a systemic, holistic approach in dealing with risk [Haimes, 1998]. In this step, we conduct quantifiable risk management. Risk management is successfully accomplished when applied to a small number of risk scenarios. During the previous steps within the IA methodology, the following tasks were accomplished:

- Identified risk scenarios associated with IA (STEP A).
- Quantified the consequences of the scenarios (STEP B).
- Quantified the likelihood of the scenarios (STEP B).
- Identified IA metrics associated with remaining risk scenarios (STEP C).
- Modeled the remaining filtered and ranked risk scenarios (STEP C)

During the course of modeling (i.e., influence and event tree diagrams) and addressing the risk management questions, policy options for the risk scenario: *qualified personnel* (i.e., for tactical network system administrators) were generated in Table 21 (Page 140). The policy options parallel the People Capability Maturity Model (P-CMM) [Curtis, 1995]. The P-CMM is a process that guides organizations to improve their organizational capabilities and increase personnel quality. Although not all risk scenarios afford the opportunity to match policy options to a model or structure, it is important not to “recreate the wheel.” The IA project team decides that cost, number qualified, level of qualification and organizational unreliability are attributes that represent the policy options. There may be other attributes (e.g., time away from station) that organizations feel are important and these attributes form trade-offs. The computation of the costs for the different scenarios was computed taking the cost for the basic scenario (do nothing policy option) and assigning it the lowest value of 0 while the highest cost is assigned 100. The cost may be assigned any monetary value (e.g., thousands, millions) by the organization and the cost function can be related to cost of effort or implementation. Actual cost figures should be used if available. Organizational unreliability is a subjective measurement defining the quality of service the unit supplies to its customers. In this example, automation personnel must install, and maintain data networks for the division, reliably. Organizational unreliability measures the lack of effectiveness, lack of effort or training of the unit.

The set of policies form a trade-off between capability (number trained, level of qualification) and cost although other attributes may be considered. The execution the Multi-objective Trade-off Analysis is conducted in Step F.1 and the risk scenario: *qualified personnel* there is no further need for additional quantitative analysis.

Policy Option	Policy Description	Cost	Number Qualified	Level of Qualification	Organizational Unreliability
A	Do not mitigate the risk scenario even though there is a lack of qualified personnel within the division.	0	2	Low	0.10
B	Centralize DAMO support at the division main command post and disperse technical support based on priority and situation. Conduct internal classes within DAMO. Train additional personnel in each brigade and above unit to augment the DAMO with certain tasks.	55	10	Medium	0.03
C	Improve personnel competency development by sending all of the soldiers (8) for a one-week networking and information system course with vendors. Conduct any other unit improvement training (e.g., leadership, military occupation, specialty, management)	30	10	High	0.04
D	Increase DAMO staffing by 2-5 soldiers. Conduct internal classes within DAMO. Decentralize DAMO at each division and brigade command post.	100	12-15	Low	0.01
E	Send 5 soldiers to one-week networking and information system vendor certification course.	15	10	High	0.05

Table 21: Policy Options for the Risk Scenario: Qualified Personnel

The project team decides that the risk scenario *radio communication* requires further quantitative analysis after the modeling and risk management steps. The policy options in Table 22 (Page 141) represent a mix of decisions (i.e., training and technology aspects) for quantitative analysis. Mitigating these risk scenarios increases the

reliability, availability and trust of the information networks and systems. Policy options may be combined at the decisionmaker's discretion in Step F.2 prior to executing any recommendation from the project team. Again, the computation of the costs for the different scenarios was computed taking the cost for the basic scenario (do nothing policy option) and assigning it the lowest value of 0 while the highest value is assigned 100. The costs for Policy H and I do not represent additive costs between their respective policy options.

Policy Option	Policy Description	Cost
A	Status Quo; do nothing. Do not mitigate the risk scenario.	0
B	Conduct division wide radio operator training classes.	15
C	Conduct unit radio operator training classes with division auditing.	50
D	Increase the number of division retransmission elements for the command net. Use parallel retransmission elements to increase reliability.	90
E	Increase the number of division retransmission elements for the command net. Use serial retransmission elements to increase the range of the radio net.	100
F	Centralize radio maintenance on the battlefield	25
G	Decentralize radio maintenance on the battlefield	35
H	Policy Option C and F.	45
I	Policy Option C and G.	65

Table 22: Policy Options for Risk Scenario: Radio Communications

7.6.4 Step D.4: Quantitative Risk Identification and Analysis

This section has two key components. First, determine the appropriate risk analysis tools to facilitate decisionmaking within IA. The tools developed in this section are interpreted for decisionmaking in Step F. Second, execute quantitative risk analyses on the information collected throughout the methodology. There are an assorted number of risk techniques, and tools to assist decisionmakers with IA. Tools such as Fault-tree analysis, Risk of Extreme Event analysis, Partitioned Multi-objective Risk Method (PMRM) [Haimes, 1998], Fractile Distribution Analysis, and Uncertainty and

Sensitivity Analysis are applied to the risk scenarios to validate and demonstrate the benefits of risk analysis and management for IA problems. Within the scenario-based example the tools are explained and illustrated with the exception of the Uncertainty and Sensitivity Analysis. The Uncertainty and Sensitivity Analysis is only described in Section 7.6.4.5 but for more information consult Haimes [1998]. The risk scenario *radio communications* is used to illustrate quantitative risk analysis. Table 23 represents some of analysis tools that may be used within this methodology and their associated level of effort.

Requires Less Quantitative Analysis	Requires More Quantitative Analysis
• Fractile Method	• Probability Distributions
• Triangular Distribution Method	• Statistical Analysis
• Scenario Analysis	• Simulations

Table 23: Quantitative Analysis Effort

7.6.4.1 Fault-tree Analysis

Fault-tree analysis is discussed briefly here as it pertains to the methodology but is illustrated in Chapter 8 within the context of this scenario example. Fault-trees are an analytic and graphical technique, which asks the question, “how could it happen?” It is a principle method used to identify potential system weaknesses within a sequential combination of faults. It is a diagnostic tool for predicting the most likely causes of system failure or system breakdown. The results of the fault-tree analysis allow the analyst to construct the fractals of each policy option by applying the overall measurement (e.g., reliability) to the median value in the fractile.

In fault-tree analysis, the sequence of events leading to the probable occurrence of a predetermined event is systematically divided into primary events whose failure probabilities are estimated [Haimes, 1998]. The system is analyzed to find all credible ways in which an un-favored event can occur. The HHM discussed in Step A.3 plays a

major role in identification of most of the components needed to model within the fault-tree analysis. Influence diagrams and event-tree analysis also assists in identifying and understanding the components. The following steps summarize fault-tree analysis:

1. Specify the un-desired state of the system whose occurrence probability we are interested in determining [Tulisani, 1989].
2. Specify all possible way the state of the system can occur until it is not feasible or cost effective to obtain additional data. Limited availability of data within the analysis is overcome with approximations and subjective estimates of the failure rates by a probability distribution.
3. The events are arranged in a tree representing levels of the tree diagram. The events form relationships between successive levels of the tree connected by “gates.” Figure 38 (Page 143) depicts the most common symbols used for fault-tree and analysis and construction.
4. Determine if the fault-tree should represent discrete or continuous cases.
5. Calculate the probabilities according to the relationships among the events at each step. The failure probabilities may be estimated or analysts may use simulation or numerical methods to approximate a probability distribution.

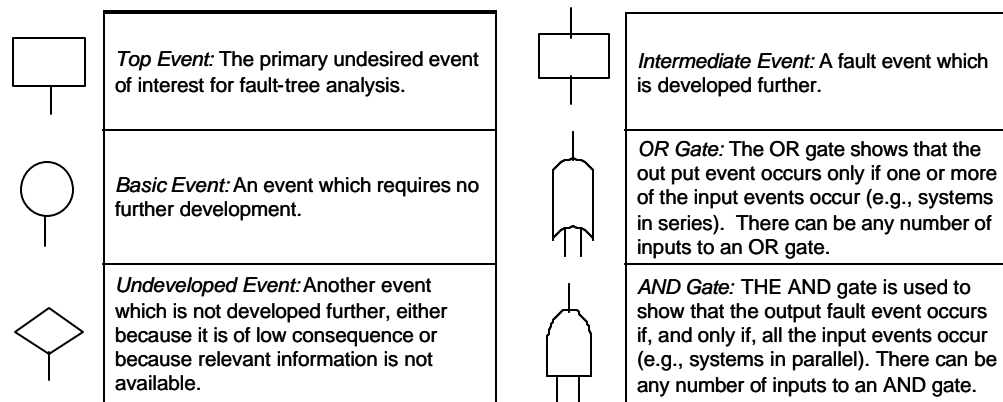


Figure 38: Fault-tree Symbols

There are three important limitations to fault-tree analysis. First, it is possible to overlook a system failure mode yielding an incomplete fault-tree based on gaps in the identification of all risk scenarios associated with the system. Second, it is difficult to

apply Boolean logic to describe some component failure modes when their operation is partially successful [Haimes, 1998]. Lastly, there is a lack of appropriate data on failure modes even if the data is available. This last limitation has the largest impact on IA because human and organizational reliability rates are inaccurate and very sketchy at best. For more information on fault-tree analysis consult Fault Tree Handbook [NRC, 1981].

7.6.4.2 Risk of Extreme Event Analysis

Information assurance incidents (e.g., failures, attacks) are often low-probability events having catastrophic effects within an organization. Decisionmakers not only want to know the expected risk of an IA event but also the expected maximum risk value. Knowing the expected maximum risk and what measures can minimize that risk is a key component of mission accomplishment. Conducting risk of extreme event analysis examines tasks or objectives that increase the risk of the total program and impact on the mission success rate. Organizations cannot afford an IA incident based on the average set of conditions and events because many organizations have gone out of business based on estimating on the average set of conditions. Organizational critical functions cannot be out longer than 4.8 days and if organizations do not recover within 10 days, never recover at all [Sibley, 1997]. Although the military cannot go out of business, information and information systems are tied to the lives of military personnel. Also it is particularly important not to support operations or projects on the average amount of resources. Catastrophic events may occur with organizations that only take the average amount of personnel, equipment and systems. Extreme events are difficult to forecast but with this analysis one will be able to approximate those specific events that might impact the current mission and future operations. This analysis is conducted in conjunction with Partitioned Multi-objective Risk Method (PMRM) [Haimes, 1998].

7.6.4.3 Partitioned Multi-objective Risk Method

Partitioned multi-objective risk method is a risk analysis tool for solving multi-objective problems of a probabilistic nature by analyzing risks of extreme events that represent a low probability of occurrence and a high damage level or consequence. PMRM uses conditional expected values instead of traditional expected values of risk, which equates to f_5 on the damage axis (Figure 39, Page 146). Managing extreme events using “expected values” or the mean can cause catastrophic harm to the system and an organization. Conditional expectation is the expected value of a random variable given that this value lies within some probability range. The PMRM allows decisionmakers the ability to make sound judgments based on the partitioning of the damage axis. The analyst subjectively partitions the axis in order to characterize the nature of the extreme event (e.g., once every year or once every 100 years). Partitioning is tied to a selection of a probability distribution to represent the given data for a specific problem. The general PMRM formulation solves for events that have [Haimes, 1998]:

1. A low severity and high exceedance probability (f_2),
2. A moderate severity and medium exceedance probability (f_3), and
3. A high severity and low exceedance probability (f_4).

We are interested in two parts of the probability axis. The f_5 part (Equation 1) equates to the traditional expected value function and the f_4 part (Equation 2) equates to the high severity and low exceedance probability (Figure 39, Page 146) of an event (e.g., denial of service attack). In this methodology, the fractile method is used as the principle tool to examine the risk of extreme events using PMRM.

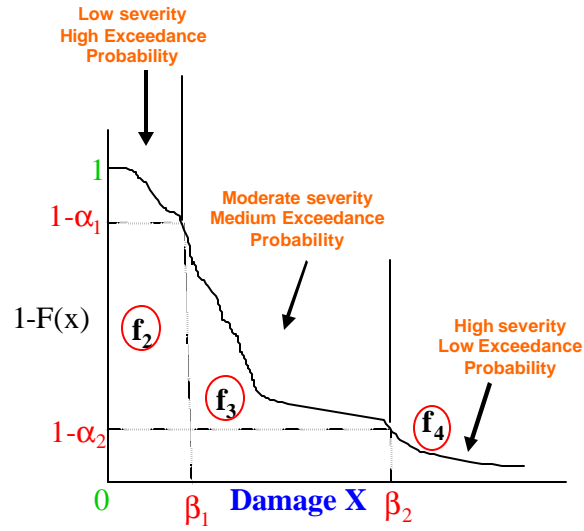


Figure 39: Probability Density Function of Failure Rate Distributions
[Haimes, 1998]

$$E[X] = f_5(\bullet) = \frac{\int_0^{\infty} xp(x)dx}{\int_0^{\infty} p(x)dx} = \int_0^{\infty} xp(x)dx$$

Equation 1: Traditional Expected Value

$$f_4(\bullet) = \frac{\int_{b_2}^{\infty} xp(x)dx}{\int_{b_2}^{\infty} p(x)dx} = E[X | b_2 > X]$$

Equation 2: Extreme Event Conditional Expected Value

7.6.4.4 Fractile Distribution Analysis

Fractile distribution analysis is discussed briefly here as it pertains to the methodology but is illustrated in Section 8.2. Fractile method refers to a method that dissects the [0,1] probability axis into section (fractals) and relates each outcome by soliciting evidence-based assessments from one or more experts [Haimes, 1998]. The major results of the Fractile Analysis are a cumulative distribution function (cdf) [Haimes, 1998], the probability density function (pdf) [Haimes, 1998] and the probability of exceedence (1-cdf). The Fractile method asks the best, median and worst case scenarios, and categorizes the cases as fractals.

Equation 3 and Equation 4 relate a continuous random variable X of damages (e.g., denial of service attack or computer network failure) to the cdf, $P(x)$ and pdf, $p(x)$. The exceedance probability of x is defined as the probability that X is observed to be greater than or equal to x , and is equal to one minus the cdf evaluated at x .

$$\text{cdf: } P(x) = \text{prob}[X \leq x]$$

Equation 3: Cumulative Distribution Function

$$\text{pdf: } p(x) = \frac{dP(x)}{dx}$$

Equation 4: Probability Distribution Function

7.6.4.5 Uncertainty and Sensitivity Analysis

Uncertainty is the inability to determine the true state of affairs of a system [Haimes, 1998] and may represent an environment in which reasonable probabilities cannot be assigned to potential outcomes. This may be a factor of incomplete

knowledge, parameter and decisionmaking variability, and stochastic processes.

Uncertainty arises from two main areas: variability or knowledge each represented by several possible subheadings within the uncertainty taxonomy (Figure 40, Page 148).

Uncertainty *variability* is caused by a fluctuation in of the quality of concern and uncertainty *knowledge* is caused when there is a lack of confidence in the data or population of values. The type and source of uncertainty impact the characterization and the methods we deal with uncertainty. The influence of uncertainty on methodology and perception emphasizes the importance of indenting uncertainty types and sources [Haimes, 1998]. Several facets of IA uncertainty impact model estimations, probabilities, and metrics but acknowledging that uncertainty leads to better risk mitigation.

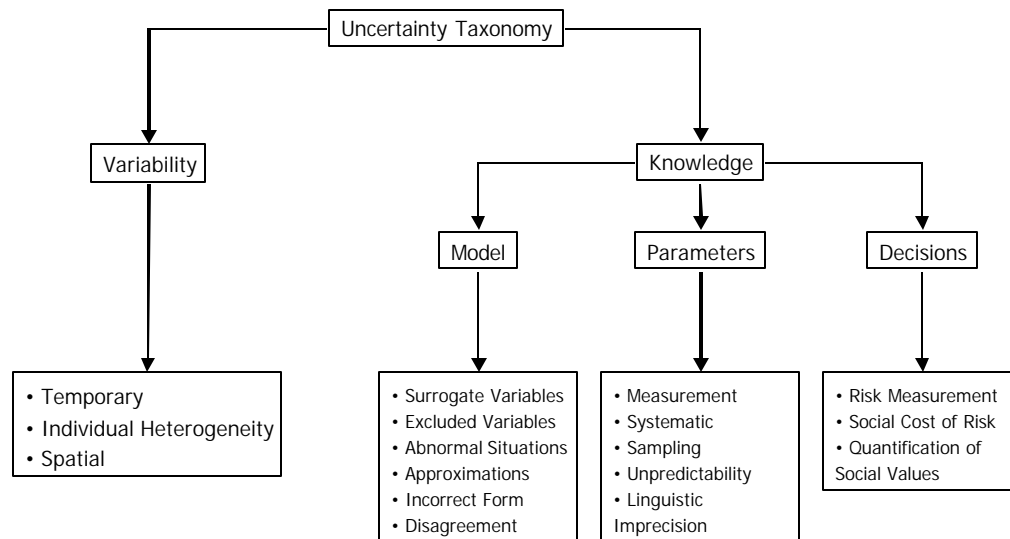
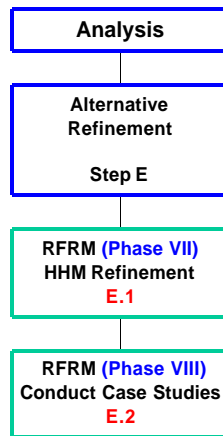


Figure 40: Major Sources of Uncertainty [Haimes, 1998]



7.7 Step E: Alternative Refinement

7.7.1 Step E.1: HHM Refinement

Reducing the initial large set of risk scenarios identified by the HHM to a small number can potentially inadvertently screen out scenarios that were originally minor but with current policy implementation could manifest into important risk scenarios. In this section, we ask and answer the question: “How robust has the policy selection and risk filtering/ranking process been [Haimes et al., 2001c]?” This section provides added confidence and redundancy that the proposed methodology creates flexible reaction plans if indicators signal the emergence of new or earlier undetected critical items. Emerging critical threats and other risk scenarios must not be overlooked in a dynamic and non-linear system (i.e., IA). In order to execute this section successfully, proper bookkeeping from Section B is essential. The major tasks within this section focus on:

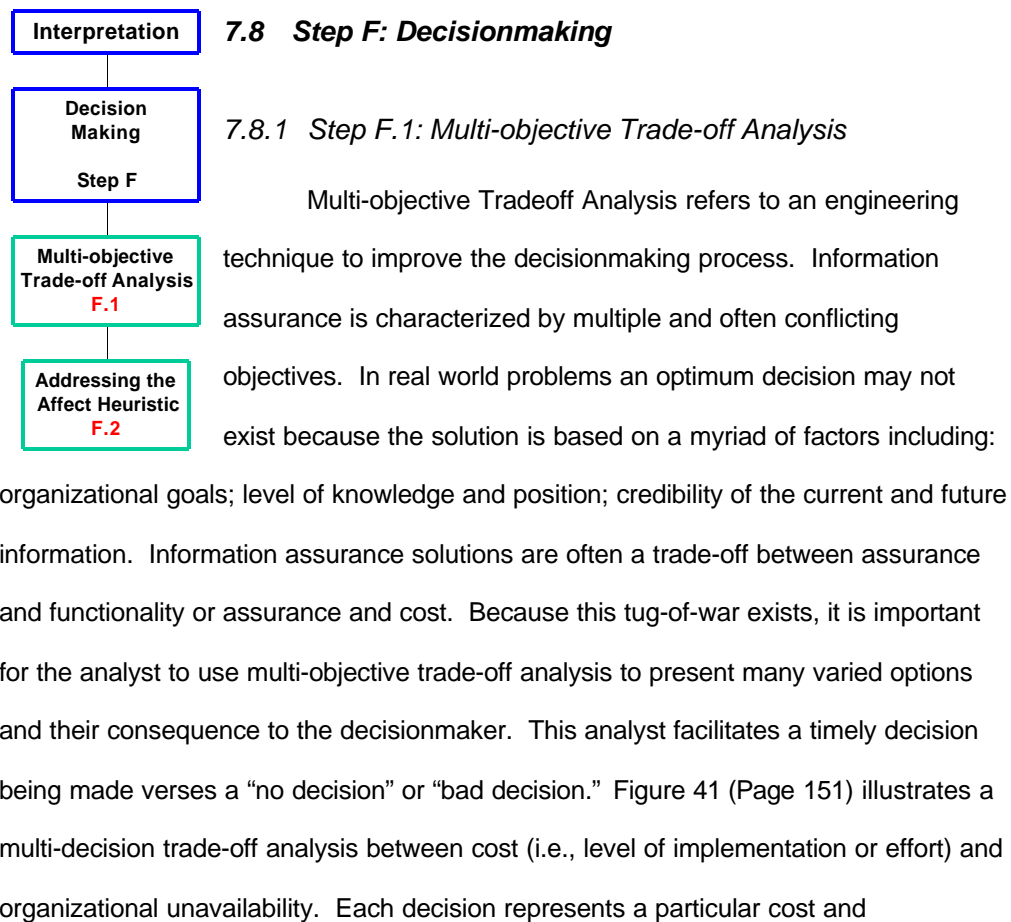
1. Review the intra- and inter-dependencies among the various success scenarios and sources of risk.
2. Determine if any risk management options developed in Step D affect any risk scenarios discarded in Step B.
3. Revise any options based on step 1 and 2 in this section (above). Generate alternative options that were not applied during Step D in light of the new knowledge gained in this section.

The guiding principle in this section focuses on revisiting possible overlooked cascading effects based on the system complexity and the inter- and intra-dependencies found within IA [Haimes et al., 2001c]. It may be necessary to revise the system’s defensive properties (redundancy, resilience, robustness and assurance) addressed in

Section B.2.3 to ensure comprehensive and systematic risk assessment and management. This step is not executed within this thesis.

7.7.2 Step E.2: Information Assurance Case Studies

This step provides a significant contribution to the methodology and therefore, is discussed extensively in Chapter 9 . Case study analysis in general is useful in three ways: 1) providing justification for conducting risk assessment and management within an organization, 2) receiving information about the policy options in place by personnel within the organization, and 3) receiving information about the methodology itself.



organizational unreliability (e.g., Policy Option B). The figure depicts the data on the risk scenario *qualified personnel* taken from Step D. The policy options characterize five different decisions that a decisionmaker or organization might face within this analysis. Multi-objective trade-off analysis assists the decisionmaker in making the best decision with an analytical foundation and the amount of knowledge present.

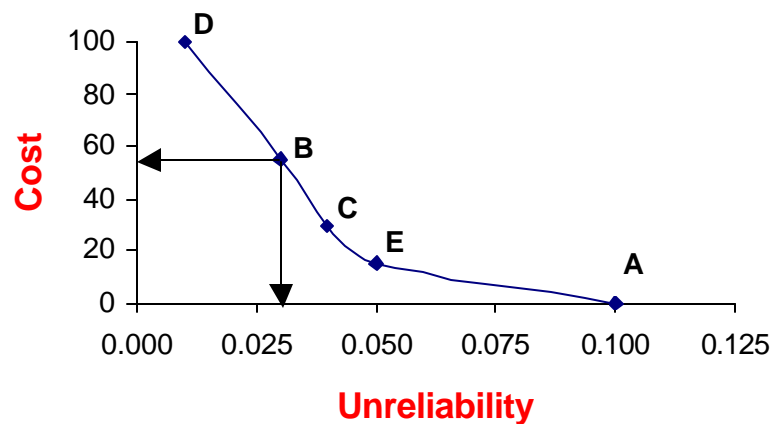


Figure 41: Multi-objective Trade-off Analysis

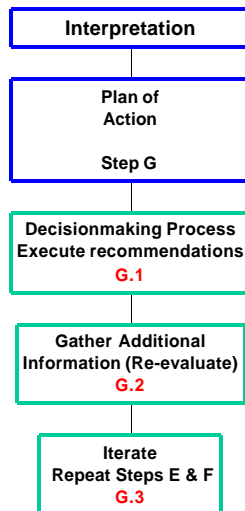
7.8.2 Step F.2: Addressing the Affect Heuristic

Neither the decisionmaking process nor the decisionmakers' preferences can be well understood, evaluated, and possibly improved upon if they are viewed, perceived, and envisioned from a single, one-dimensional perspective [Haimes et al., 2001a]. Any course of action that involves human nature and the component of technology is a complex process within the resource and time constraining organizational environment. System Engineers and analysts have their expertise within systems and quantitative analysis, and not within the behavioral sciences. This step of the methodology gives the analyst some insight that decisionmakers make decisions based on "gut feeling" and not expert evidence. Being aware of a decisionmakers "gut feeling (positive or negative)", the analyst can maximize the effectiveness and usefulness of the quantitative analysis.

Damasio [1994] argues that some guidance from our “feeling is always needed [Haimes et al., 2001a].

The analyst must understand, recognize, appreciate and validate the affect element and emotional dimension of the decisionmaker. Affect refers to subtle feelings of which people are often unaware. Our analytical system of experimentation is not optimally designed to assist decisionmakers to understand the impacts and effects of low-probability, high consequence underlying threats. [Haimes et al., 2001a] Technology has increased our perception of risks and the complexity of risks. Solutions to problems should not only have technology answers but blend intuition, analytical rationality, and coupled with policy, organizational and human solutions. Decisionmakers and engineers do not approach the problem with the same combat tools.

Finucane et al. [2000] argue, “people use an affect heuristic to make judgments.” That is representations of objects and events in people’s minds are tagged to varying degrees with affect [Haimes et al., 2001a].” Information assurance, like many complex, large-scale and hierarchical systems is grounded on the metric of time. Decisions are made quickly under uncertainty with many external factors (e.g., limited resources, organizational, personal) pulling and pushing on the decisionmaker. Time pressure constitutes an important factor and forms a large influence on the affect-based judgment. This section is about understanding the affect heuristic and directing the decisionmaking process toward a balanced approach involving engineering science and behavioral science. In the context of all military operations, staffs must understand the commander’s intent and objectives.



7.9 Step G: Plan of Action

7.9.1 Step G.1: Decision Making Process (Execute Recommendations)

Decisionmakers plan for action based on the recommendations developed in this methodology. Preparation for executing the decision is paralleled with simultaneous processes including conducting additional research and risk assessments, and developing simulations and additional testing methodologies.

7.9.2 Step G.2: Gather Additional Information (Re-evaluate)

In this section any additional information received by the decisionmaker(s) is applied to the methodology to ascertain any impacts to the current decisions.

7.9.3 Step G.3: Iterate (Repeat Steps E and F)

Any decisions and information resulting from this methodology must be updated through an organization's lifetime. New information through research, new technologies, new personnel, and organizational mission modifications are applied through the iterative process of the methodology. The IA Risk Analysis Methodology is a recursive process adapting to the dynamic and complex nature of IA. This section specifically focuses on repeating Steps E and F of the IA methodology but can include identifying additional risk scenarios (Step A), adjusting filtering and ranking attributes or methods (Step B), and modeling or metric reevaluation (Steps C and D, respectively).

Chapter 8 Fault-tree Analysis and Fractile Distribution Method Analysis

The goals of this chapter are to illustrate fault-tree analysis and fractile distribution method in conjunction with Risk of Extreme Events and PMRM as tools within the methodology in order to quantify the risks associate with IA systems. The risk scenario *radio communications* that remained after filtering form our analysis in Chapter 7 acts as a conduit to conduct the goals of this chapter. The data is fictitious and is used to illustrate the methodology as a “prototype.” Data for fault-tree analysis may be obtained using expert evidence, statistical and historical data and simulations.

8.1 Fault-tree Analysis

The fault-tree analysis of the division command operations network serves as an example to evaluate and measure the generated policy options and risk mitigations of Step D within the IA methodology. Fault-tree analysis within this methodology must account for the various policy options, which may have human, organizational, and technology components.

8.1.1 Problem Definition

Radio communications within military operations and exercises is a critical command and control information system. Radio communications is a broad topic within the Army and the fault-tree analysis focuses in on the division's command operations net. The command operation net is a frequency modulation radio system transmitting and receiving in the 30-88 Megahertz range and primarily uses the Single Channel Ground Airborne Radio System (SINCGARS). Figure 42 (Page 155) lists the typical command operations network formed at the division and brigade level, which is used

primarily to control forces, and transmit and receive reports that require immediate dissemination and mass distribution. It is an essential component of C4ISR elements. The net control station acts as the focal point to control the stability of the network and issue guidance when necessary.

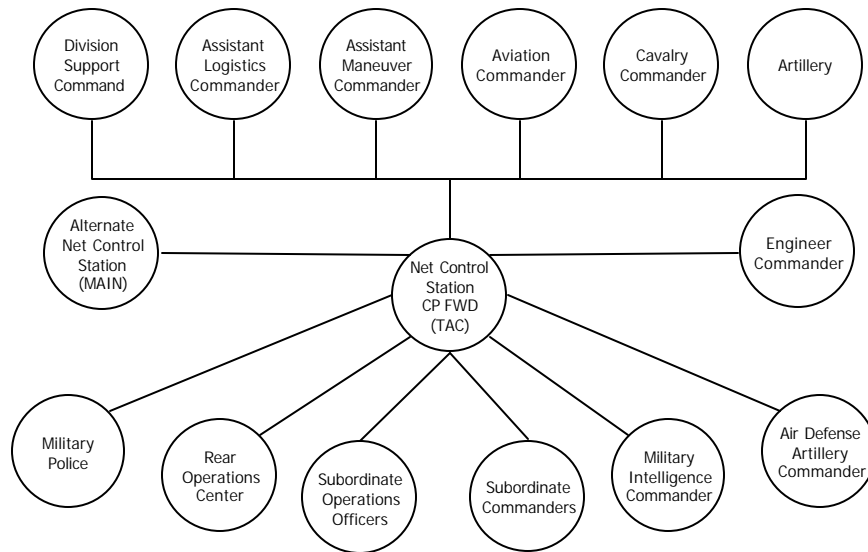


Figure 42: Command Operation FM NET [FM 11-32, 2000]

Figure 42 is transformed into a configuration hierarchy of units, which is interpreted with fault-tree analysis. The analysis is helpful in assuring information and improving the trust within information systems used in large architecture schemes that have several error or fault points (e.g., human, organizational, and technology).

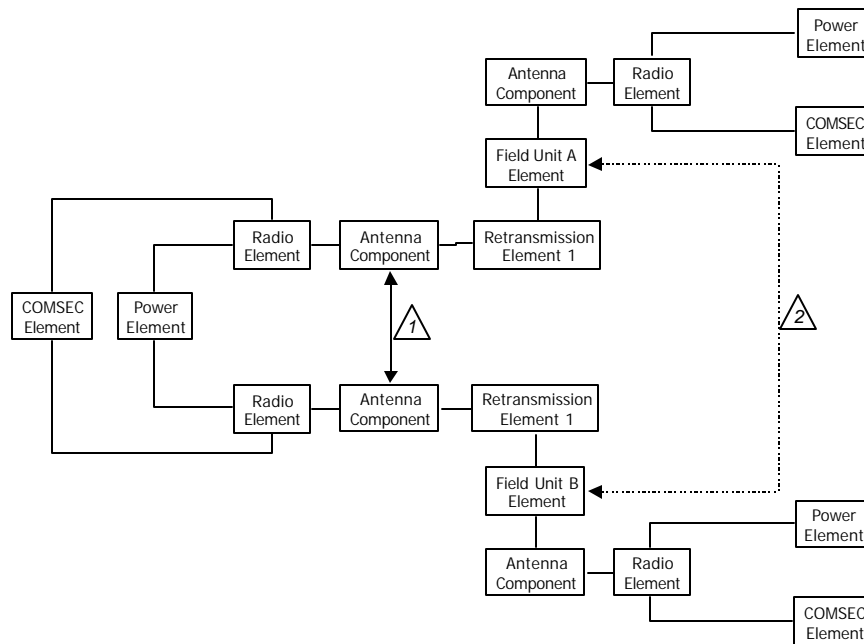


Figure 43: Radio Net Configuration Example 1

Figure 43 illustrates one possible radio net configuration or hierarchy of units for a division. In this configuration, a retransmission element serves as a relay station between two units. A retransmission element contains two radios, two antennas, one power source and one communications security device (referred to as COMSEC). Although the retransmission element has the ability to run on alternate power, i.e., vehicular power, this is considered only a short-term solution. We assume that the power generation unit is the prime power mechanism. We also assume that Field Unit A and B require the retransmission unit due to terrain, weather, or distance constraints, which is depicted by triangle 1. Triangle 2 depicts an alternate means for direct communication between the two field units, by passing the retransmission element.

Figure 44 is a varied radio net configuration based on the need of two retransmission elements. Finally, Figure 43 and Figure 44 are transformed into fault-tree

diagrams representing each policy option generated by the project team. A development of the fault-tree process begins in Section 8.1.3.

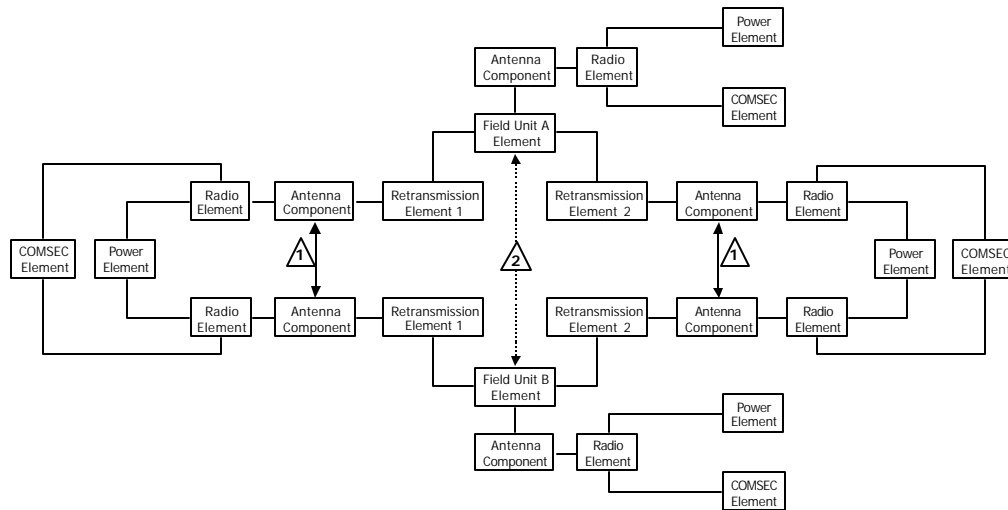


Figure 44: Radio Net Configuration Example 2

8.1.2 Reliability

Reliability ($R(t)$) is used to measure the operational rates of the radio network in the fault-tree analysis. The reliability of a system is defined as the conditional probability that a system performs correctly throughout a specified interval of time $[t_0, t]$, given that the system was performing correctly at time t_0 [Johnson, 1989]. Reliability is a critical IA metric and discussed in Chapter 6 Information Assurance Metrics. Other metrics may be used to measure the differences in policy option, e.g., percent downtime, availability, percent damage, or loss of trust on the system or organization.

Unreliability ($Q(t)$) is the probability that the system fails during interval of time $[t_0, t]$, given that the system was performing correctly at time t_0 [Johnson, 1989].

Information assurance metrics are interwoven within the entire methodology and very important in quantifying objectives (i.e., risk). The mean time to failure is considered as

the reliability rate for all basic events. For example, a 0.995 reliability has an average failure rate of 5%, and a unreliability rate of 0.005.

8.1.2.1 Series Systems

A system fails when subsystems are connected in series (Figure 45) and at least one of the subsystems fails.

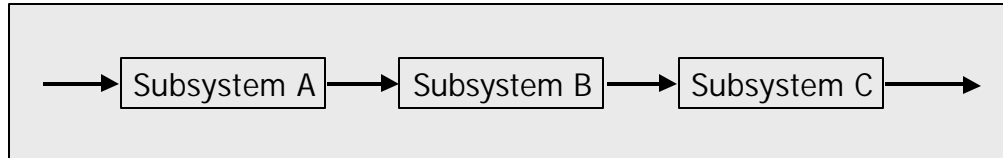


Figure 45: Components in Series

Series components are depicted with an OR gate (sometimes illustrated with a plus sign (+)), which represents the union of the events attached to the gate. Fault-tree analysis is based on Boolean algebra, where the events either occur or do not occur [Haimes, 1998]. Only one subsystem event must occur to cause the event above the gate to occur (Figure 46). Haimes [1998] and Tulsiani [1989] describe fault-tree analysis and its relationship to extreme event analysis but for more information on fault-tree analysis and its applications to engineering consult Fault Tree Handbook [NRC, 1981].

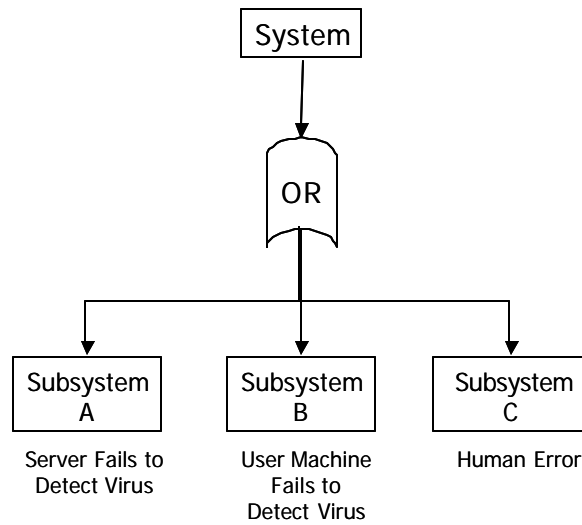


Figure 46: OR Gate

The reliability probability of the total system is equivalent to the product of the reliability of each subsystem (Equation 5).

$$System \ R(t) = R_A(t) * R_B(t) * R_C(t)$$

Equation 5: System Series Reliability

8.1.2.2 Parallel Systems

A system fails when subsystems are connected in parallel (Figure 47, Page 160) and all subsystems fails.

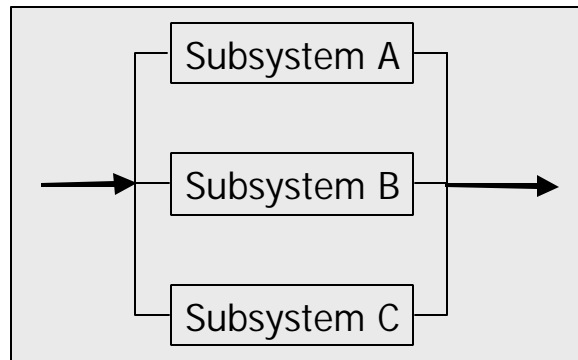


Figure 47: Components in Parallel

Parallel components are depicted with an AND gate (sometimes illustrated with a dot (•)), which represents the intersection of the events attached to the gate. All the subsystem events must occur to cause the event above the gate to occur (Figure 48).

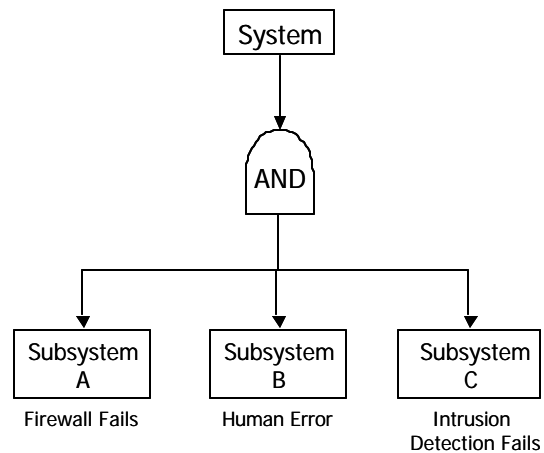


Figure 48: AND Gate

The reliability probability of the total system is equivalent to the one minus the product of the unreliability probabilities of each subsystem (Equation 6). Equation 6 depicts several sub-equations for calculating reliability with AND gates but illustrates the importance of unreliability in the calculations. The equations are grounded on the principle that the system assumes only two phases: operational or failure.

$$\begin{aligned}
 R(t) + Q(t) &= 1 \\
 Q(t) &= Q_A(t) * Q_B(t) * Q_C(t) \\
 \text{System } R(t) &= R_A(t) * [R_A(t) * Q_B(t)] * [R_A(t) * Q_B(t) * Q_C(t)] \\
 \text{System } R(t) &= 1 - [1 - R_A(t)] * [1 - R_B(t)] * [1 - R_C(t)] \\
 \text{System } R(t) &= 1 - [Q_A(t) * Q_B(t) * Q_C(t)]
 \end{aligned}$$

Equation 6: System Series Reliability

8.1.3 Description of each event

The cost of each policy option depends on the scope and size of the operation, and effort of implementing the policy; therefore, a scaled cost function between 0 and 100 is used to demonstrate the use of fault-tree analysis. Policy A (Do nothing) forms the base policy and is assigned a value of zero (Table 24, Page 162).

Policy Option	Policy Description	Cost
A	Status Quo; do nothing. Do not mitigate the risk scenario.	0
B	Conduct division wide radio operator training classes.	15
C	Conduct unit radio operator training classes with division auditing.	50
D	Increase the number of division retransmission elements for the command net. Use parallel retransmission elements to increase reliability.	90
E	Increase the number of division retransmission elements for the command net. Use serial retransmission elements to increase the range of the radio net.	100
F	Centralize radio maintenance on the battlefield	25
G	Decentralize radio maintenance on the battlefield	35
H	Policy Option C and F.	45
I	Policy Option C and G.	65

Table 24: Radio Net Policy Options

This particular problem has a total of 14 events containing four levels. There are 8 intermediate events and five basic event blocks. The top level has three antecedent events connected through an OR gate. The policy options vary the basic events and levels below those antecedent events by modifying the architecture of the figure or modifying the gates through which the events flow. Each policy option represents an iteration of the fault-tree analysis and may depict an improvement or decline in the reliability of the system based on the configuration of the events or the scenario. The events are numbered (1-14) from top down where events on the same level are numbered left to right, and repeating events are not numbered more than once. A detailed description and a list of assumptions for each event are given starting in Section 8.1.3. Fault-tree diagrams for the remaining policy options are illustrated in Appendix B.

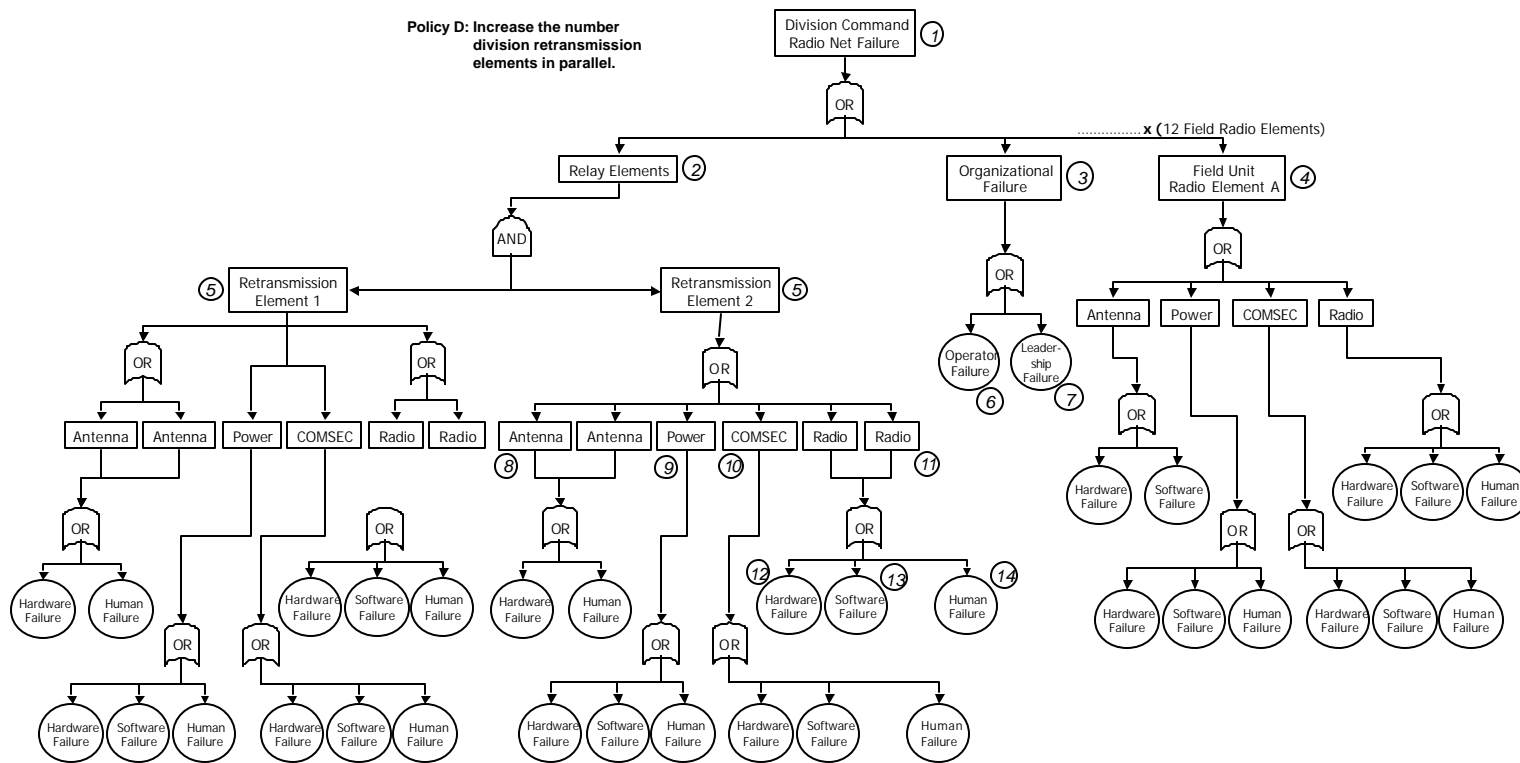


Figure 49: Fault-tree for Policy Option D

8.1.3.1 Event 1: Division Command Radio Net Failure

This is the top event and occurs when any one of the three antecedent event acting through an OR gate occur. This event covers the failure of the division command radio network and occurs when one field unit cannot communicate within the network for more than 2 hours.

8.1.3.2 Event 2: Organizational Failure

The intermediate event occurs when operator or leadership failures occur within the organization. These failures have a significant impact on IA and consist of logistic errors, network architecture errors, resource allocation errors, and maintenance errors.

8.1.3.3 Event 3: Relay Elements

This intermediate event block addresses the failure of retransmission elements within the network. The relay elements are critical components in adding robust, reliable and available communications. The retransmission elements are connected to the relay element through a gate if the policy option contains two retransmission elements, otherwise the gate is removed and the reliability rates (e.g., policy option A, B, C, F, G, H and I) are the same.

8.1.3.4 Event 4: Retransmission Elements

This event occurs when any one of the four antecedent events (i.e., antenna, power, COMSEC, and radio) occurs. Retransmission elements extend range to field units outside the normal communication radius, provide area coverage to field units not in line-of-sight of other field units based on terrain or weather, and provide robustness

and reliability to the total network. The antecedent failures are hardware, software or human failures.

8.1.3.5 Event 5: Field Unit Radio Elements

This intermediate event block addresses the communication failure of any field unit within the network. In this example, 12 units are considered active subscribers and communication failure of any one unit for more than two hours initiates the event.

8.1.3.6 Event 6: Operator Failure

This basic event covers an operator or user error impacting the organization and the radio network. For example, communication operators may issue incorrect frequency ranges for field units or retransmission elements.

8.1.3.7 Event 7: Leadership Failure

This basic event covers leadership failures impacting the organization and the radio network. For example, lack of supervision during maintenance of critical communication components impacts the reliability of the network.

8.1.3.8 Event 8: Antenna

This intermediate addresses one of the critical components within the network. The antenna component covers all mechanical elements (e.g., cables, connectors) that allow units to transmit and receive information. This antecedent failure event occurs due to hardware and human failures.

8.1.3.9 Event 9: Power

This intermediate addresses the critical component of power generator or batteries to run radios. Operational radios and a radio network require power generation or batteries. This antecedent failure event occurs due to hardware, software, and human failures.

8.1.3.10 Event 10: COMSEC

This intermediate covers communication security, commonly referred to as COMSEC. The division radio networks operate securely based on a 128-bit cryptographic key used to secure transmission between field units, which is stored in a COMSEC device. This antecedent failure event occurs due to hardware, software (i.e., cryptographic algorithm) and human failures (i.e., improper key distribution and management).

8.1.3.11 Event 11: Radio

This intermediate covers the critical component and the nucleus of the network. Other components provide support functions for the radio at each field unit and retransmission element. This antecedent failure event occurs due to hardware, software and human failures (i.e., improper radio operator training causing reliability problems).

8.1.3.12 Event 12: Hardware Failure

This basic event addresses hardware failures related to the radio network and is an antecedent event for all components in the retransmission and field unit elements. For example users may not conduct maintenance on the radio, power unit or antenna elements causing an increase in radio failures or radio unreliability.

8.1.3.13 Event 13: Software Failure

This basic event addresses software failures as a major failure component in the radio network. This event is an antecedent event for all components in the retransmission and field unit elements except for the event *antenna*. For example software failures in the radio may cause a degradation of signal, which increases radio and network unreliability.

8.1.3.14 Event 14: Human Failure

This basic event addresses human failures related to the radio network and is an antecedent event for all components in the retransmission and field unit elements. This is a critical component of IA and causes a majority of network failures.

8.1.4 Policy Option Designs

A total of nine fault-tree design options corresponding to the generated policy options (Table 24) are considered for this scenario. The objective of the data (reliability probabilities) is to demonstrate the applicability of the methodology; therefore, effort in data collection is not expended. The policy options are not inclusive but form a framework for the analyst and decisionmaker to conduct quantitative analysis. Another objective for conducting fault-tree analysis is to provide a means to mitigate the risks associate with an event. For instance, the organization may decide to allocate resources in order to increase the reliability of the radio components by conducting random maintenance checks prior to the exercise. The overall system reliability then forms multi-objective trade-off analysis in section 8.1.5.

Within this example, antenna and radio events appear twice because of their redundancy capabilities. We assume antenna and radio reliability probabilities are independent but equal for the retransmission elements. Also, we assume 12 field units are in the radio network and their reliability probabilities are independent but equal. The total system reliabilities are a function of only two field units based on the problem definition. We also assume that there is a correlation between hardware reliability rates for the different components (i.e., antenna, power, COMSEC and radio) although sub-organizations affect the reliability rates differently. The organization assigns *software* a 0.98 reliability rate across all policy options (normalizes the basic event) because the organization feels that it has not played a part in recent exercises.

Table 25 (Page 171) represents the subjective reliability probabilities for the intermediate events, and basic events for the nine policy options. These reliability rates are used to calculate the total reliability rate for each fault-tree diagram. Each policy option represents a reduction or increase in the basic events of the fault-tree diagram. For example, policy B increases the reliability of the human and hardware basic events by 4% and 3%, respectively through large-scale training sessions within the organization. The organizational reliabilities are increased by 7.7%.

Policy C increases the human and hardware reliabilities for all radio components by improving the training aspects within the organization. Small unit training affords better quality training sessions and improves on the reliability values in Policy B. The human and hardware reliability rates increase by 7% from the base policy (Policy A).

Policy D and E are variations of Policy C. Policy D adds an additional retransmission element in parallel to improve the radio net reliability. Policy E adds an additional retransmission element in series to extend the range of the radio net.

Policy F and G improve the aspect of maintenance and the locality of organizational maintenance elements. Policy F considers centralizing maintenance on

the battlefield, which increases the human and hardware reliabilities for components by fixing and maintaining non-operational components within the organization. The human and hardware reliability rates increase by 4% and 2%, respectively from the base policy (Policy A) for Policy F. Policy G considers decentralizing maintenance on the battlefield and further increasing human and hardware reliability rates. Decentralizing maintenance affords better reliability by dispersing experts and resources throughout the organization. The human and hardware reliability rates increase by 6.6% and 7.5%, respectively from the base policy (Policy A). Human and hardware reliability rates are reduced for organizational events because of the lack of training aspects for Policy F and G.

Policy H and I are variations on Policy C and combine the aspects of individual unit training with division auditing and maintenance locality. Policy H assumes a reduction in hardware reliability rates from Policy C by decentralizing maintenance by 1.5%. Policy I increases human and hardware reliability rates by 0.03% and 2.3%, respectively from the Policy H. Policy I improves organizational basic events (i.e., operator and leadership) reliability rates by 0.05% over Policy H and 9.5% over the base policy (Policy A).

Figure 50 (Page 170) represents the reliability rate designs for all policy options but only captures values for four basic events. The basic events are depicted in the following order (top to bottom) for each policy option: human, hardware, leadership and operator.

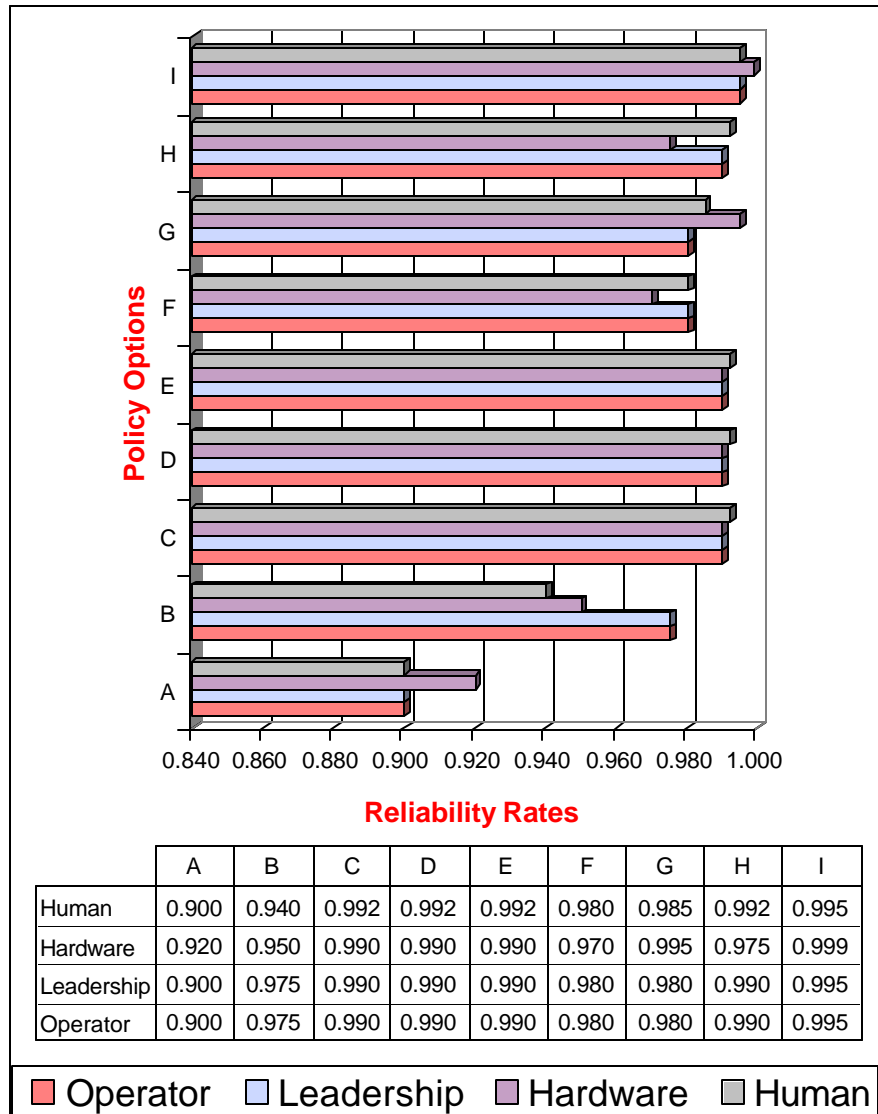


Figure 50: Reliability Rate Design

Intermediate Event	Basic Event (Failures)	Policy Options								
		A	B	C	D	E	F	G	H	I
Organizational	Operator	0.900	0.975	0.990	0.990	0.990	0.980	0.980	0.990	0.995
	Leadership	0.900	0.975	0.990	0.990	0.990	0.980	0.980	0.990	0.995
Antenna	Hardware	0.920	0.950	0.990	0.990	0.990	0.970	0.995	0.975	0.999
	Human	0.920	0.960	0.992	0.992	0.992	0.980	0.985	0.992	0.995
Power	Hardware	0.920	0.950	0.990	0.990	0.990	0.970	0.995	0.975	0.999
	Software	0.980	0.980	0.980	0.980	0.980	0.980	0.980	0.980	0.980
	Human	0.920	0.940	0.992	0.992	0.992	0.980	0.985	0.992	0.995
COMSEC	Hardware	0.920	0.950	0.990	0.990	0.990	0.970	0.995	0.975	0.999
	Software	0.980	0.980	0.980	0.980	0.980	0.980	0.980	0.980	0.980
	Human	0.900	0.940	0.992	0.992	0.992	0.980	0.985	0.992	0.995
Radio	Hardware	0.920	0.950	0.990	0.990	0.990	0.970	0.995	0.975	0.999
	Software	0.990	0.990	0.990	0.990	0.990	0.990	0.990	0.990	0.990
	Human	0.900	0.940	0.992	0.992	0.992	0.980	0.985	0.992	0.995
Total System Reliability		0.057	0.180	0.647	0.748	0.547	0.402	0.617	0.523	0.774

Table 25: Reliability Data for Policy Options

8.1.5 Analysis of the Fault-Tree

In the analysis, reliability rates are converted into unreliability rates in order to form a trade-off analysis between cost and unreliability. Table 26 (Page 172) represents the cost, the reliability and unreliability rates for each policy option. The table is sorted (descending) by the unreliability rate.

Policy	Cost	Reliability R(t)	Unreliability Q(t)
E	\$100,000	0.547	0.453
D	\$90,000	0.748	0.252
I	\$65,000	0.774	0.226
C	\$50,000	0.647	0.353
H	\$45,000	0.523	0.477
G	\$35,000	0.617	0.383
F	\$25,000	0.402	0.598
B	\$15,000	0.180	0.820
A	\$0	0.057	0.943

Table 26: Fault-tree Analysis Data

Figure 51 (Page 173) represents the cost and unreliability plot for all policy options. Policy G dominates policy H by having a lower cost function and lower unreliability. Policy I dominates Policy D and E by having a lower cost function and lower unreliability. A policy is selected based on the decisionmaker and the objectives of the organization. Each policy equates to a specific cost or effort and an unreliability rate. This plot may be used in the multi-objective trade-off analysis (Step F of the methodology) to aid decisionmakers.

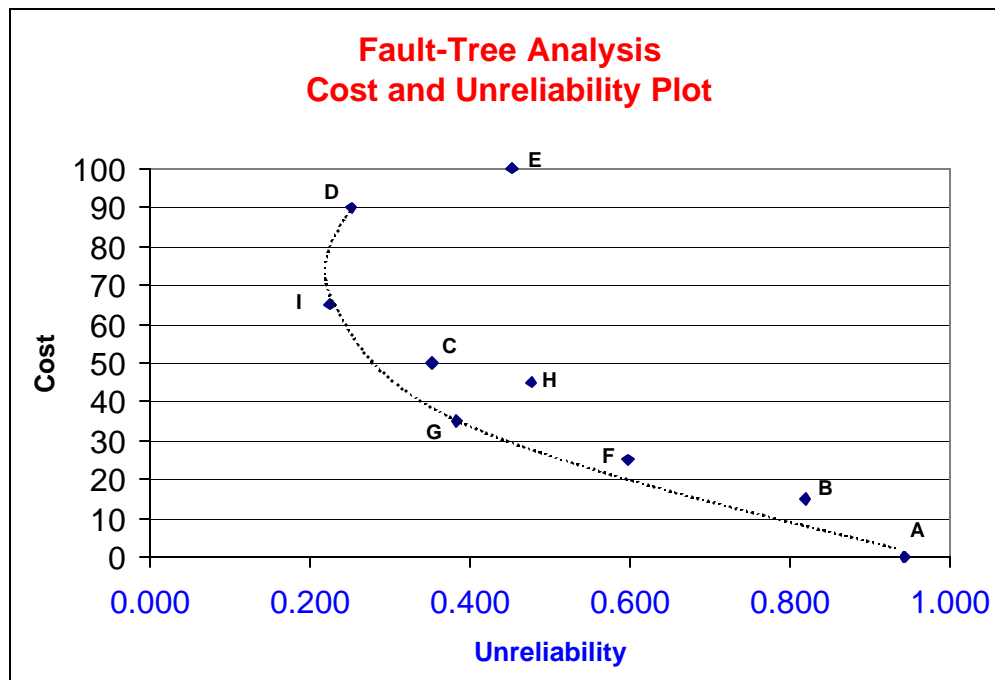


Figure 51: Cost and Unreliability Plot

8.2 Fractile Distribution Analysis

In the previous section, fault-tree analysis is used to compute the expected value of unreliability of the division radio system. The expected value is the mean or the average measure of the parameters specified by the model (i.e., human, hardware, software, and organizational unreliability rates). There are other factors that influence unreliability rates not characterized by fault-tree analysis (e.g., enemy, weather, and terrain). These factors affect the risk scenario in many different ways. Risk of extreme event analysis focuses on low-probability and high severity events rather than medium-probability and moderate severity events, which is based on expected values (mean). This section is necessary because the US Army and other organizations do not plan operations or projects based on expected values. For example, A logistics unit does not plan to bring the average number of rations or ammunition, and military planners do not send the average number of soldiers to execute a mission. Put into IA terms, it is necessary to plan for extreme events with information systems, considering their value within the organization.

The goal of this section is to present a comparison between the traditional expected value (f_5) and the conditional expected value (f_4). The former represents the mean of the policy option and the latter represents the risk of extreme event calculation. Probability distributions represent fictitious data, which generated the fractals in Table 27 (Page 175). Data for this section may be generated by simulation, or organizational, statistical and decisionmaker knowledge about the system. The median values are taken from the fault-tree analysis conducted in Section 8.1.4 and for simplistic purposes the 25th and 75th fractals are calculated as the average between the best and worst case scenarios, respectively.

Policy Option	Policy Description	Best (0)	25th	Median 50th	75%	Worst (100)
A	Status Quo; do nothing. Do not mitigate the risk scenario.	0.7500	0.8464	0.9428	0.9714	1.0000
B	Conduct division wide radio operator training classes.	0.6000	0.7098	0.8195	0.8948	0.9700
C	Conduct unit radio operator training classes with division auditing.	0.2000	0.2763	0.3525	0.4513	0.5500
D	Increase the number of division retransmission elements for the command net. Use parallel retransmission elements to increase reliability.	0.0800	0.1659	0.2518	0.3509	0.4500
E	Increase the number of division retransmission elements for the command net. Use serial retransmission elements to increase the range of the radio net.	0.1000	0.2766	0.4532	0.5166	0.5800
F	Centralize radio maintenance on the battlefield	0.5000	0.5490	0.5979	0.6490	0.7000
G	Decentralize radio maintenance on the battlefield	0.2600	0.3217	0.3834	0.4117	0.4400
H	Policy Option C and F.	0.0800	0.2786	0.4771	0.5636	0.6500
I	Policy Option C and G.	0.0500	0.1378	0.2256	0.2978	0.3700

Table 27: Risk Scenario (Radio) Unreliability Probabilities

To demonstrate the methodology, policy E is used as an example throughout the Fractile Distribution Analysis.

- Worst case of unreliability: 0.1000
- Best case of unreliability: 0.5800
- Median value (equal likelihood of being great than or less than the value; obtained from fault-tree analysis): 0.4532
- 25th percentile is $(0.1000 + 0.4532/2) = 0.2766$
- 75th percentile is $(0.4532 + 0.5800)/2 = 0.5166$

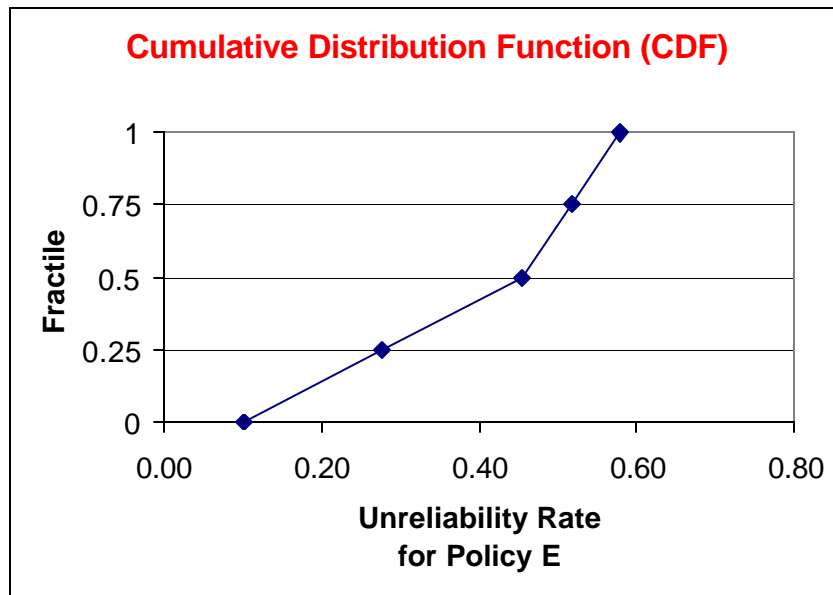


Figure 52: Cumulative Distribution Function for Policy E

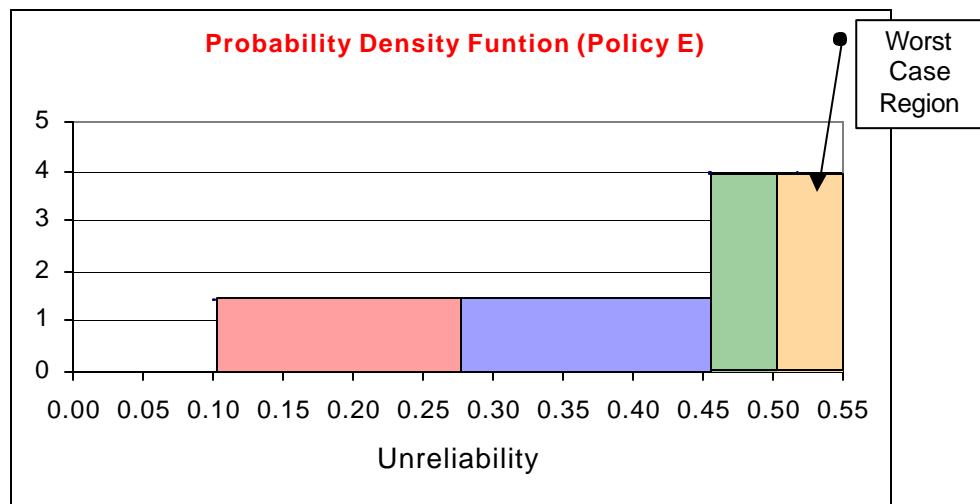


Figure 53: Probability Density Function (Policy E)

Figure 52 and Figure 53 (previous page) depict the cumulative distribution function and the probability density function. In order to illustrate Figure 52, geometry is used to compute the height of each fractile. For example, the height of the first bar is equal to its area (0.25) divided by its base (0.2766-0.1000), i.e., $0.25/(0.2766-0.1000) = 1.4156$. Table 28 represents each fractile and its appropriate base and height. The cumulative probability of the four fractals adds to 1.

Fractile	Cumulative %	Base	Height
1 st	0.25	0.1766	1.4156
2 nd	0.50	0.1766	1.4156
3 rd	0.75	0.0634	3.9433
4 th	1.00	0.0634	3.9433

Table 28: Probability Density Function Statistics for Figure 53

The expected value (f_5) of the unreliability rate is calculated geometrically by using Equation 7. The f_5 values are depicted in Table 29 (Page 178) and an illustration of the f_5 calculation is represented in Equation 8. The f_5 value represents the extreme event measure for each policy option.

$$E[x] = f_5(\bullet) = p_1x_1 + p_2x_2 + p_3x_3 + p_4x_4$$

Equation 7: Traditional Expected Value

$$f_s(\bullet) = 0.25 * \left(0.1000 + \left(\frac{0.2766 - 0.1000}{2} \right) \right) + 0.25 * \left(0.2766 + \left(\frac{0.4532 - 0.2766}{2} \right) \right) + 0.25 * \left(0.4532 + \left(\frac{0.5166 - 0.4532}{2} \right) \right) + 0.25 * \left(0.5166 + \left(\frac{0.5800 - 0.5166}{2} \right) \right) = 0.3966$$

Equation 8: Policy E Traditional Expected Value Calculations

Policy Option	Cost	f_s
A	0	0.9089
B	15	0.7923
C	50	0.3638
D	90	0.2584
E	100	0.3966
F	25	0.6115
G	35	0.3667
H	45	0.4211
I	65	0.2253

Table 29: Cost and Traditional Expected Value

Figure 54 (Page 179) represents a graphical depiction of the cost verses the expected value of the unreliability of policy E.

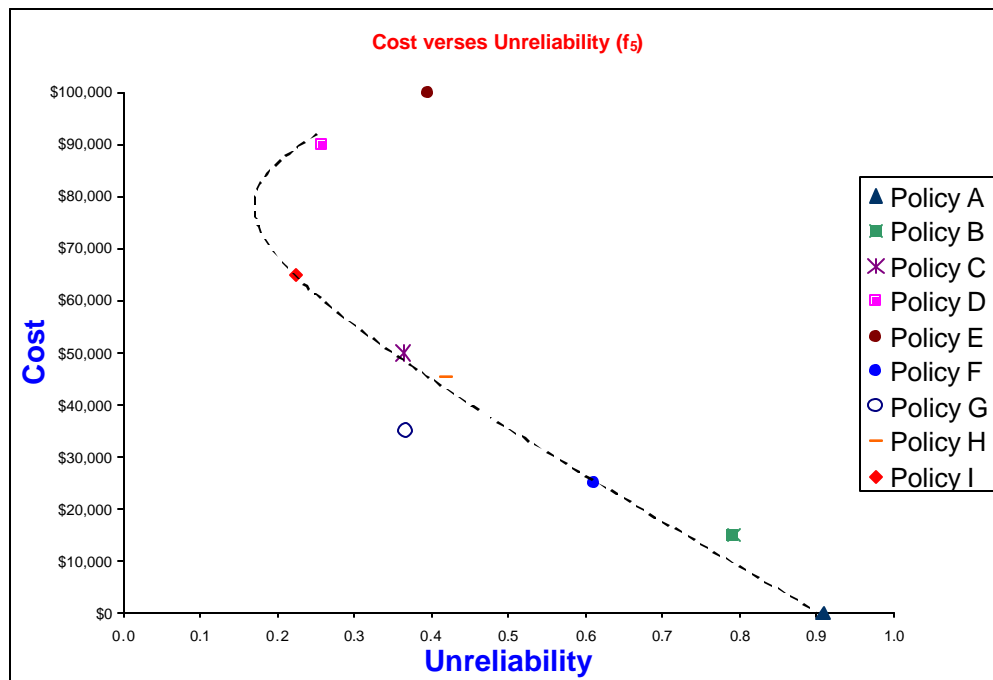


Figure 54: Cost versus Traditional Expected Value (f_5)

The organization is interested in the worst 10% scenario, which signifies the expected value of unreliability, given that the unreliability occurs with a probability of 0.10, or lower. This equates to a partition point on the unreliability axis corresponding to 0.10 or $\alpha = 0.90$. Figure 55 (Page 181) illustrates a geometric means of calculating the unreliability which corresponds to a probability of exceedance (1-cdf) of 0.10 for Policy E and Table 30 (Page 180) depicts the worst 10% scenario for all policy options, labeled as x. In Figure 55, 0.5546 represents the $1-\alpha$ probability exceedance, which is calculated with Equation 9.

$$\frac{x - 0.5166}{0.5800 - 0.5166} = \frac{0.25(1 - a)}{0.25}; a = 0.90$$

$$\frac{x - 0.5166}{0.5800 - 0.5166} = \frac{0.25 * (0.10)}{0.25}$$

$$x = 0.5546$$

Equation 9: Probability of Exceedance at the 0.10 (Policy E)

Policy Option	x
A	0.9886
B	0.9079
C	0.5105
D	0.4104
E	0.5546
F	0.7196
G	0.4287
H	0.6154
I	0.3651

Table 30: Worst 10% Unreliability Calculations for Policy Options

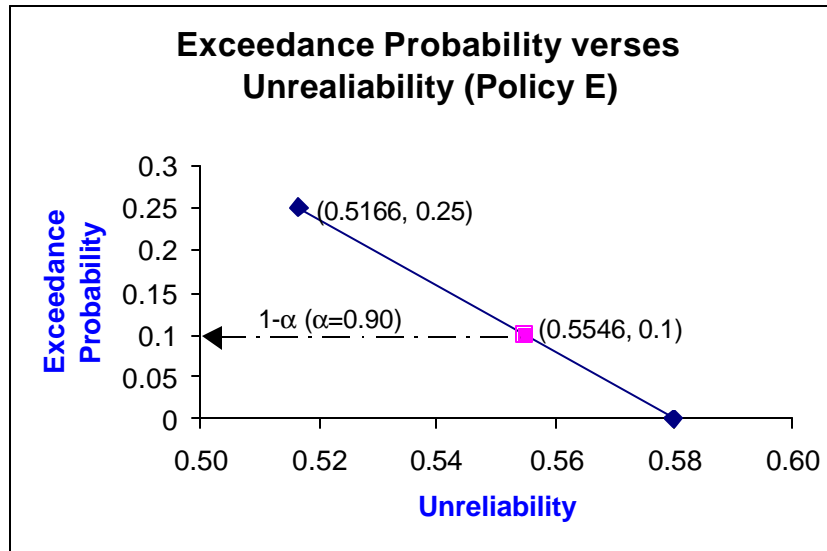


Figure 55: Exceedance Probability and Unreliability Rate for Policy E

The partitioned points computed as the exceedance probability at 0.10 (x) are used to calculate the conditional expected values (f_4) by averaging the exceedance probability and the highest value. Integration can also be used to solve the problem. Both methods are depicted in Equation 10 and Equation 11. Haimes [1998] describes both methods in detail.

$$f_4(\bullet) = \frac{0.5800 + 0.5546}{2} = 0.5673$$

Equation 10: Conditional Expected Value for Policy E

$$f_4(\bullet) = \frac{\int_{0.5546}^{0.5800} xp(x)dx}{\int_{0.5546}^{0.5800} p(x)dx} = \frac{\int_{0.5546}^{0.5800} xKdx}{\int_{0.5546}^{0.5800} Kdx} = \frac{\left. \frac{x^2}{2} \right|_{0.5546}^{0.5800}}{\left. x \right|_{0.5546}^{0.5800}} = \frac{(0.3364 - 0.3076)}{2(0.5800 - 0.5546)} = 0.5673$$

Equation 11: Conditional Expected Value for Policy E by Integration

Table 31 summarizes the results of the fractile distribution analysis and Figure 56 (Page 183) plots conditional expected value (f_4) along side of traditional expected value (f_5).

Policy Option	Policy Description	Cost	f_5	f_4
A	Status Quo; do nothing. Do not mitigate the risk scenario.	0	0.9089	0.9943
B	Conduct division wide radio operator training classes.	15	0.7923	0.9190
C	Conduct unit radio operator training classes with division auditing.	50	0.3638	0.5303
D	Increase the number of division retransmission elements for the command net. Use parallel retransmission elements to increase reliability.	90	0.2584	0.4302
E	Increase the number of division retransmission elements for the command net. Use serial retransmission elements to increase the range of the radio net.	100	0.3966	0.5673
F	Centralize radio maintenance on the battlefield	25	0.6115	0.7348
G	Decentralize radio maintenance on the battlefield	35	0.3667	0.4343
H	Policy Option C and F.	45	0.4211	0.6327
I	Policy Option C and G.	65	0.2253	0.3826

Table 31: Summary of Results for Policy Options

The analysis of Figure 56, Policy Options E, D, C, H and I have a larger risk of extreme events. In the figure, the dotted line represents conditional expected values and the solid lines represent traditional expected values. Using only the expected values, it appears that Policy C and G have similar unreliability rates. If random factors play an increasing part (i.e., enemy, terrain, weather) in the unreliability rates, then the conditional expected value for Policy G is more stable than Policy C and more favorable. Policy options B, F G, and I have the smallest differences between f_5 and f_4 and are the most stable policy option, with policy G having the smallest difference.

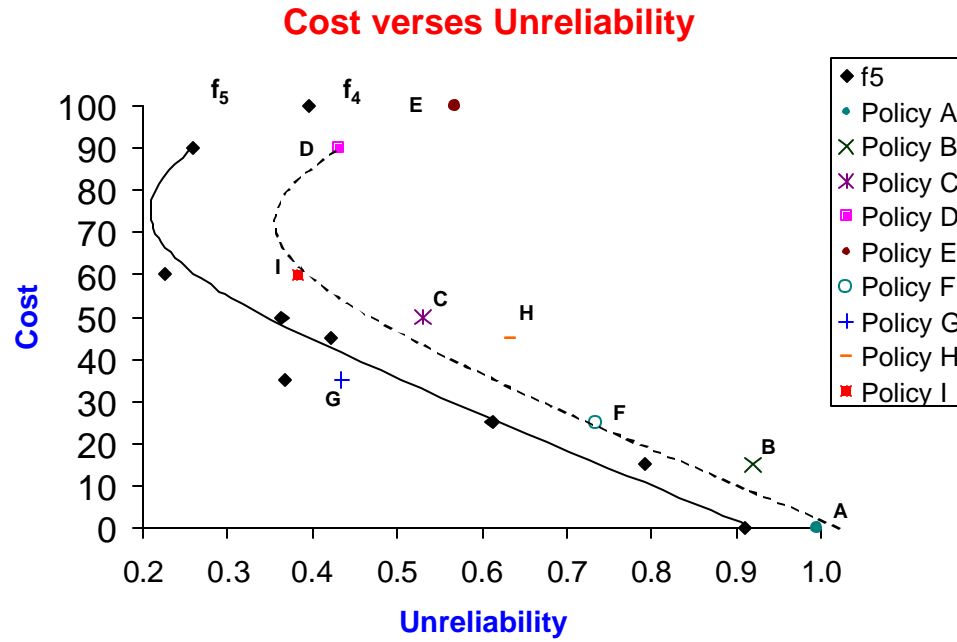


Figure 56: Traditional and Conditional Expected Value Comparison

Chapter 9 Information Assurance Case Studies

9.1 *Introduction*

This section identifies examples of organizations that employ or fail to employ risk assessment measures within the IA spectrum to illustrate proactive risk assessment investment equates to an increase in IA. The case studies verify the suitability of the methodology as a “prototype” for this complex problem, and identify gaps and weakness of the risk assessment process within the methodology. This process analyzes the wealth of statistical data on IA losses due to system failures, to intrusions or to vulnerabilities. Executing a risk assessment and management methodology may save millions of dollars in assets and lost production time. The separate “organizational anecdotes” are converted into valuable statistical information that can further be converted into probabilistic analysis. This analysis adds credibility to quantification of the efficacy of risk management (Figure 57, Page 185) due to the existence of the Heisenberg principle within IA. The results from several organizations are normalized in order to make general comparisons using statistical information.

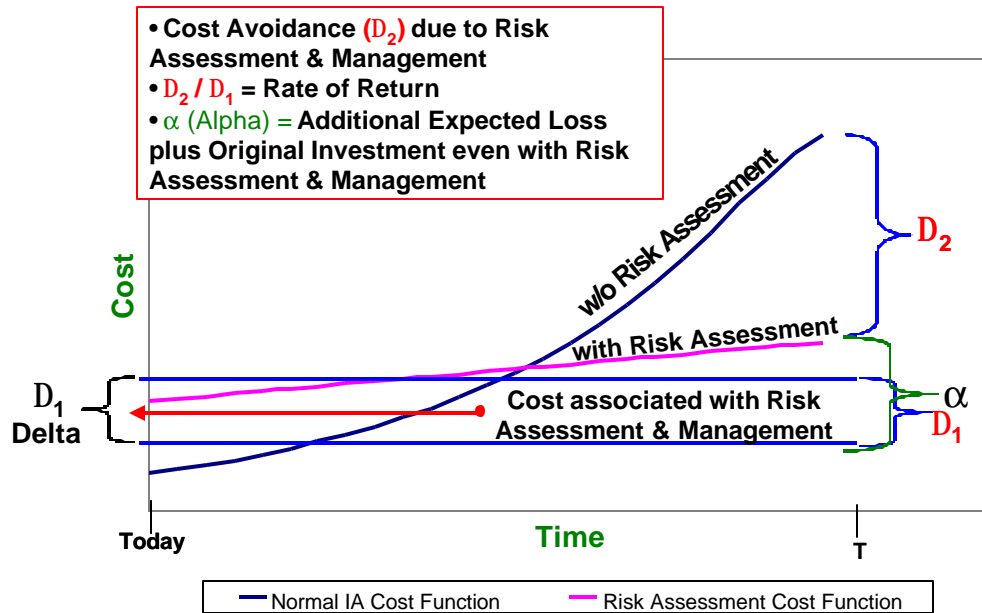


Figure 57: Case Study Analysis

As an example, organization “A” conducts risk assessment and management for \$250,000 and has an increase cost (delta (Δ_1)) compared to organization ‘B’ which did not conduct any risk assessment and management (Figure 57). Over time n-years, organization “B” pays \$1 million in IA related incidents (i.e., failures, attacks, faults) while organization “A” pays \$250,000 in IA related incidents. There is no 100% assurance with any system and therefore, organization “A” pays the initial \$250,000 in risk assessment costs plus an additional \$250,000 in IA related incidents for a total of \$500,000 (shown as Alpha (α) in Figure 57). This section provides in depth statistical data that risk assessment and management saves money, resources and lives (reducing or eliminating delta (Δ_2)).

The methodology is improved based on the feedback and information gathered on several organizations dealing with IA concepts. Data collection from these organizations will improve the overall methodology in several areas:

- 1) New sources of risk may be discovered and applied to the HHM (this is important because the HHM is never thought to be complete) and enhances the robustness of the HHM.
- 2) New benefits, costs, and risks may be discovered which have relevance to the identified organizational policy options in Step D of the IA methodology.
- 3) The organizational information is used to show the risk assessment and management process saves money, resources and lives within the IA spectrum.
- 4) Help the analyst to train the model (i.e., calibrate the parameters) and then test and verify the suitability of methodology.

Table 32, Table 33 and Table 34 (Pages 187 to 189) represent case study material to illustrate the importance of proper risk management. The organizational names are generically defined (e.g., Case A) due to the sensitivity of the information. Some numbers are slightly rounded-off to conceal any organization's identity. Some of the information contained in the tables was researched at CERT/CC with their approval.

Attributes	<i>Scope (Size)</i>	<i>Personnel Strength</i>	<i>Organizational Type</i>	<i>Specific IA Incident Type</i>	<i>Duration of Incident (t)</i>
Cases					
<i>A</i>	Worldwide Production Corporation	~1500+ ⁸	Industry; Production	Computer Network Upgrade	3 Months
<i>B</i>	Local City IPO	<ul style="list-style-type: none"> • 2 FTE⁹ • 13 PTE¹⁰ 	Industry; Small Business	Intrusion (Hacker)	5 Days
<i>C</i>	Global Web-based Service Provider	~1000+	Industry; Web Services	Hardware & Organization Failure (Network Crash)	25 Hours
<i>D</i>	University Assets in 2000: \$4.4 Billion	10,500	Academia; Large	Virus ("I Love You")	2 Days
<i>E</i>	Education Web-based Service	<ul style="list-style-type: none"> • 50 Personnel • 5 UM¹¹ 	Educational Sector	Root Compromise (Hacker)	1 Day

Table 32: Information Assurance Case Study Attributes

⁸ Number indicates approximate personnel values. A plus sign (+) denotes numbers are probably higher than number listed.

⁹ Full-time Employees

¹⁰ Part-time Employees

¹¹ Upper Management

Attributes	Loss Estimates (\$)	Other Impacts	Number of Targets
Cases			
<i>A</i>	\$18 Million (Lost Revenues)	<ul style="list-style-type: none"> • 19% Net Income Loss (yr) • 9% Sales Loss (yr) • Stock Shares Fell (yr) • Increased Freight and Warehousing Costs 	Entire Network
<i>B</i>	\$40,000	<ul style="list-style-type: none"> • Loss of Customers • Insurance Settlement 	1 Computer
<i>C</i>	\$6.1 Billion (Lost Revenues) \$6.6 Billion (Total Losses between two incidents)	<ul style="list-style-type: none"> • \$3-5 million (customer compensations) • \$48 decrease per share (one week) • 4% 1-day drop in share price • \$5 million loss; 26% loss in share price (1-quarter) 	Entire Network
<i>D</i>	<ul style="list-style-type: none"> • \$3,000 Recovery Person hours • 1,500 hours of lost production (\$45,000) • \$0 hardware and software 	<ul style="list-style-type: none"> • User Downtime • System Trust 	<ul style="list-style-type: none"> ▪ 100 workstations ▪ 2500 workstations (partial)
<i>E</i>	\$10,000 (man-hours, 2 people)	<ul style="list-style-type: none"> • Spent 5 days investigating the incident 	1 Multipurpose Server (email, web, etc.)

Table 33: Information Assurance Case Study Attributes (Continued)

Attributes	<i>RA/RM Invested (\$) prior to Incident</i>	<i>Reoccurrence (Yes or No)</i>	<i>Action Taken after Incident</i>
Cases			
<i>A</i>	\$0	N	<ul style="list-style-type: none"> • Risk Assessments • Hired IT personnel to fix the problem
<i>B</i>	\$0	N	<ul style="list-style-type: none"> • Reconstitution • Risk Assessment costing ~\$5,000 • Contracted out to fix the problem
<i>C</i>	\$10 Million ¹²	Y (Lost \$0.5 Million Last Time)	<ul style="list-style-type: none"> • \$14 million spent in redundancy, warm backup sites and disaster recovery assessments • \$40 Million on total architecture and redesign engineering investments
<i>D</i>	Very Negligible <ul style="list-style-type: none"> • Antivirus Software • Training (education) 	Y (Minor Last Time)	<ul style="list-style-type: none"> • Reconstitution • Virus Protection • Alerts and notifications
<i>E</i>	\$5,000 <ul style="list-style-type: none"> • Training (education) 	N	<ul style="list-style-type: none"> • Hired IT personnel to fix and investigate the problem • Some Education about the incident

Table 34: Information Assurance Case Study Attributes (Continued)

¹² There is no actual data on risk assessment and management for this organization. We estimated the invested amount at \$10 million, which equates to a quarter of their total engineering and architecture investments for that organization based on expert evidence.

9.2 Analysis of Case Studies

Table 35 is a summation of the case study results and represents the percent spent on risk assessment prior to and after an IA incident. Percentages within the table are calculated based on a ratio between the amount spent on risk assessment and the amount lost for a particular incident. The table illustrates the case organizations conducted risk assessment and management after an IA incident and in the course of returning their information systems to normal operations. Although the numbers vary greatly, Cases B and E both stated that they believed if some level of proactive risk assessment and management was conducted their losses due to the IA incidents would have been mitigated.

Cases	Percent spent on risk assessment prior to IA incident	Percent spent on risk assessment after the IA incident
A	0%	0.2%
B	0%	12.5%
C	0.15%	0.6%
D	Not enough data	10.42%
E	Not enough data	50.00%

Table 35: Case Study Results

Chapter 10 Conclusions and Future Research

10.1 Conclusions

A methodology is practical if it can be applied easily and aids the decisionmaking process in an acceptable timeframe. The proposed methodology merges two separate engineering processes (United States Military Academy Systems Engineering Design Process (SEDP), and Risk Assessment and Management Engineering Process) to produce a comprehensive and systematic “prototype” to assess and manage information assurance risks. The methodology is adaptable for all organizations and focuses on improving the level of trust between user, and information or system. Information assurance is a multi-dimensional issue and requires a methodology that: 1) identifies all levels of decisionmaking and risk, 2) allows users to manage those levels, 3) allows behavioral and human aspects to emerge during the process, 4) allows users to qualify and quantify the risks and generated policy options for the system, and 5) allows multiple perspectives to attempt to model the entire system.

The US Army engages in a future that is characterized with greater ambiguity and presents unique challenges in IA with an increase in technology reliance for military operations. The methodology contributes to handling current and future uncertainty and risks facing the US Army. The methodology provides the system engineering and the military communities with: 1) an initial HHM that may be adapted to any organization based on their mission and scope, 2) quantitative risk analysis tools which utilize both the mean and extreme event values, and 3) a IA metric taxonomy to generate organizational objectives and system metrics in order to measure the improvement in reducing IA risks.

10.2 Future Research

Joint Vision 2020 is a strategic plan for a large-scale hierarchical system of systems. Information Assurance is a core focus of Joint Vision 2020 in achieving information superiority on the future battlefield. Information systems will play a crucial role in enhancing the capabilities of the military for the next two decades and beyond. As an instructor and researcher at the United States Military Academy, I plan to conduct research within the IA spectrum. My focus consists of improving information assurance modeling, metrics, simulation methods, and automating the IA methodology.

1. Modeling: Construct Leontief [Haimes, 2000b] interconnected and interaction matrices of all C4ISR systems to improve the critical IA measurements (e.g., reliability, availability) of the Army's information networks and decrease the complexity of those networks.
2. Metrics: Improve IA metrics with simulation and scenario testing of Army information networks and products. Research or develop lower and upper bounds, benchmarks for IA metrics.
3. Simulation: Build simulation guidelines that identify potential IA problems and risk of extreme events on C4ISR systems within the Army through the use of simulation software. The simulation results will focus on reducing the risks of information assurance and identify gaps in systems.
4. Methodology: Ultimately, decisionmakers will make the decisions affecting IA and an automated process increases the chance for success when dealing with large, complex and integrated systems. The methodology can be enhanced with the use of decision support tools, and automation to allow users to better and quickly identify and manage IA risks.

Appendix A: Fault-tree Diagrams

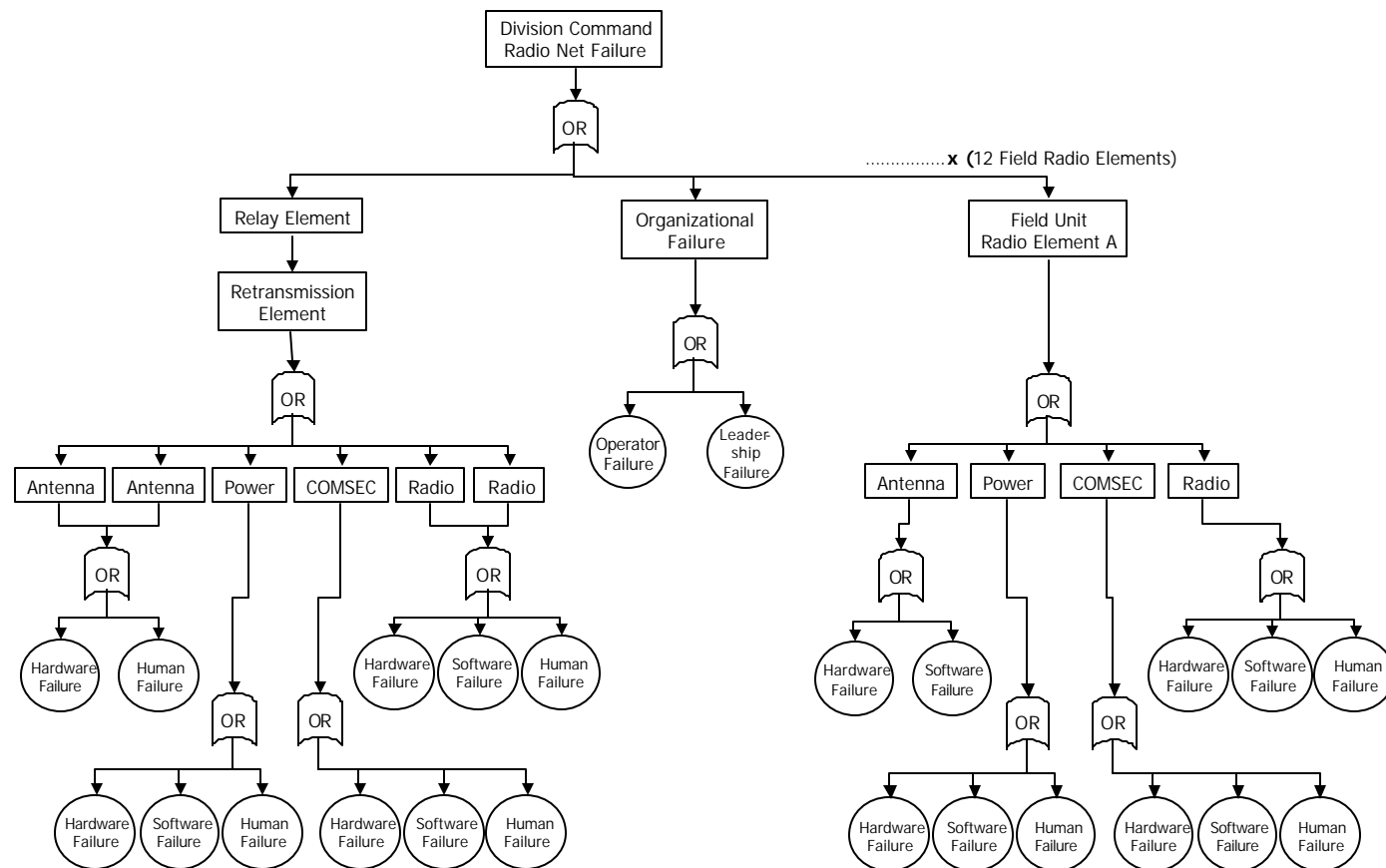


Figure 58: Fault-tree Diagrams for Policy Options A, B, C, F, G, H, and I

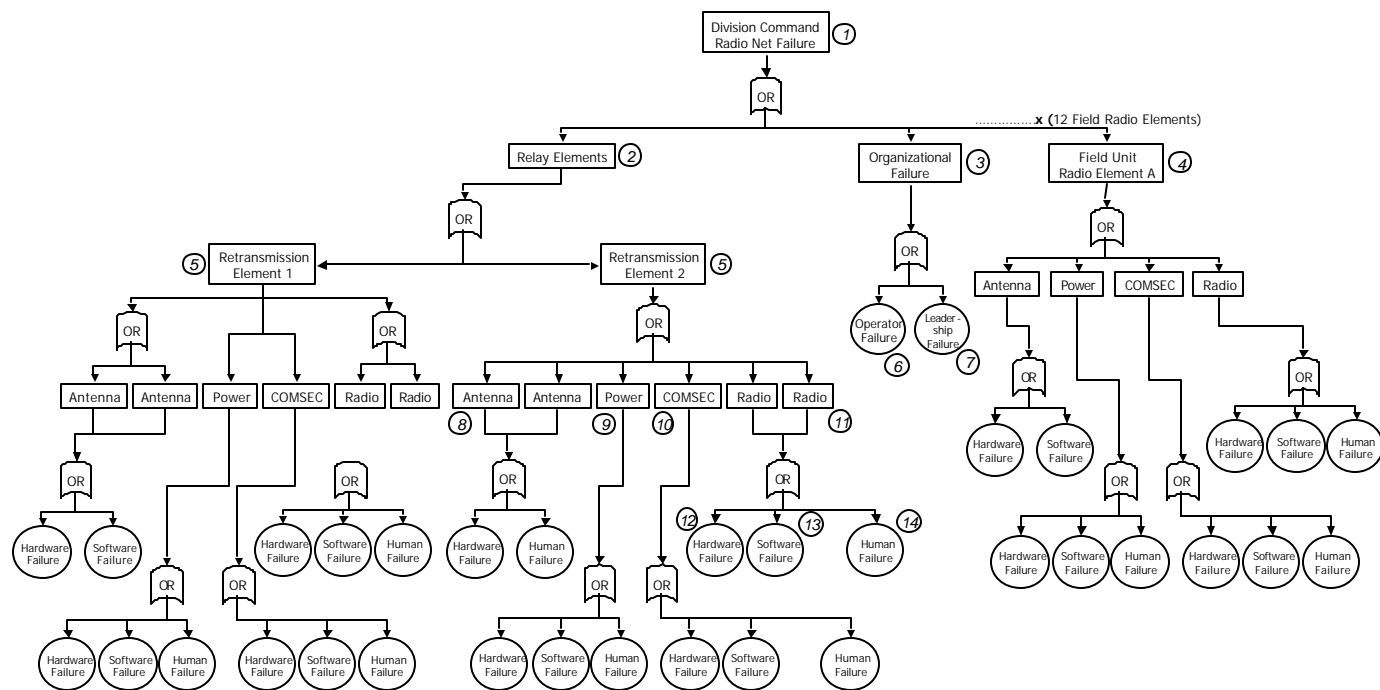


Figure 59: Fault-tree Diagram for Policy Option E

Appendix B: HHM Figures

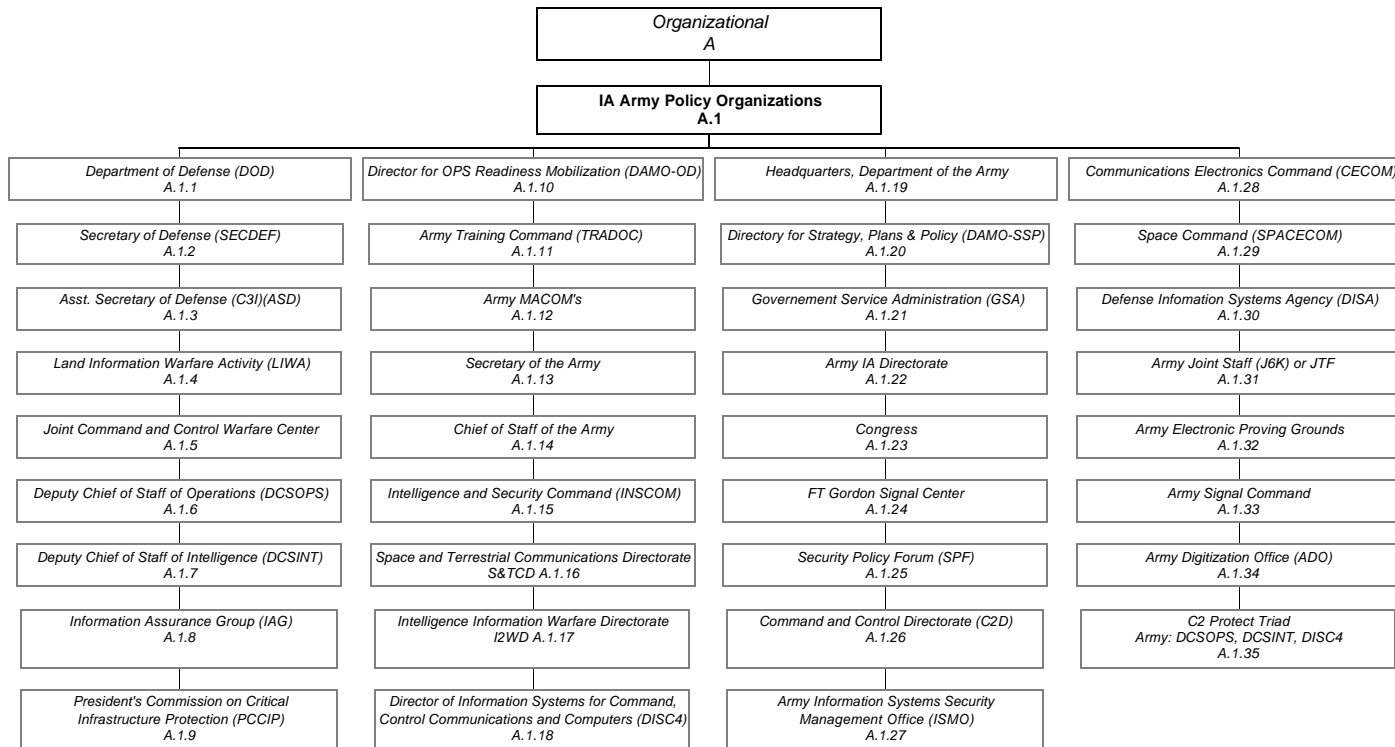


Figure 60: HHM Diagram (Head-topic: A.1)

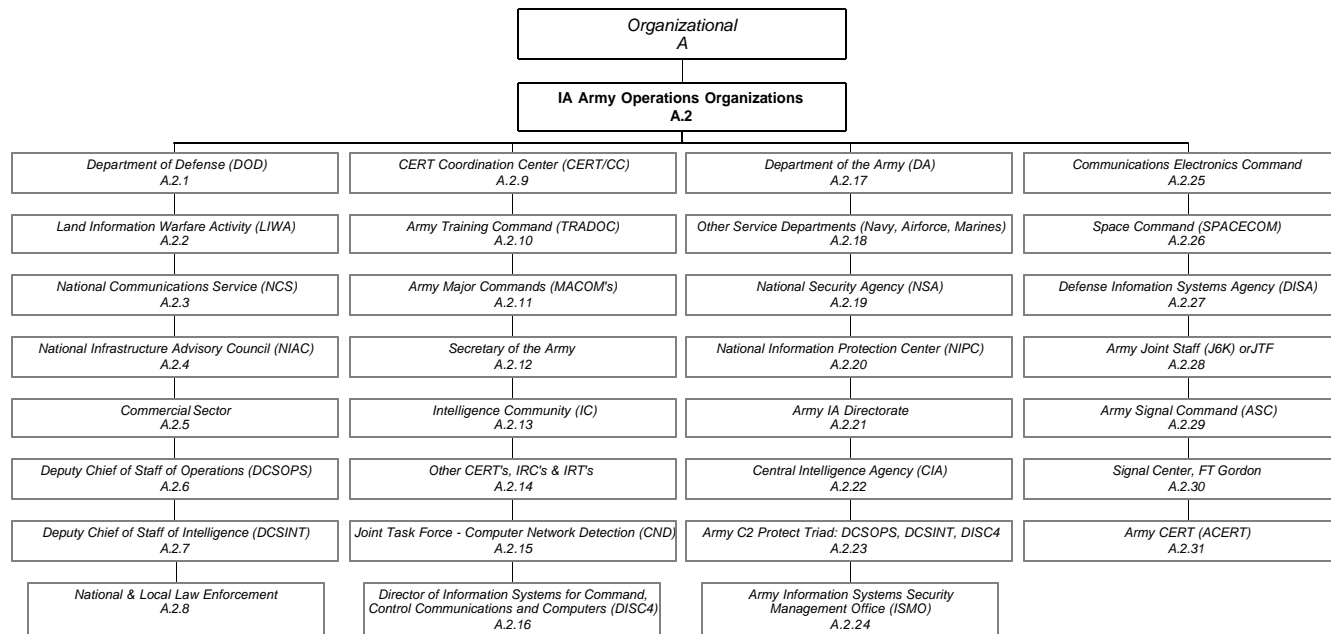


Figure 61: HHM Diagram (Head-topic: A.2)

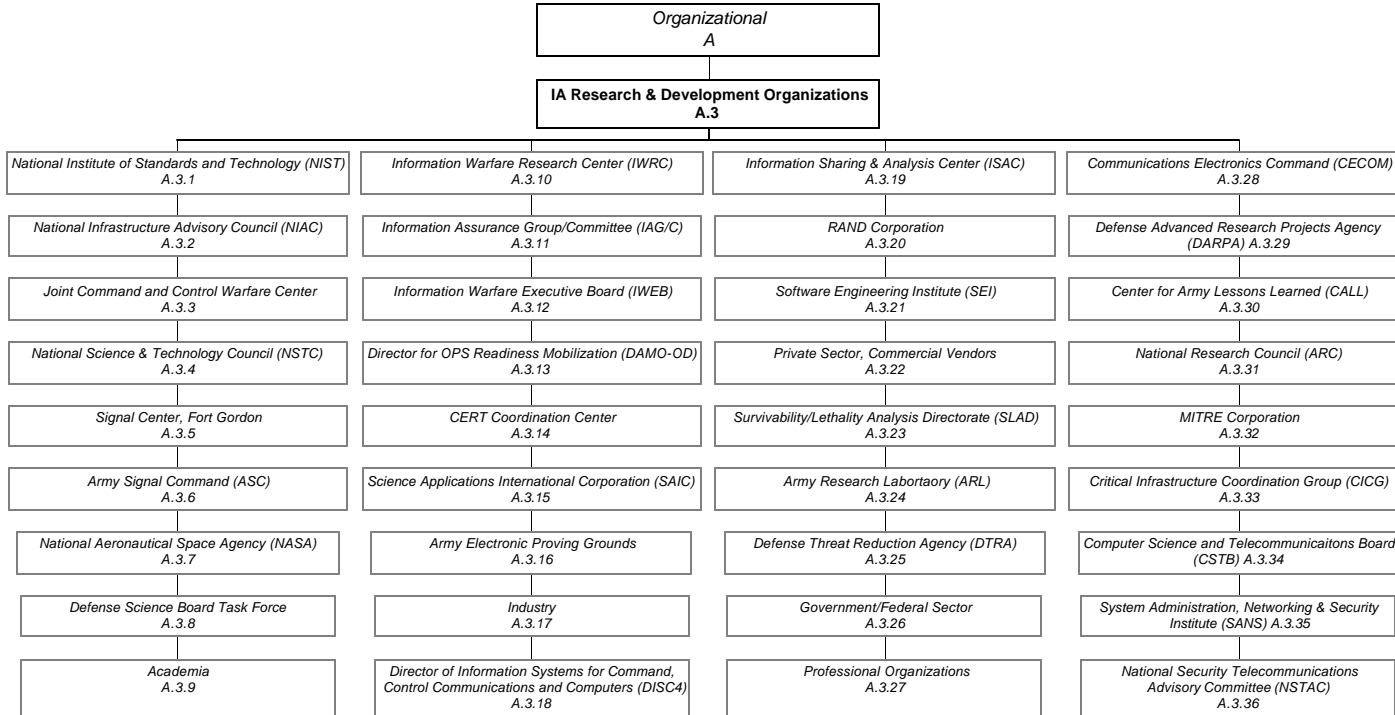


Figure 62: HHM Diagram (Head-topics: A.3)

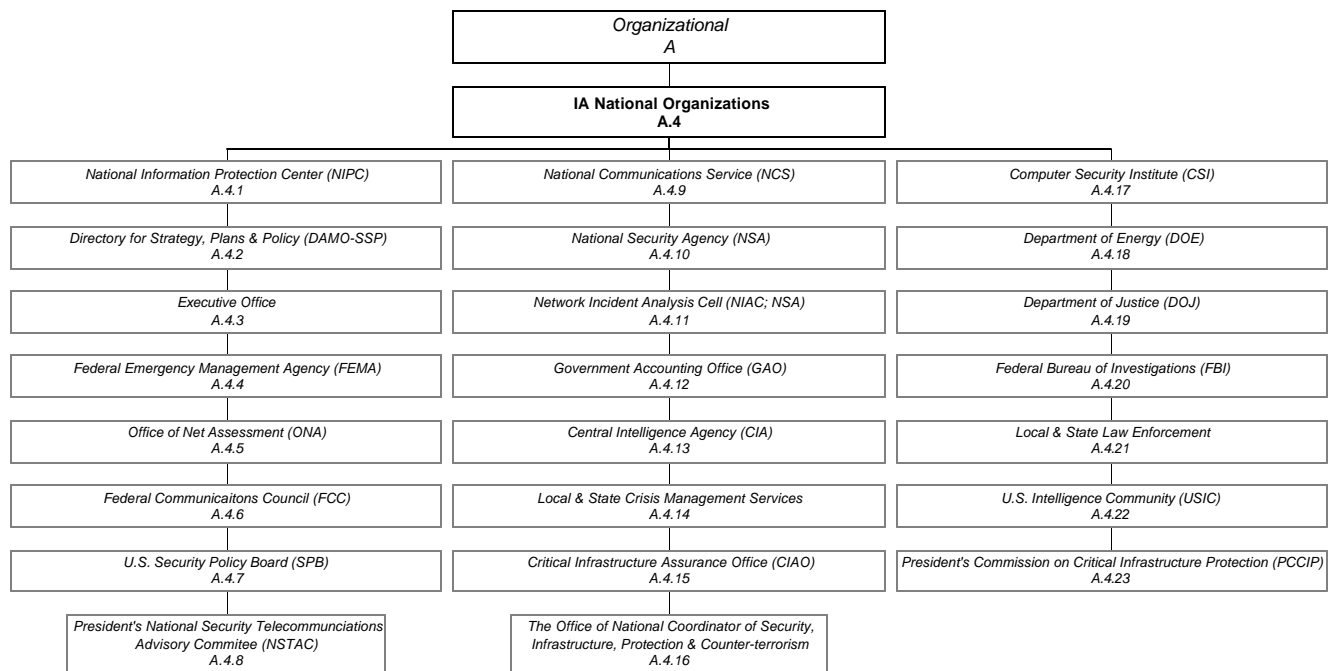


Figure 63: HHM Diagram (Head-topic: A.4)

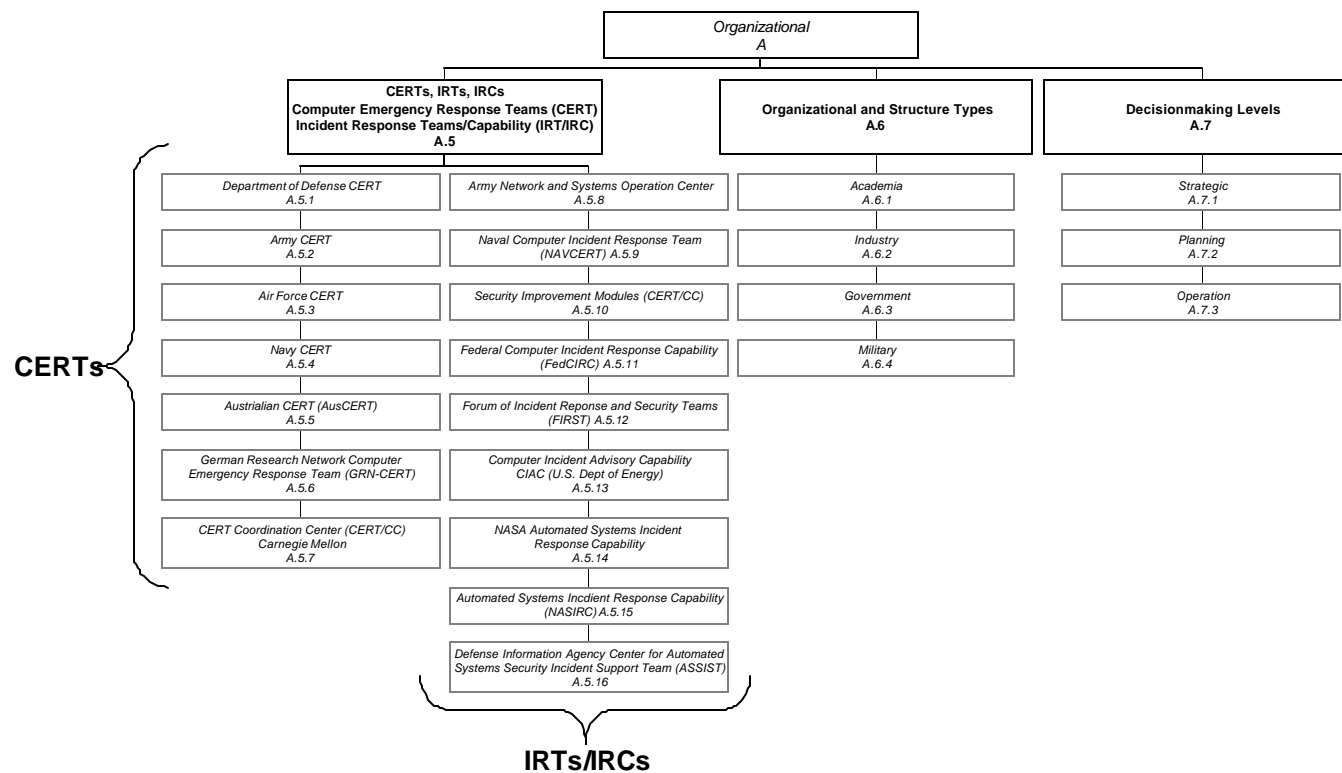


Figure 64: HHM Diagram (Head-topics: A.5, A.6 and A.7)

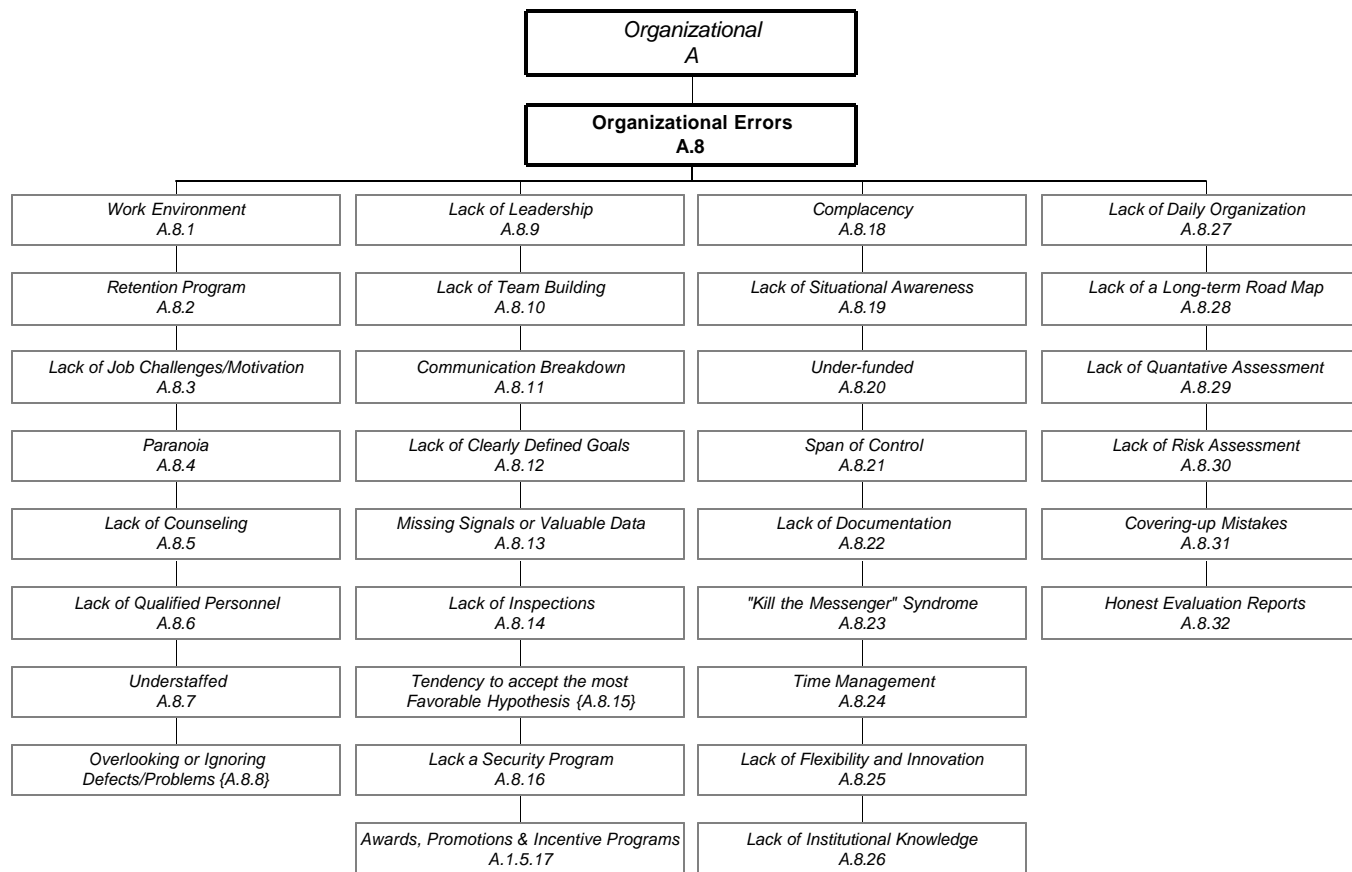


Figure 65: HHM Diagram (Head-topic: A.8)

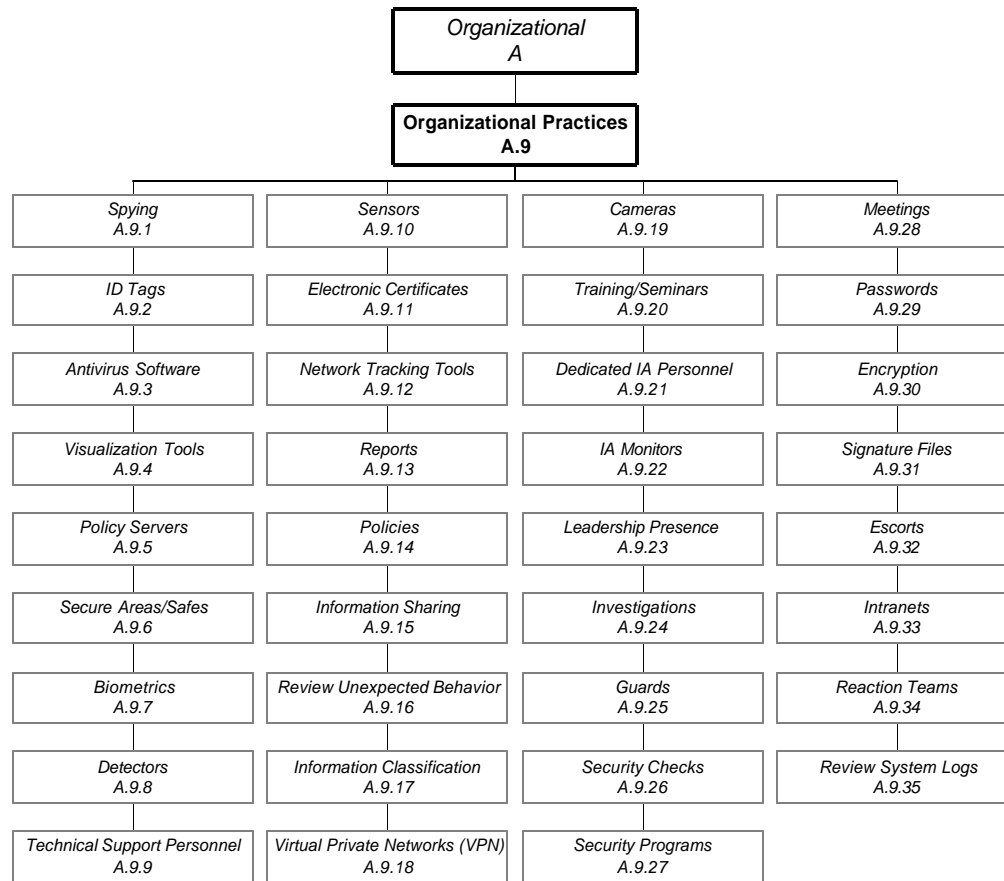


Figure 66: HHM Diagram (Head-topic: A.9)

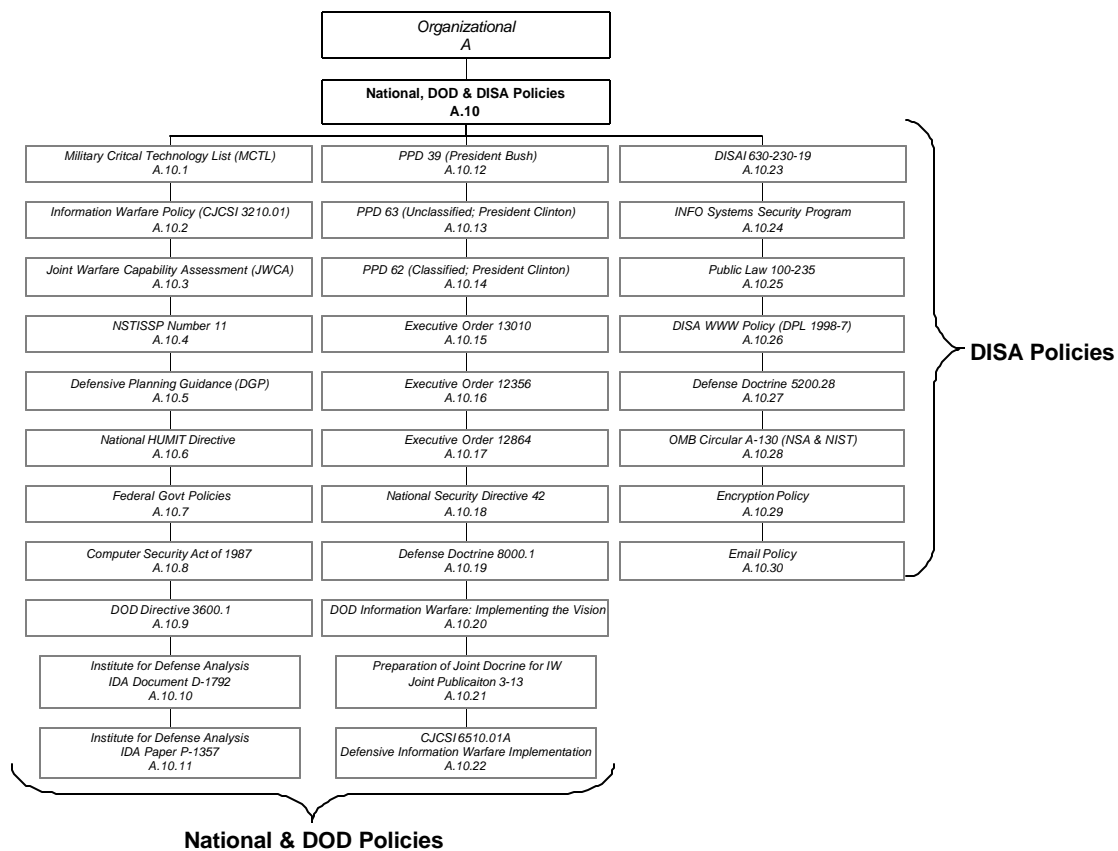


Figure 67: HHM Diagram (Head-topic: A.10)

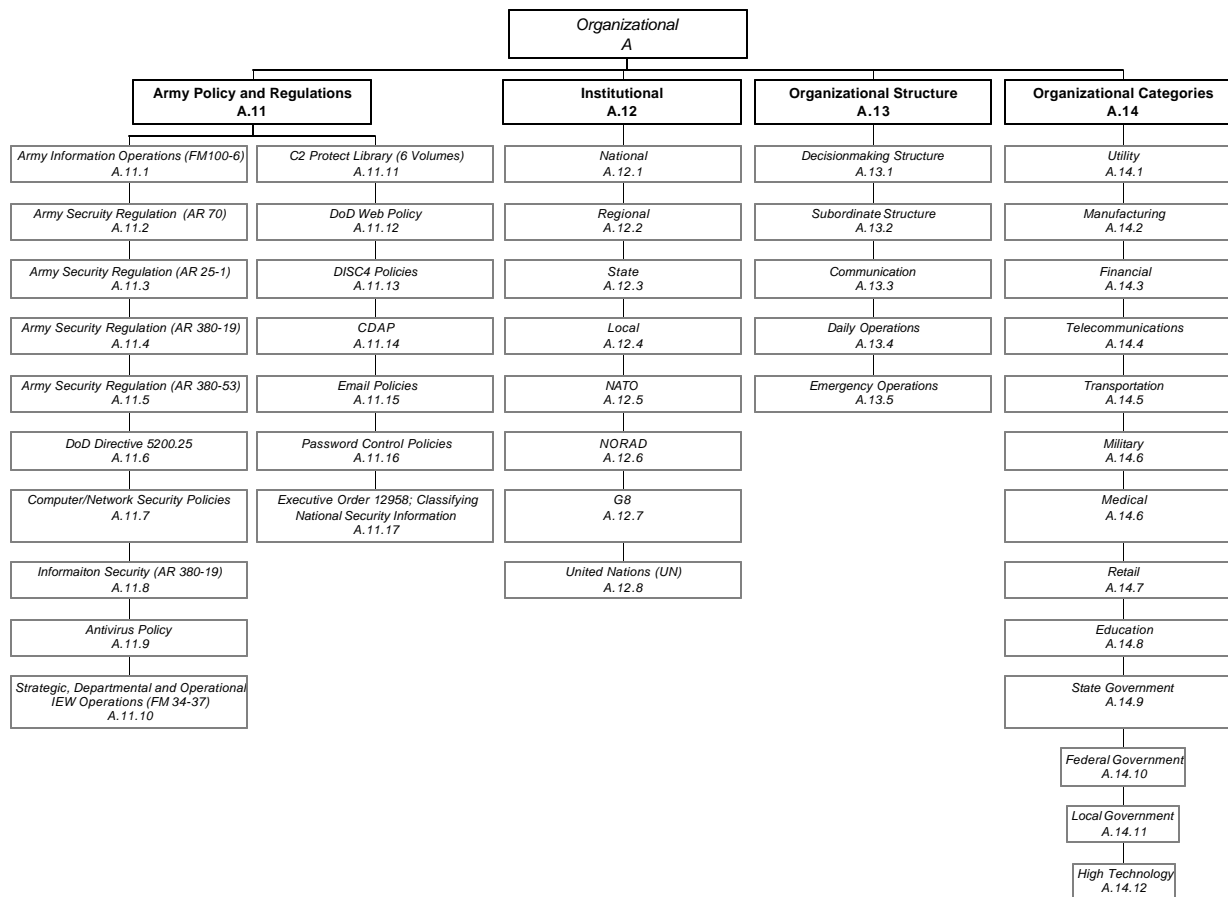


Figure 68: HHM Diagram (Head-topics: A.11, A.12, A.13 and A.14)

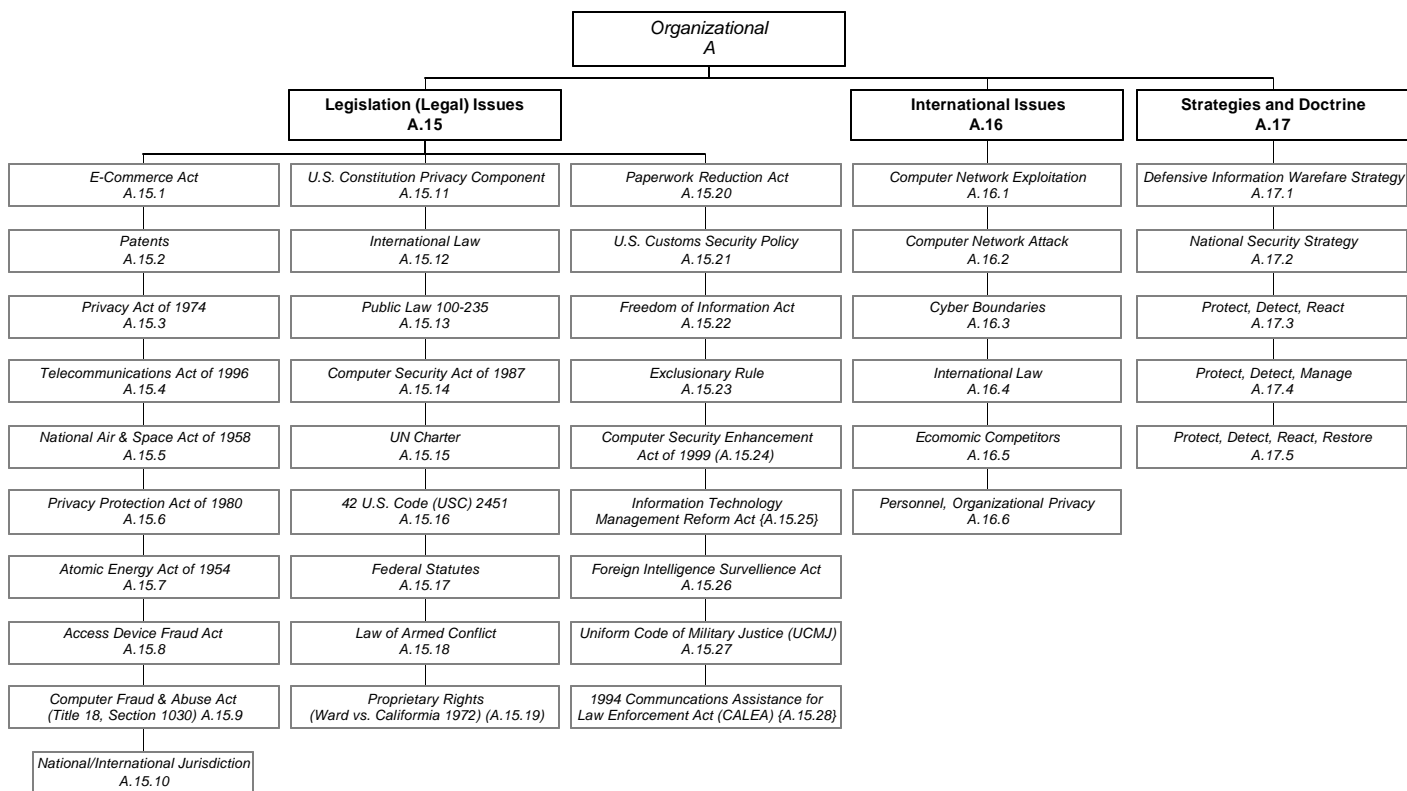


Figure 69: HHM Diagram (Head-topics: A.15, A.16, A.17 and A.18)

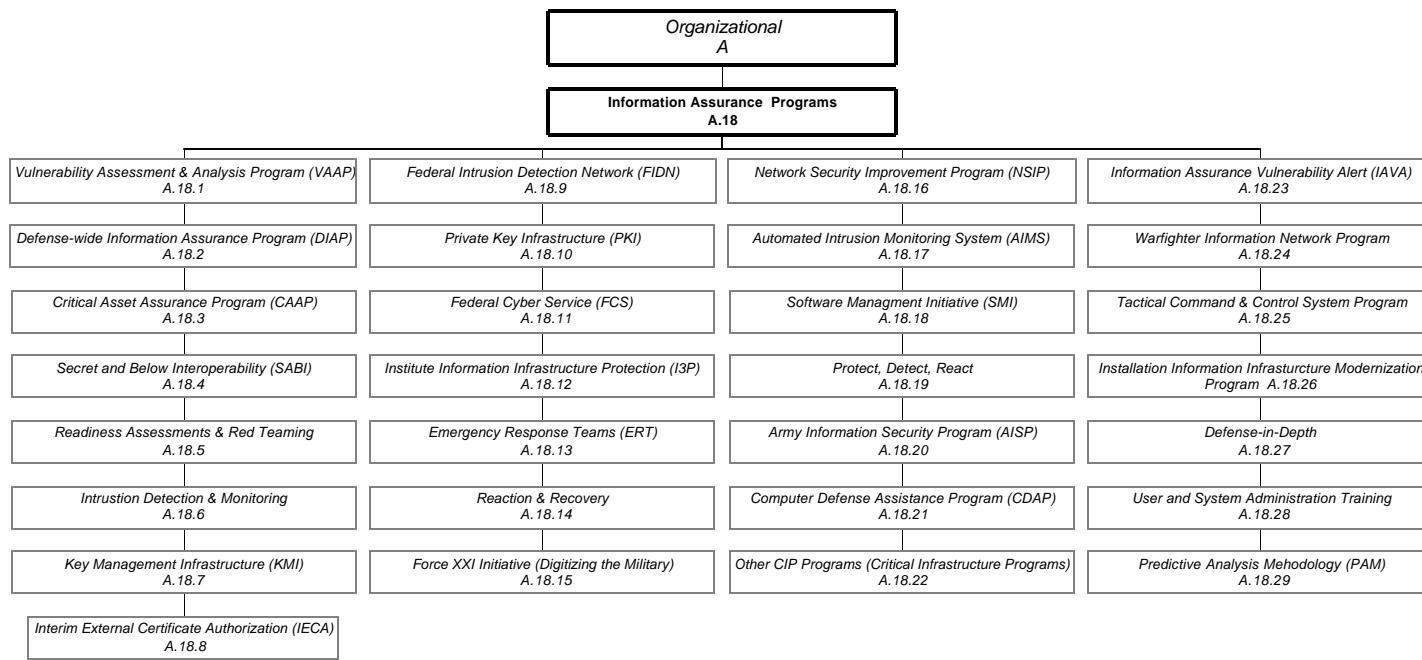


Figure 70: HHM Diagram (Head-topic: A.18)

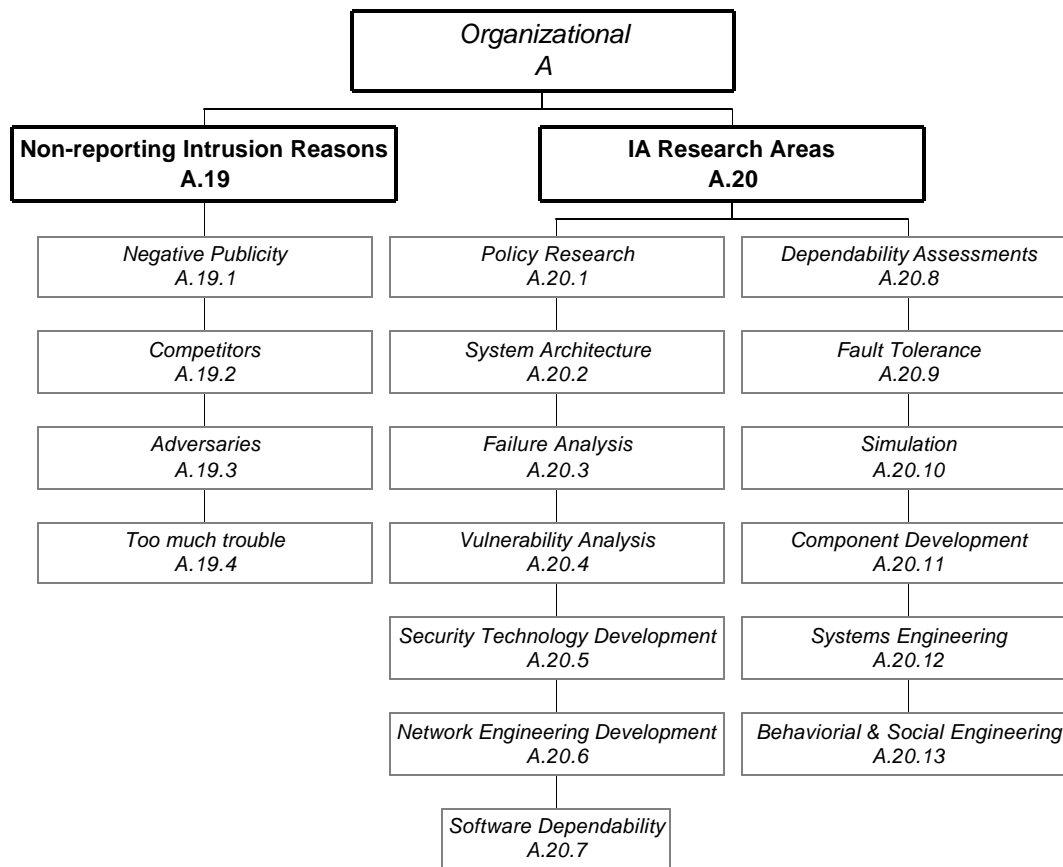


Figure 71: HHM Diagram (Head-topics: A.19 and A.20)

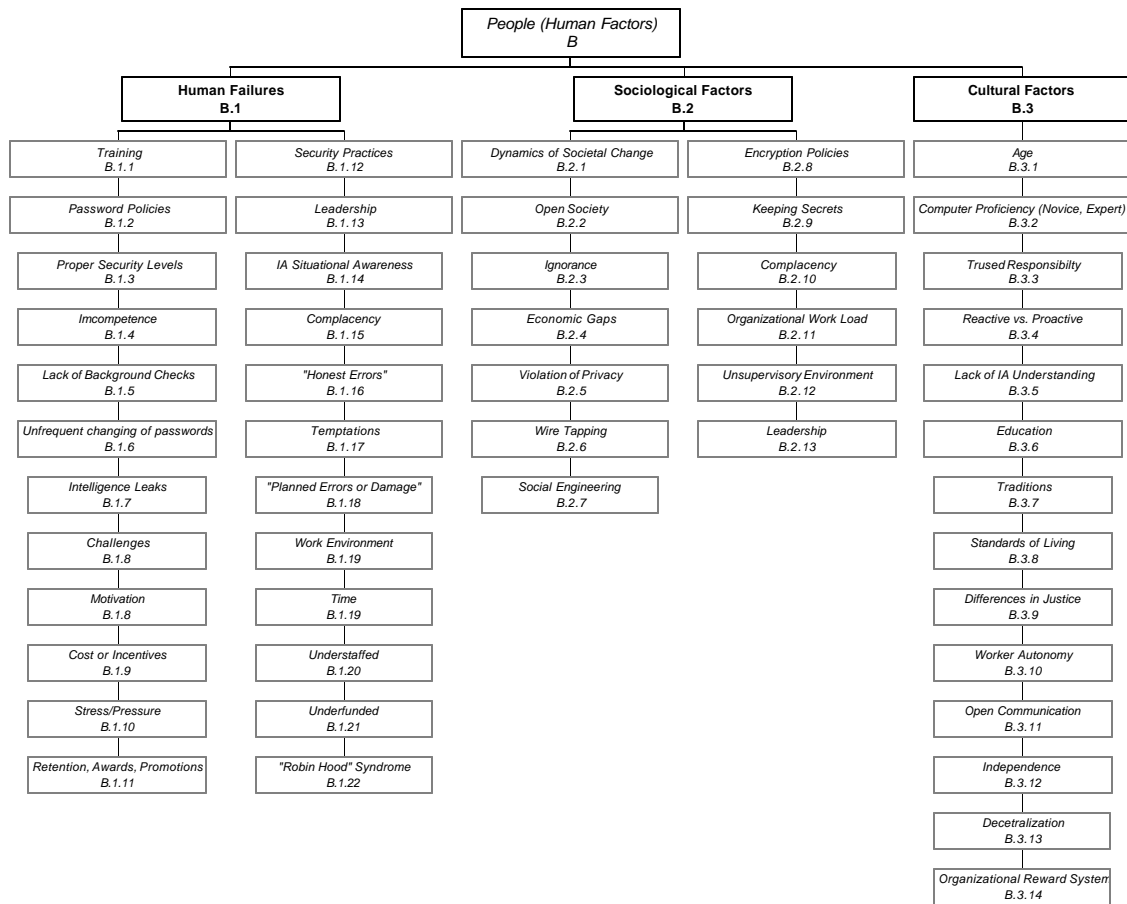


Figure 72: HHM Diagram (Head-topics: B.1, B.2 and B.3)

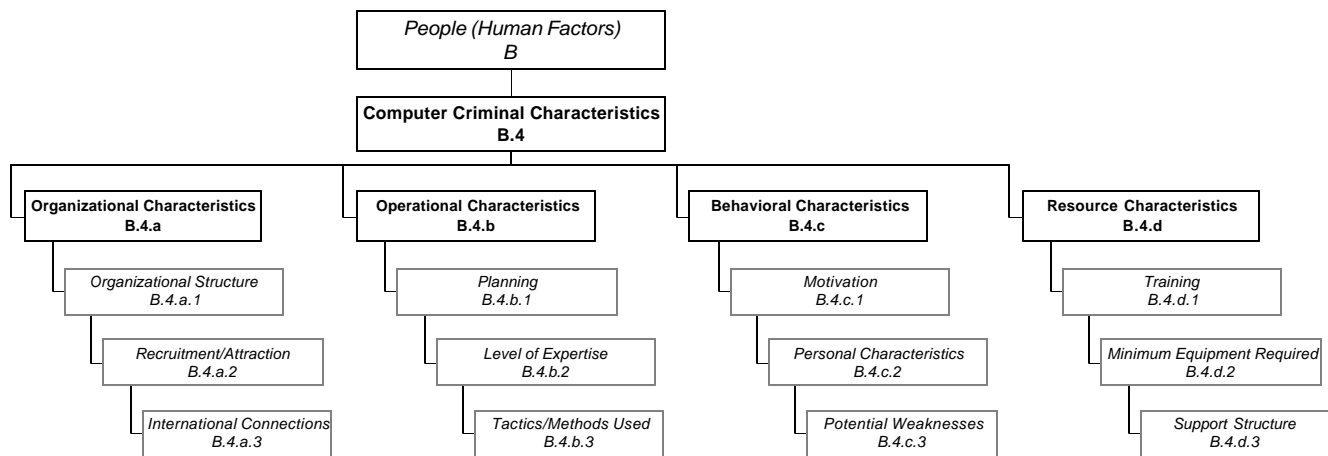


Figure 73: HHM Diagram (Head-topic: B.4)

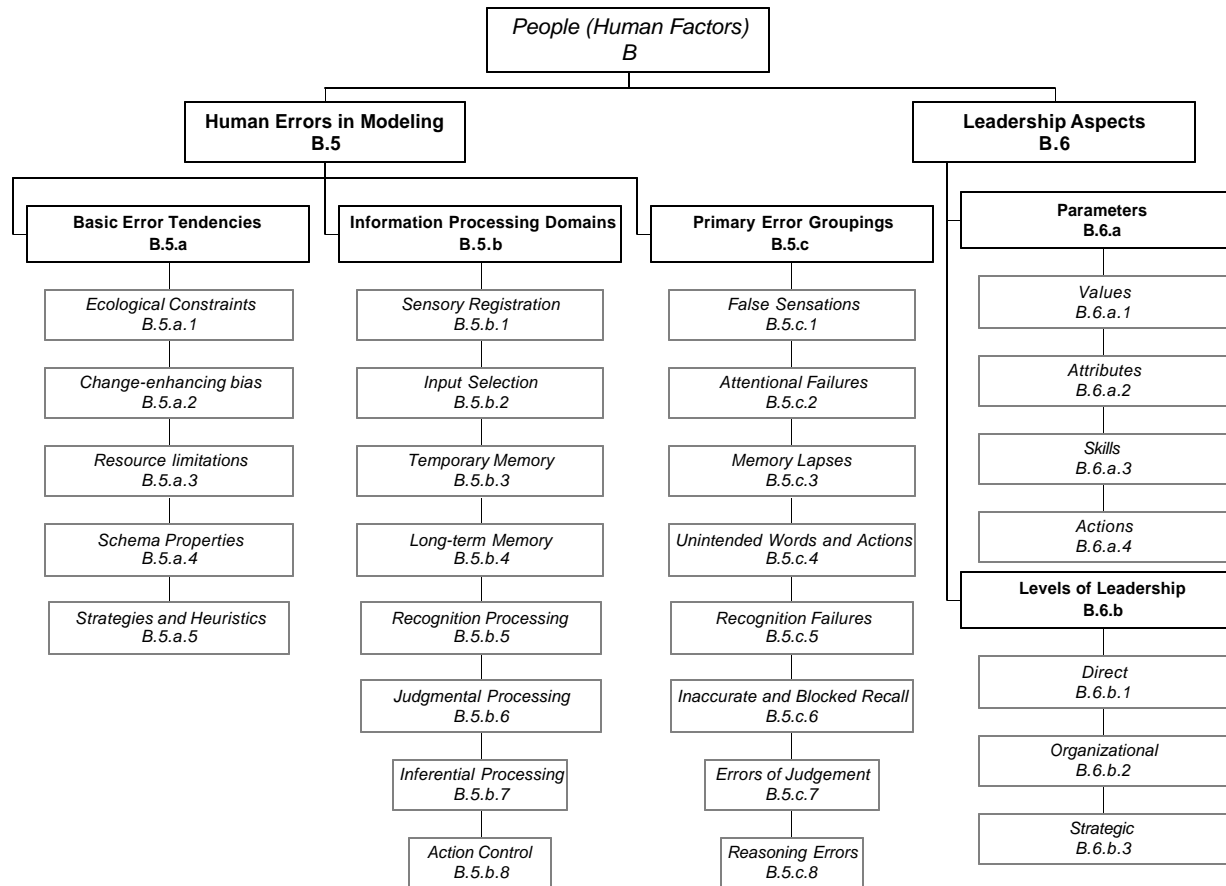


Figure 74: HHM Diagram (Head-topics: B.5 and B.6)

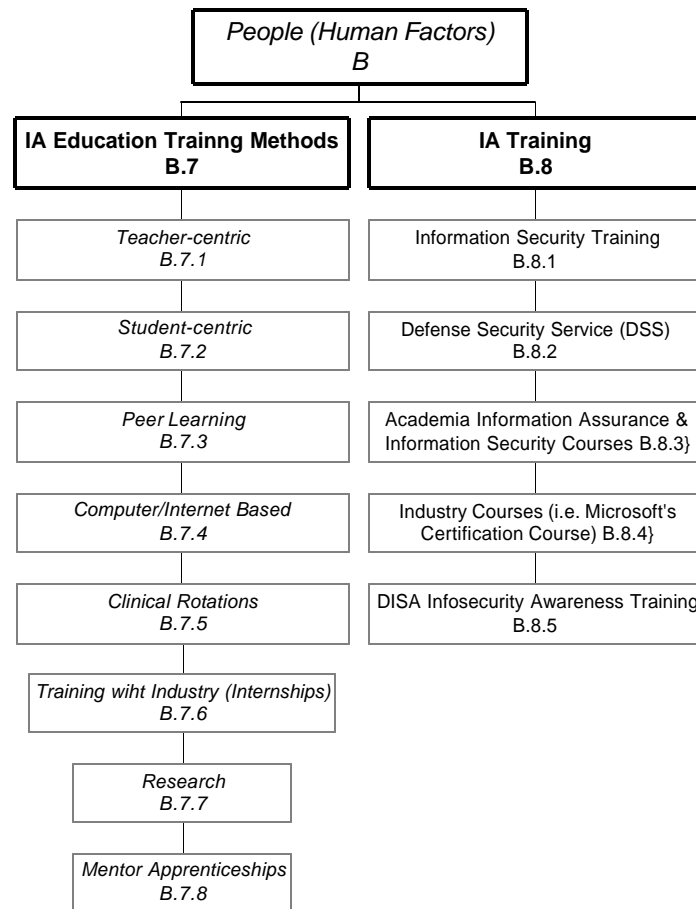


Figure 75: HHM Diagram (Head-topics: B.7 and B.8)

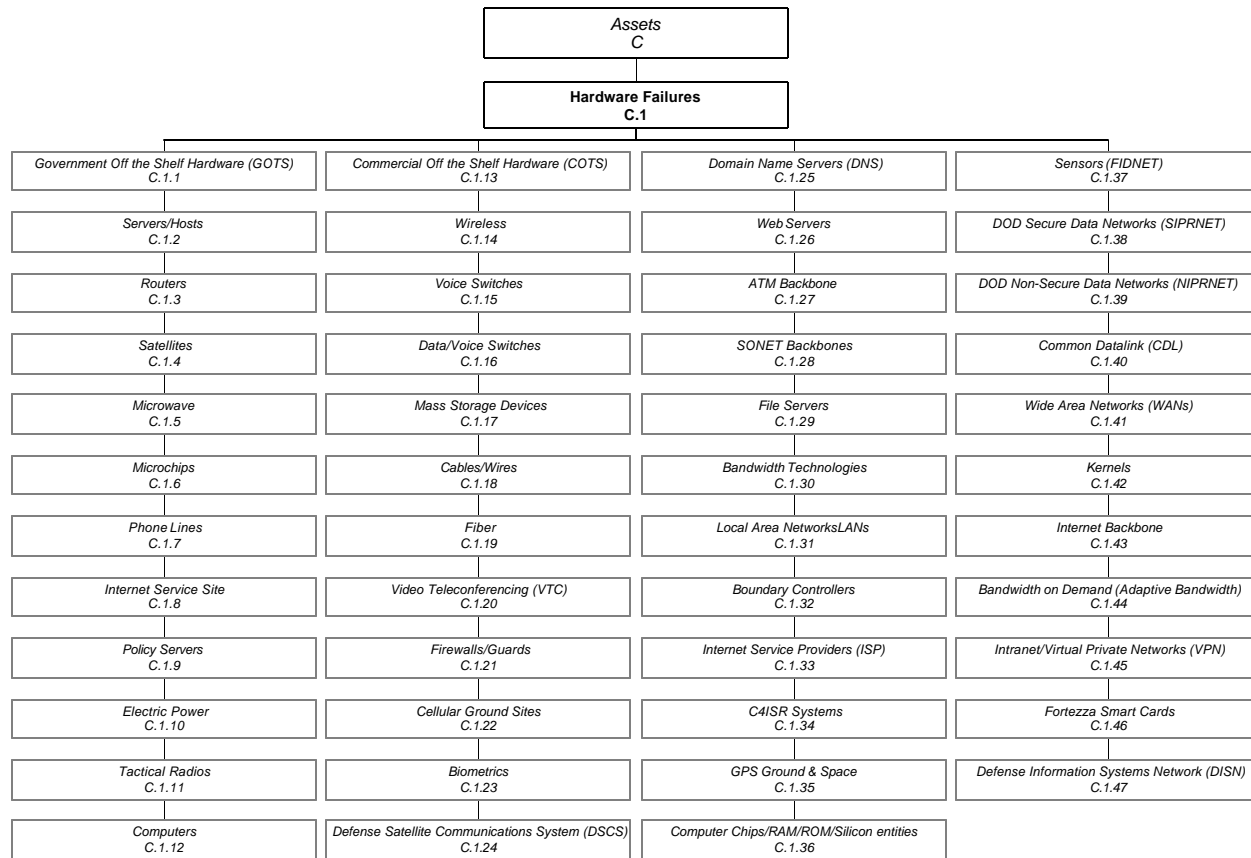


Figure 76: HHM Diagram (Head-topic: C.1)

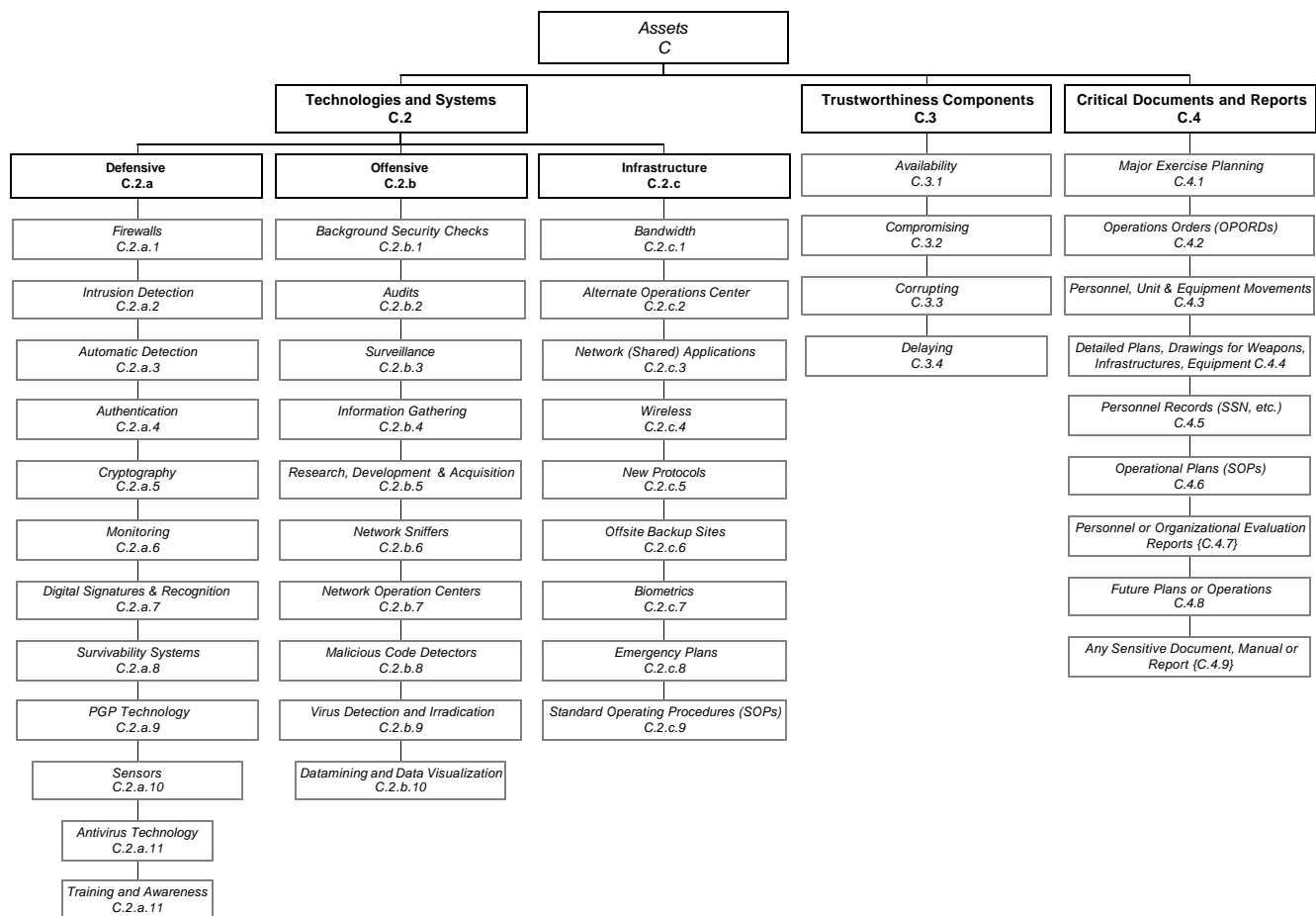


Figure 77: HHM Diagram (Head-topics: C.2, C.3 and C.4)

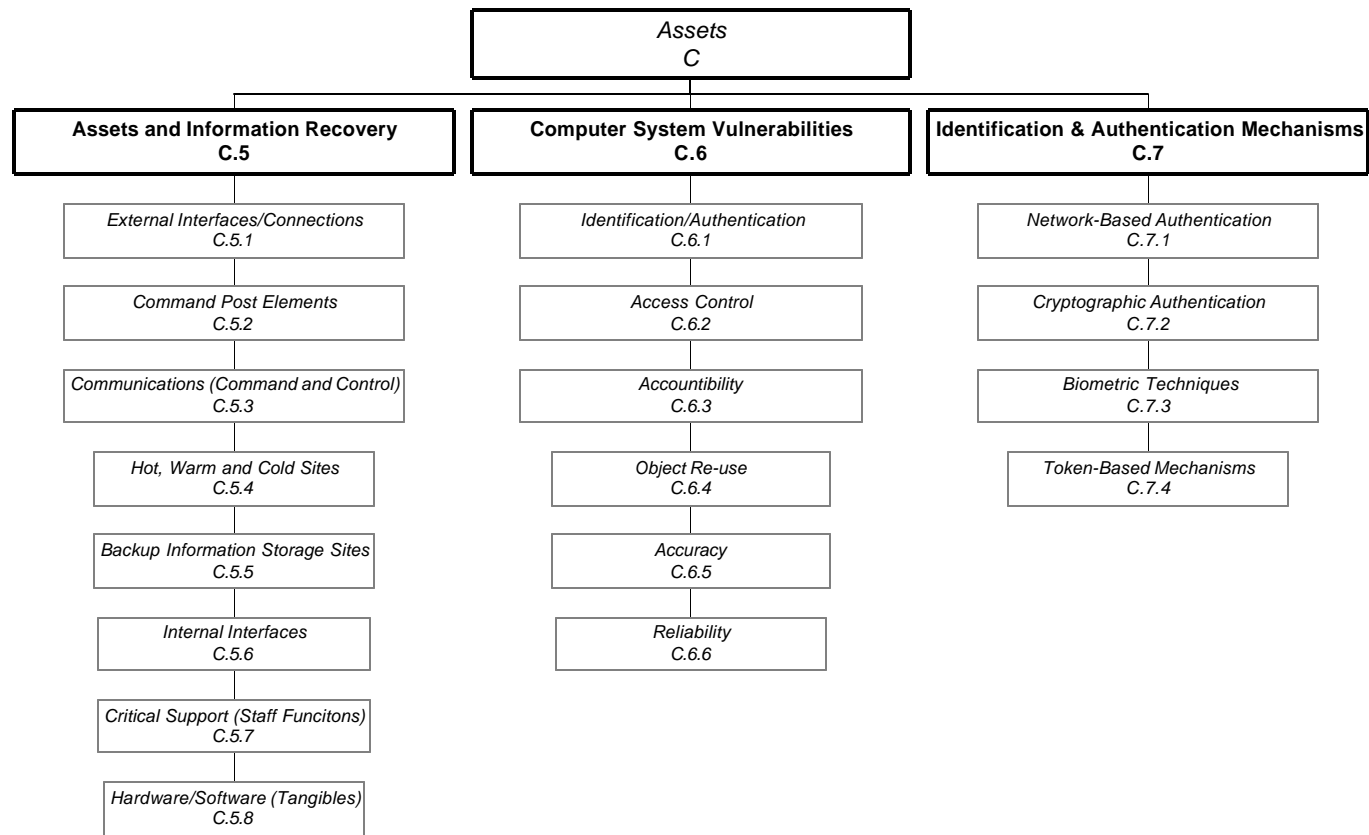


Figure 78: HHM Diagram (Head-topics: C.5, C.6 and C.7)

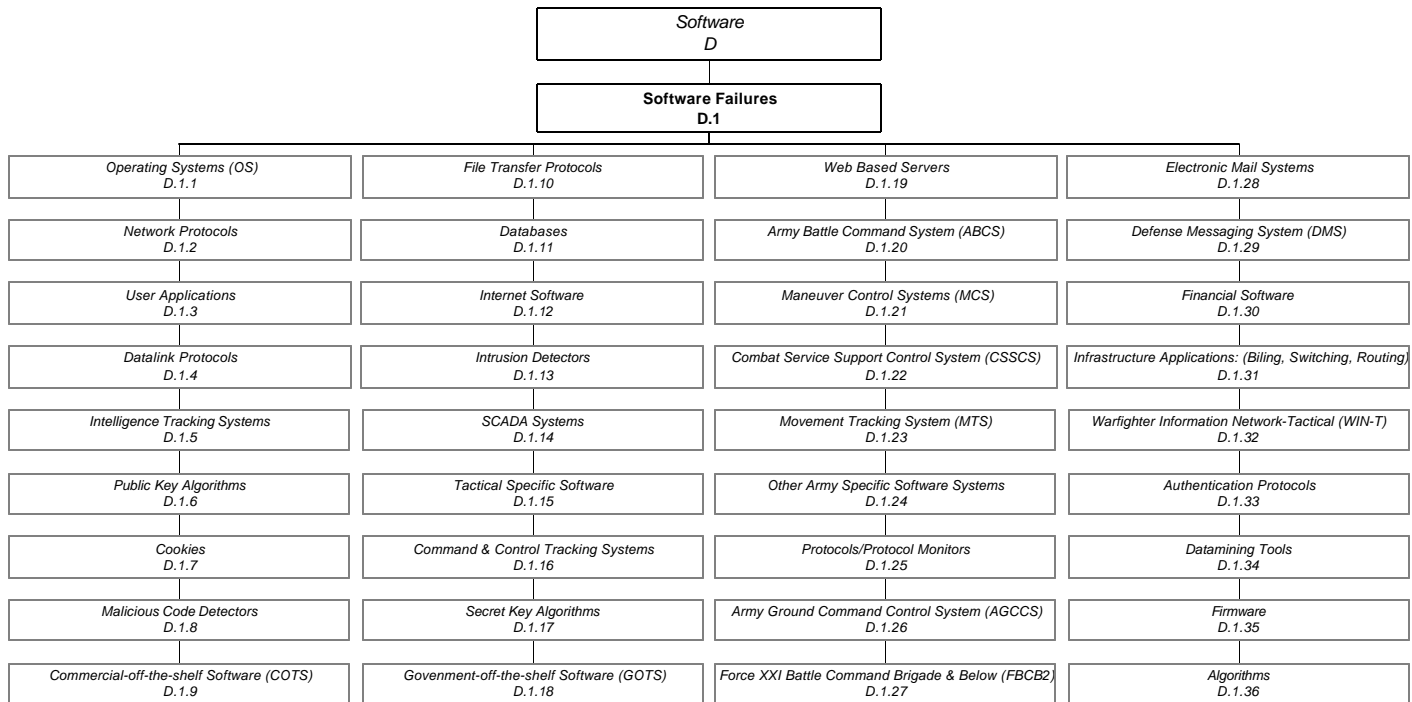


Figure 79: HHM Diagram (Head-topic: D.1)

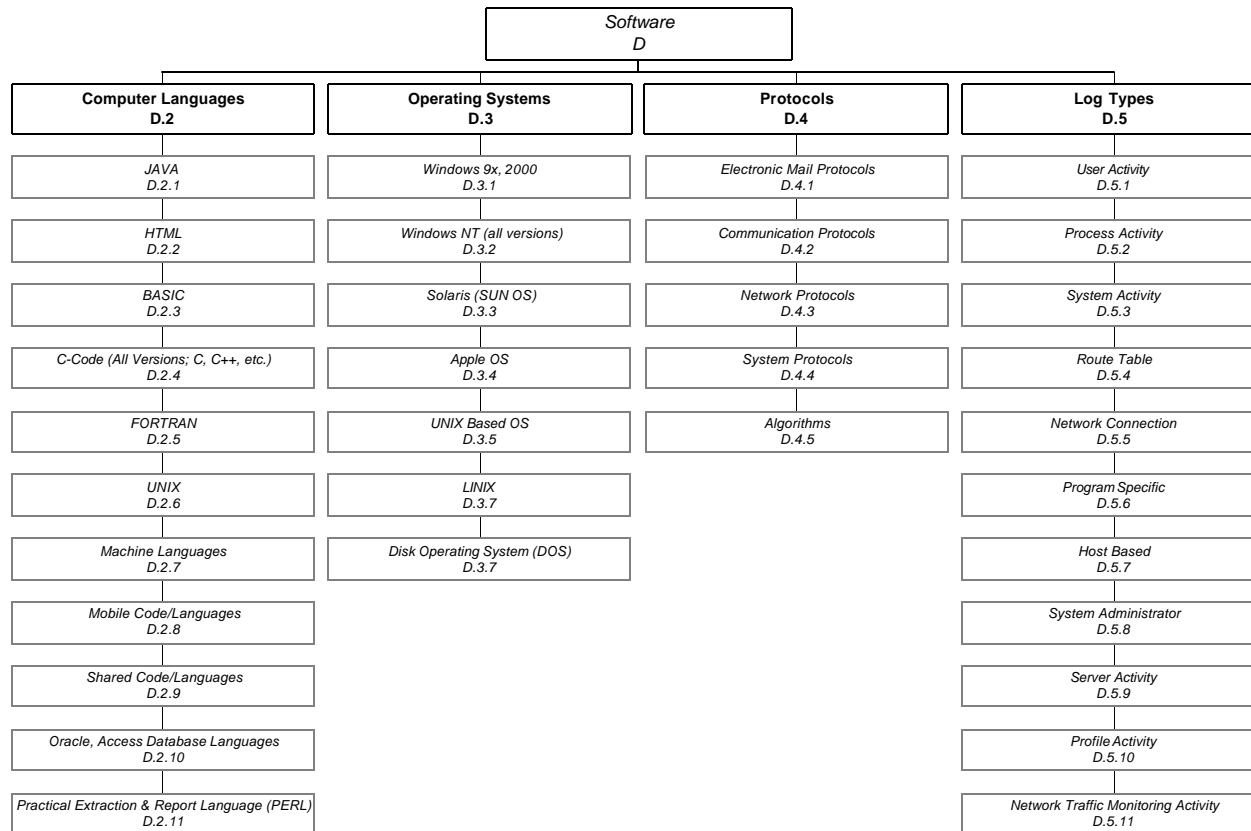


Figure 80: HHM Diagram (Head-topics: D.2, D.3, D.4 and D.5)

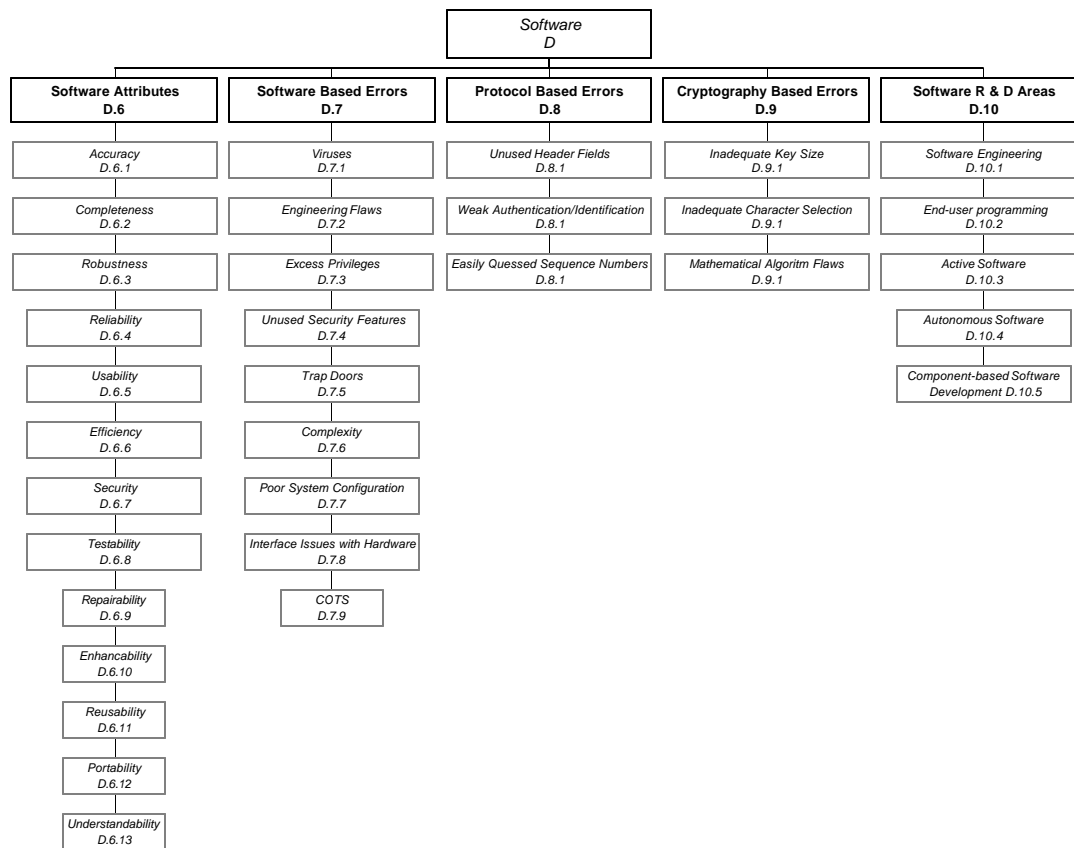


Figure 81: HHM Diagram (Head-topics: D.6, D.7, D.8, D.9 and D.10)

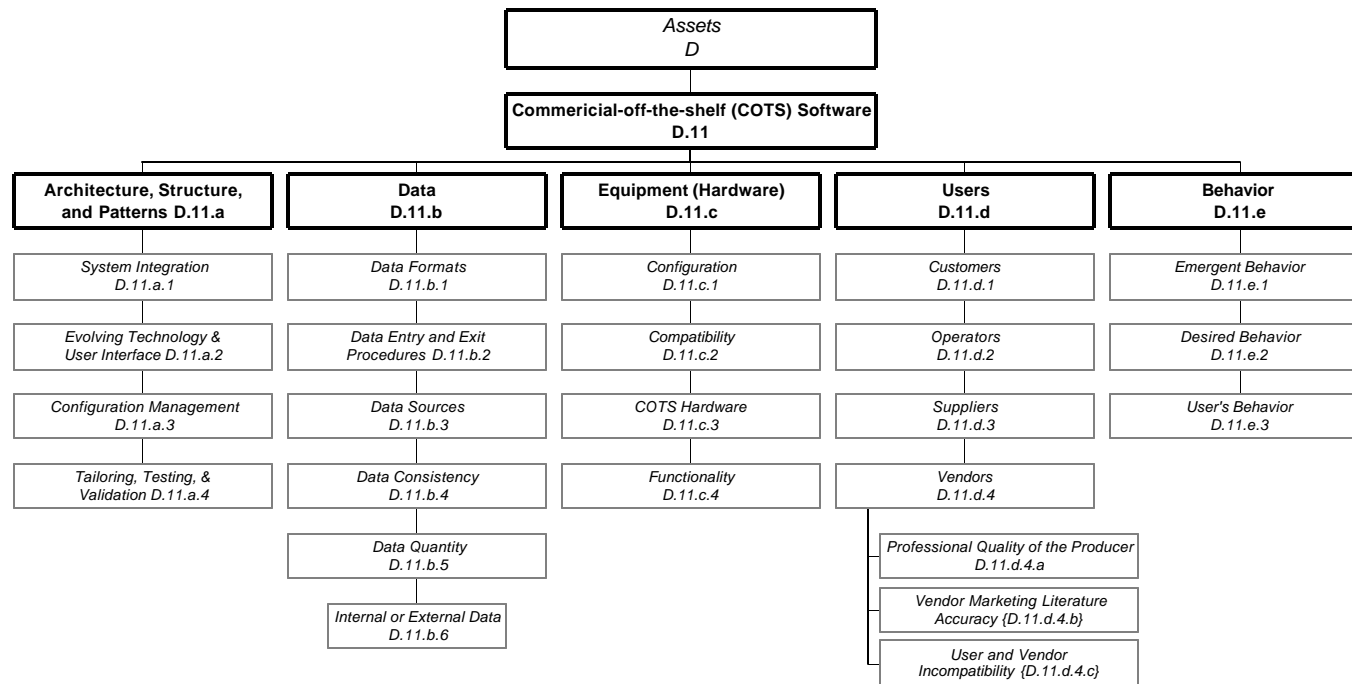


Figure 82: HHM Diagram (Head-topic: D.11a-D.11e)

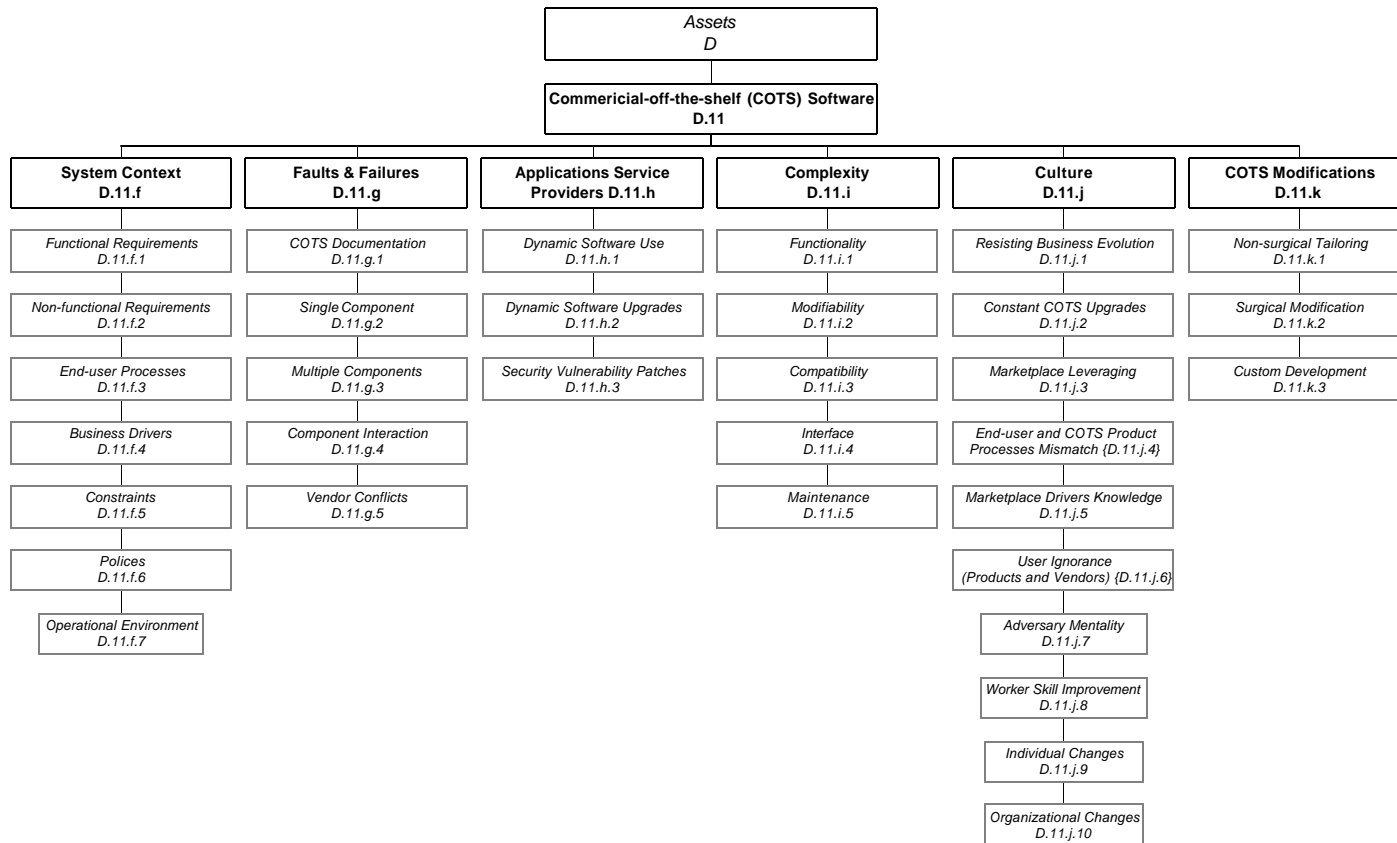


Figure 83: HHM Diagram (Head-topic: D.11f-D.11k)

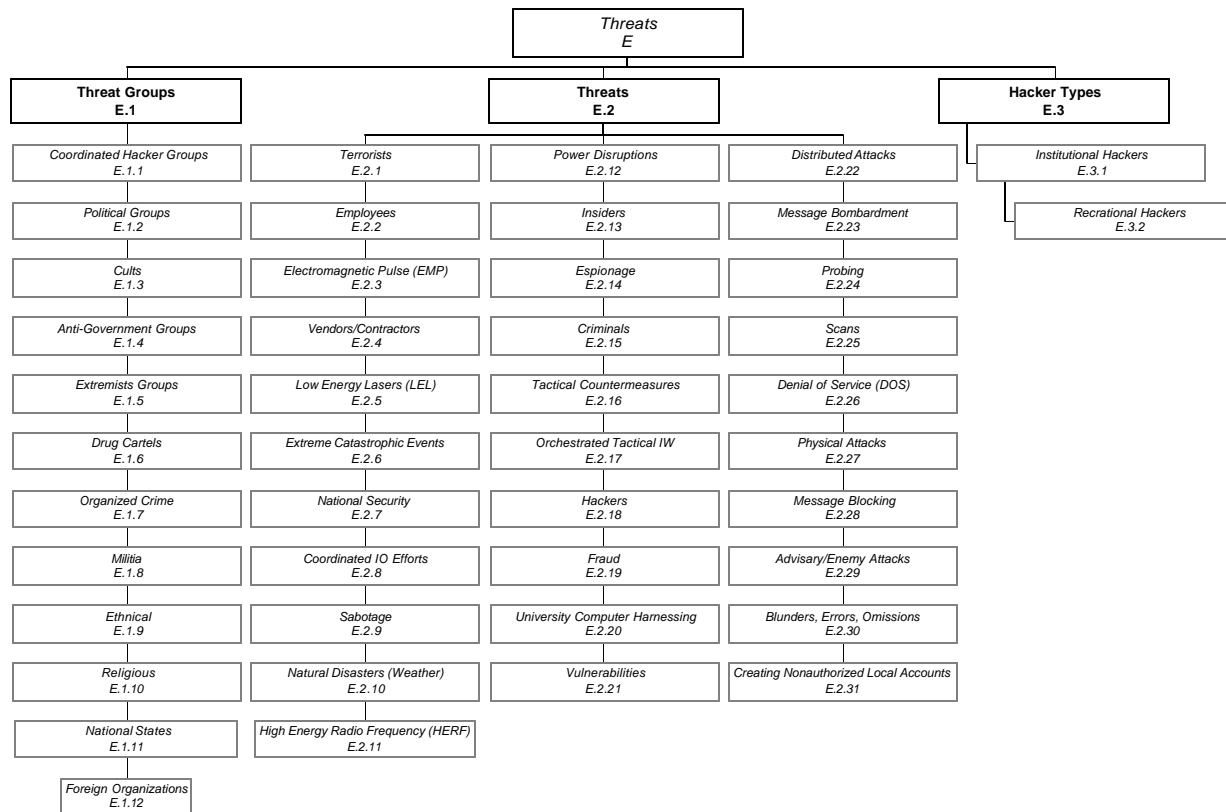


Figure 84: HHM Diagram (Head-topics: E.1, E.2 and E.3)

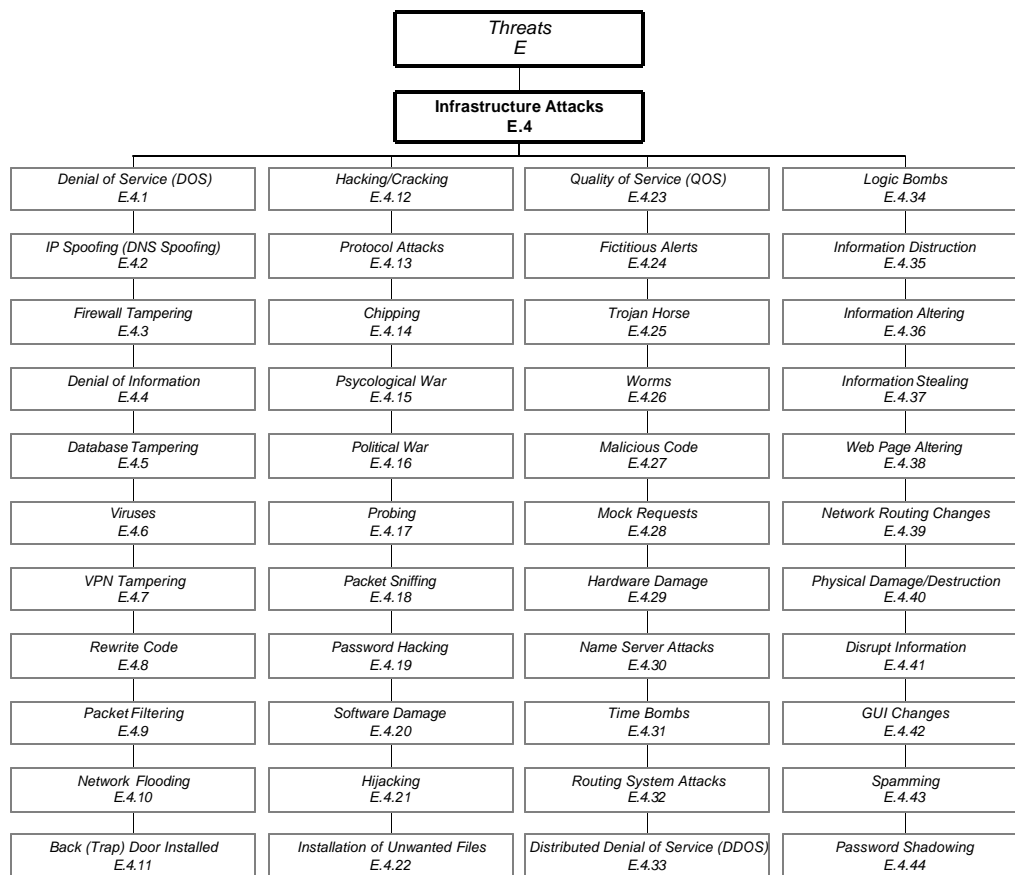


Figure 85: HHM Diagram (Head-topic: E.4)

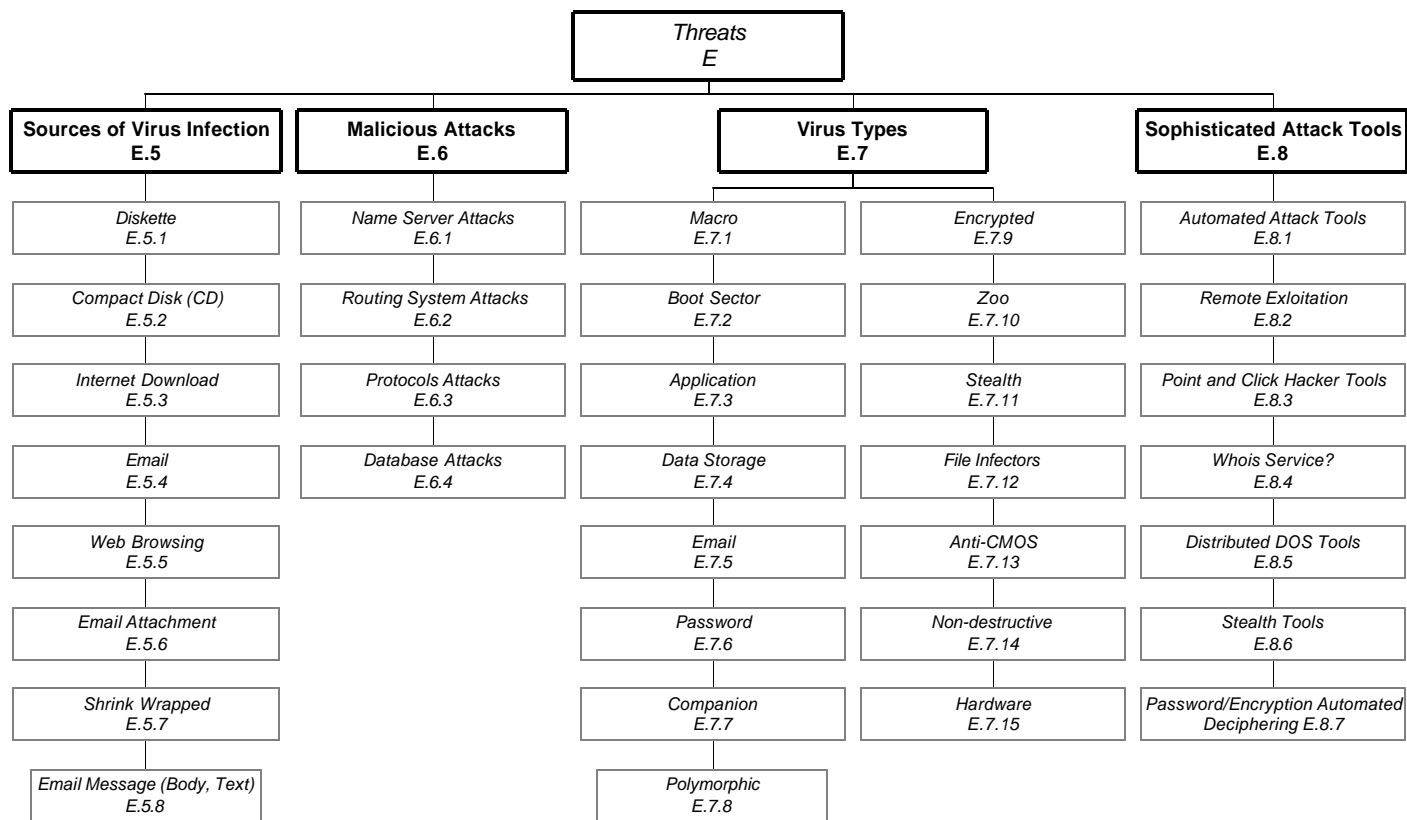


Figure 86: HHM Diagram (Head-topics: E.5, E.6, E.7, and E.8)

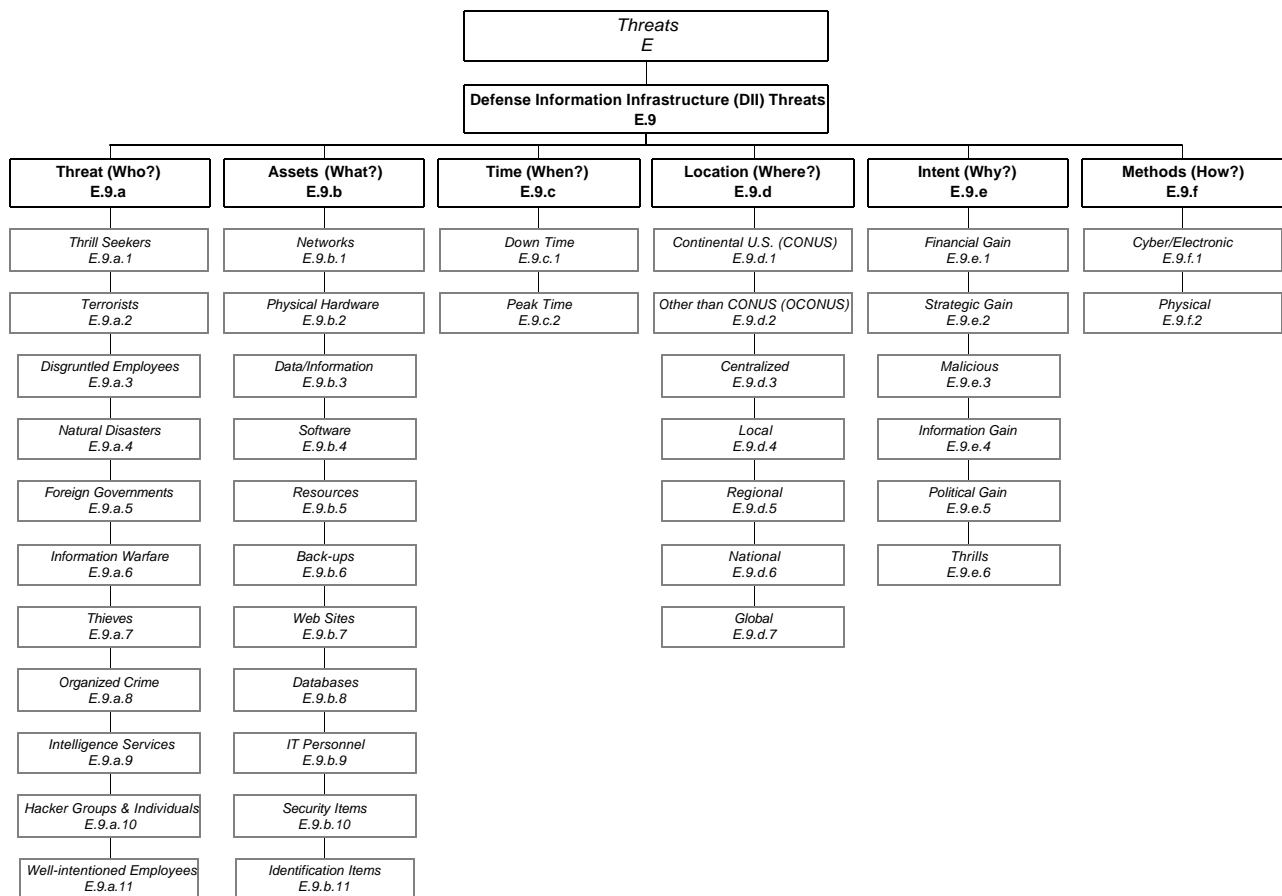


Figure 87: HHM Diagram (Head-topic: E.9)

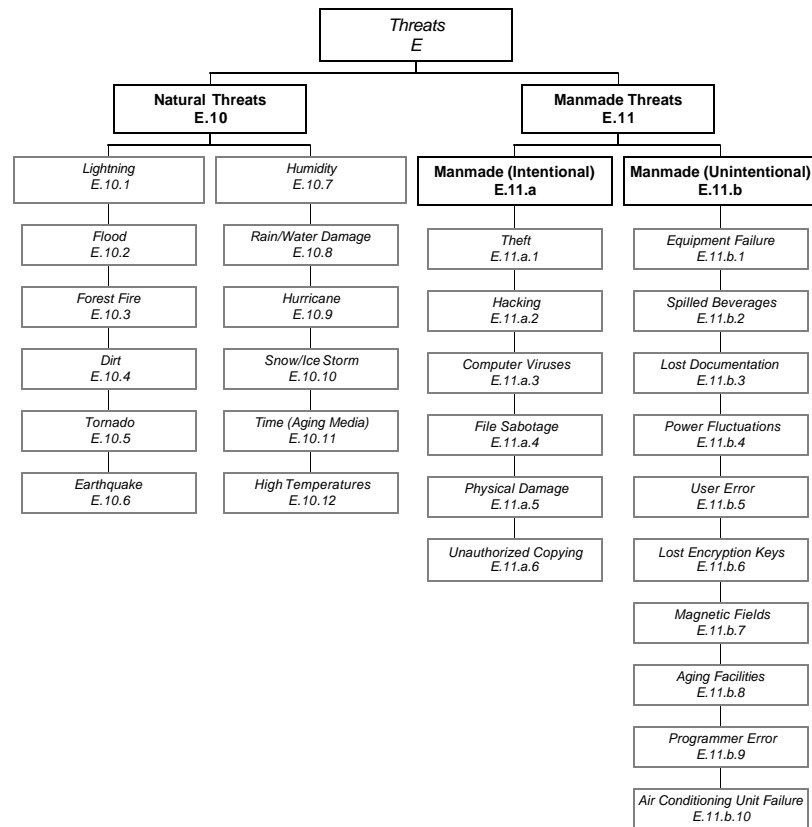


Figure 88: HHM Diagram (Head-topics: E.10 and E.11)

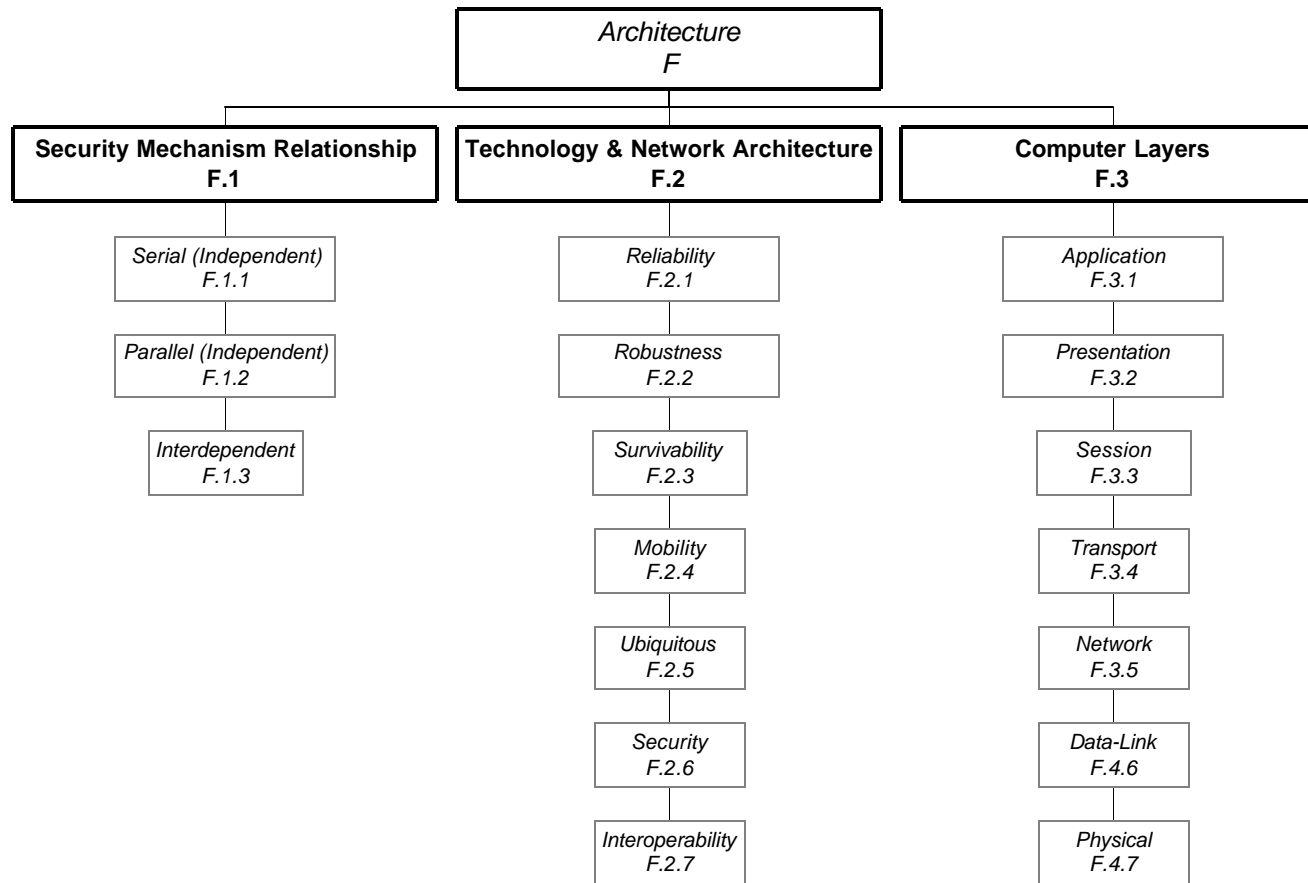


Figure 89: HHM Diagram (Head-topics: F.1, F.2 and F.3)

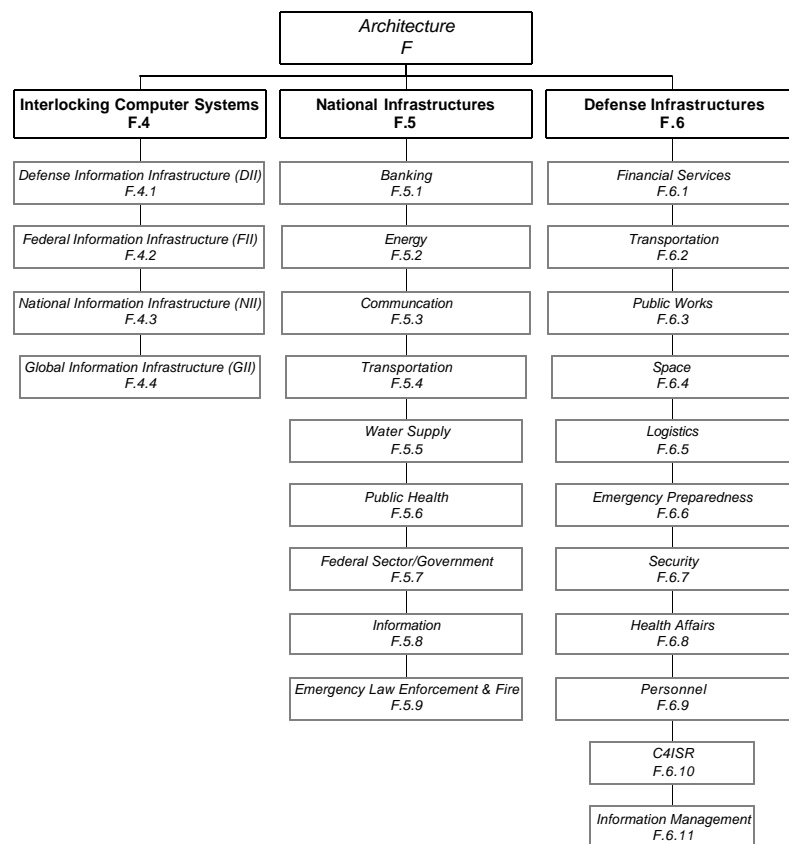


Figure 90: HHM Diagram (Head-topics: F.4, F.5 and F.6)

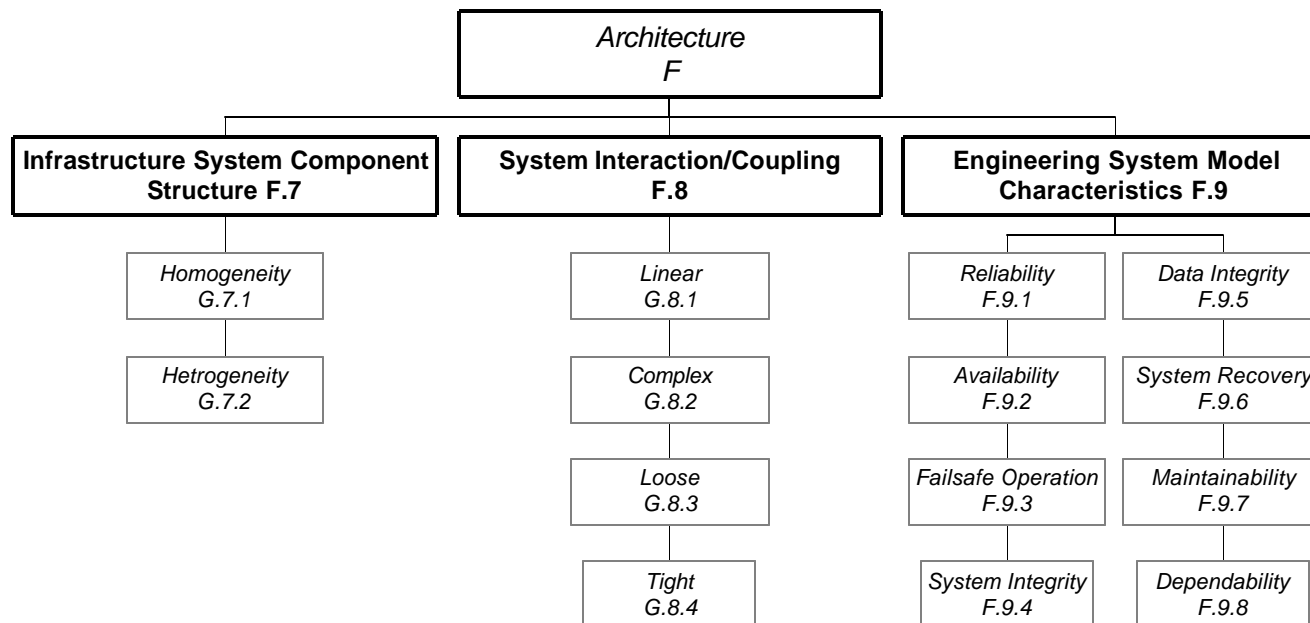


Figure 91: HHM Diagram (Head-topics: F.7, F.8 and F.9)

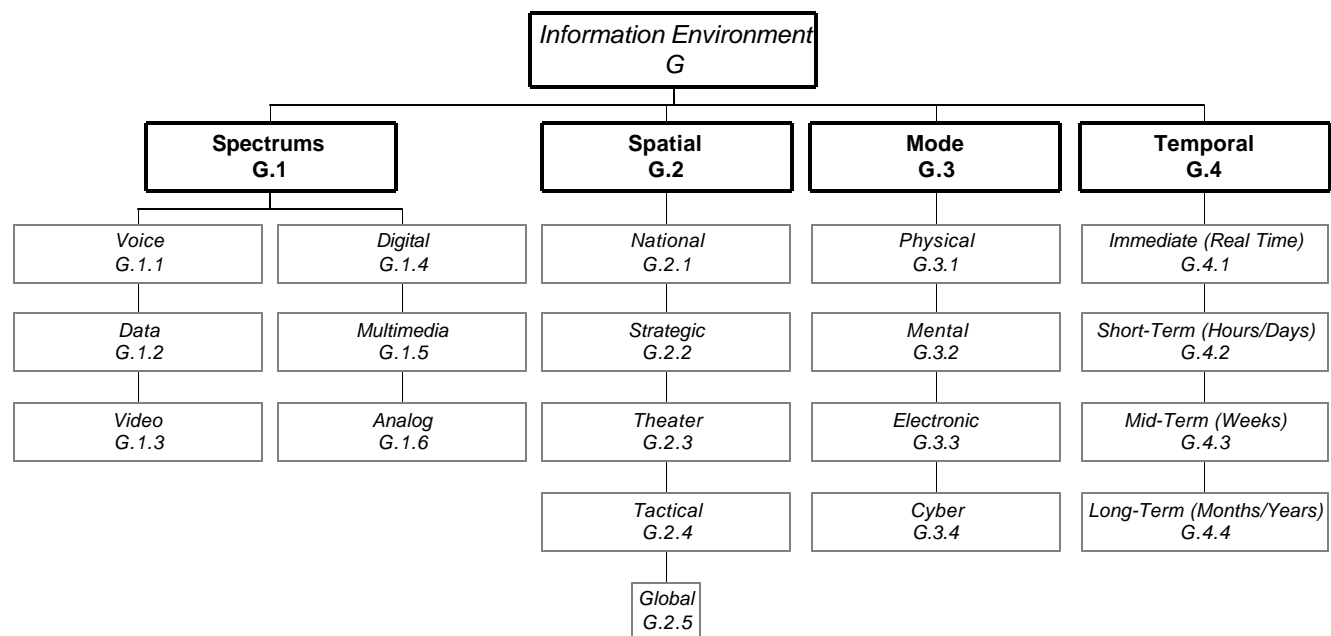


Figure 92: HHM Diagram (Head-topics: G.1, G.2 G.3 and G.4)

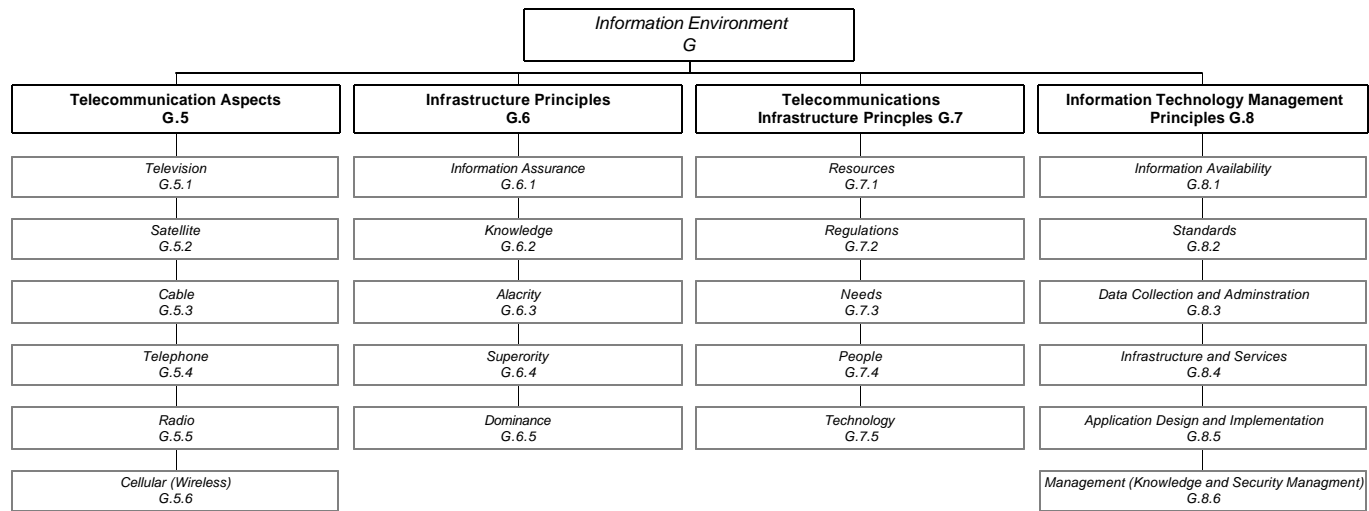


Figure 93: HHM Diagram (Head-topics: G.5, G.6, G.7 and G.8)

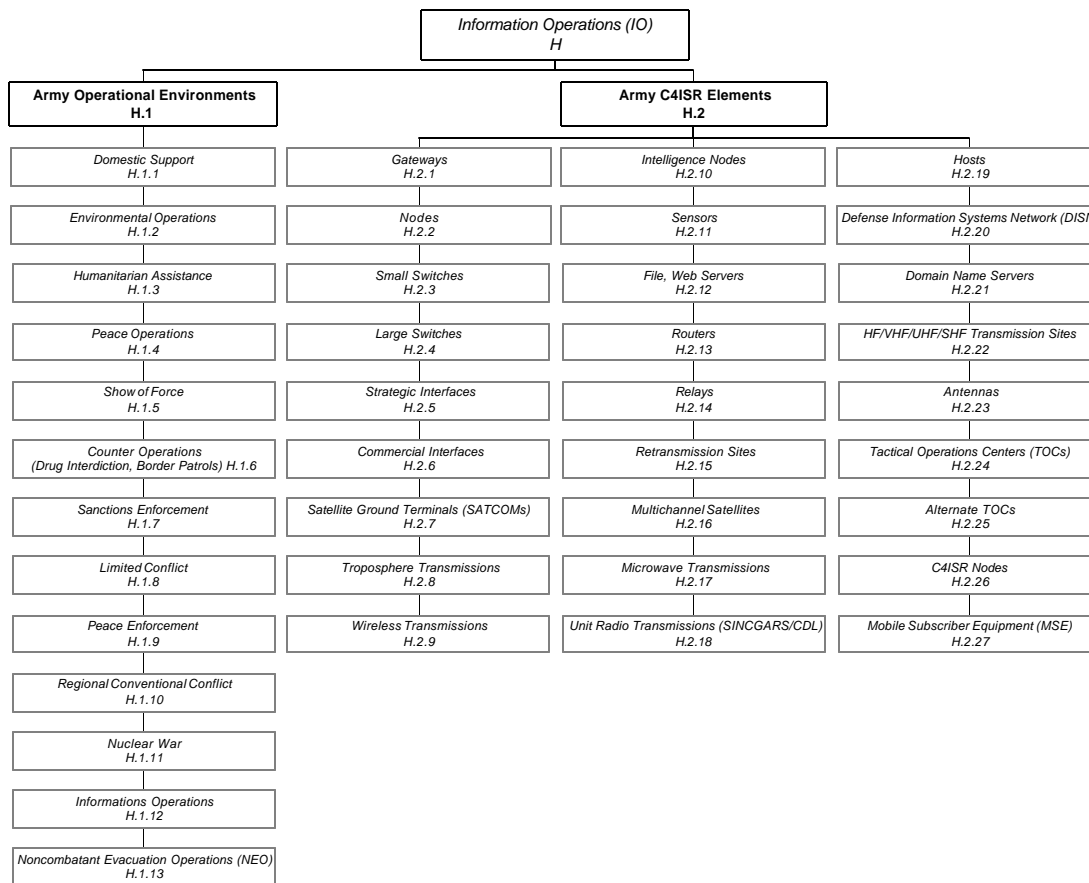


Figure 94: HHM Diagram (Head-topics: H.1 and H.2)

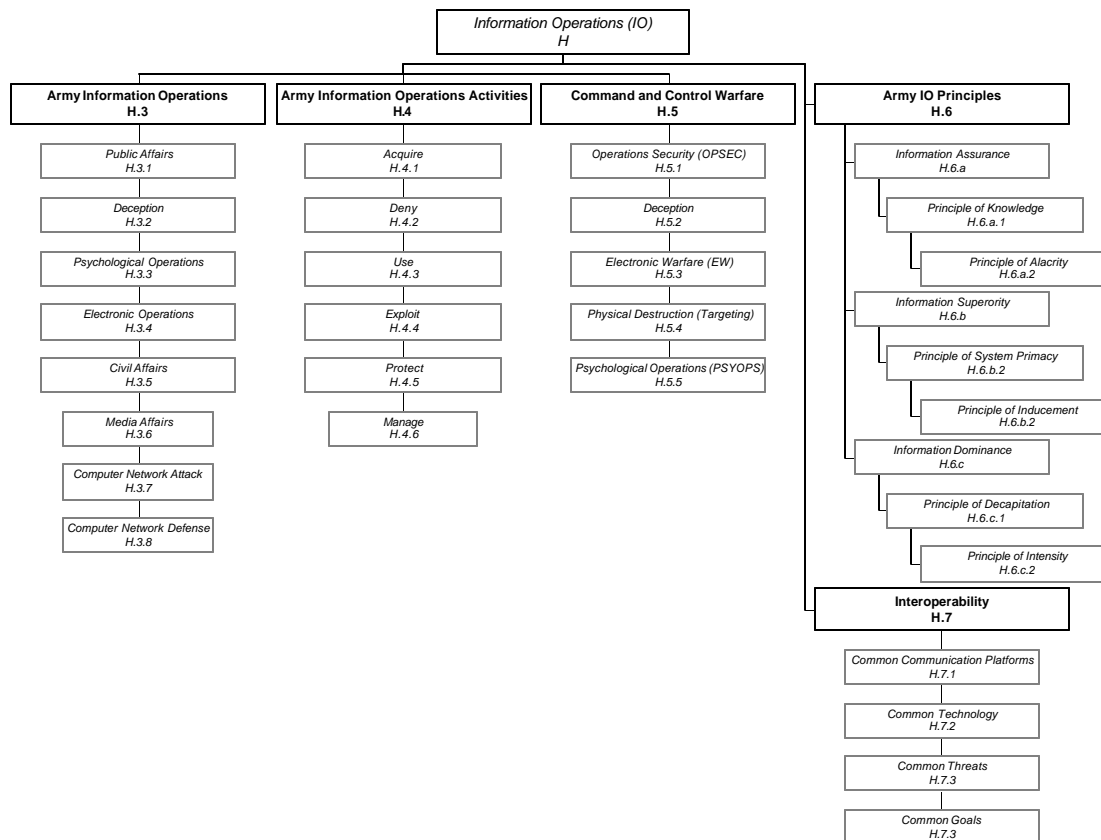


Figure 95: HHM Diagram (Head-topics: H.3, H.4, H.5, H.6 and H.7)

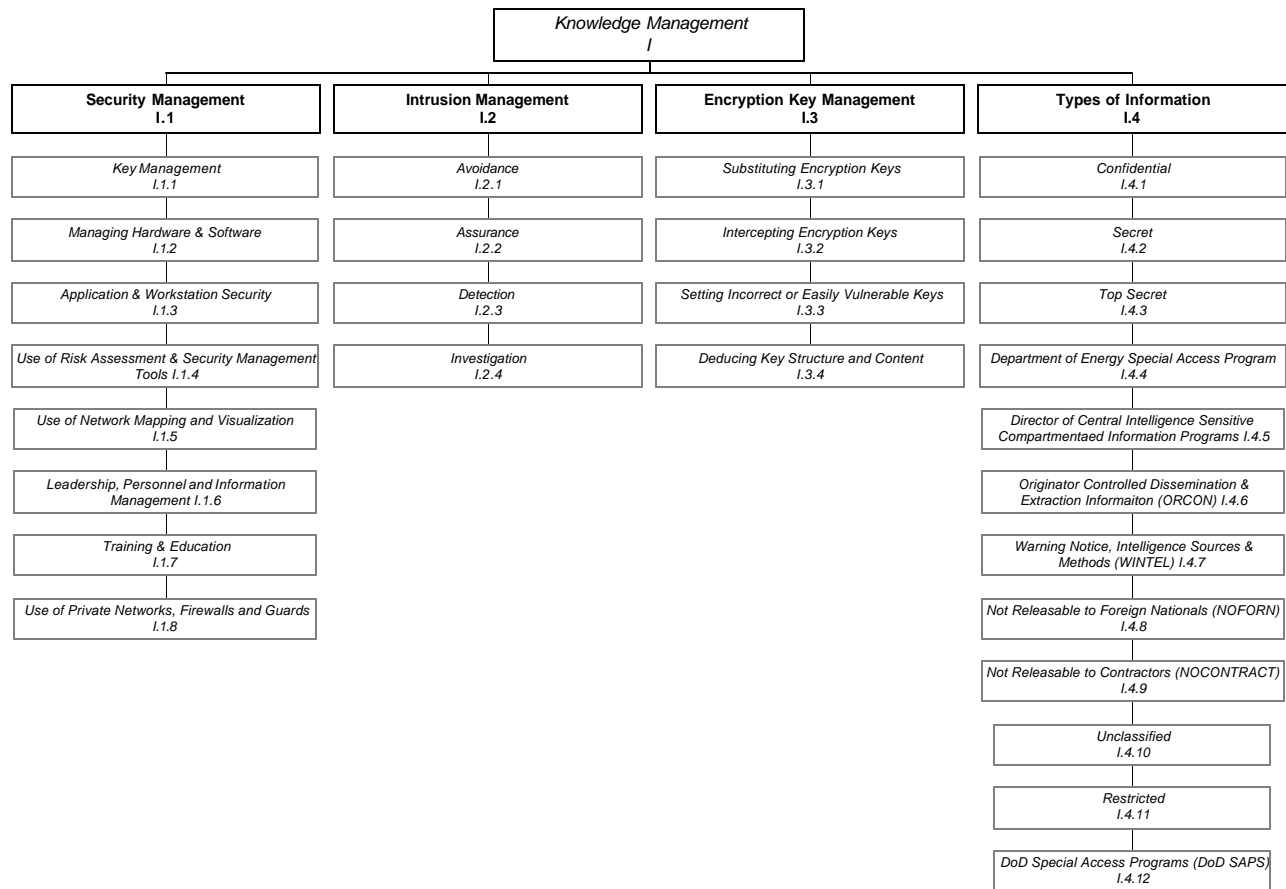


Figure 96: HHM Diagram (Head-topics: I.1, I.2, I.3 and I.4)

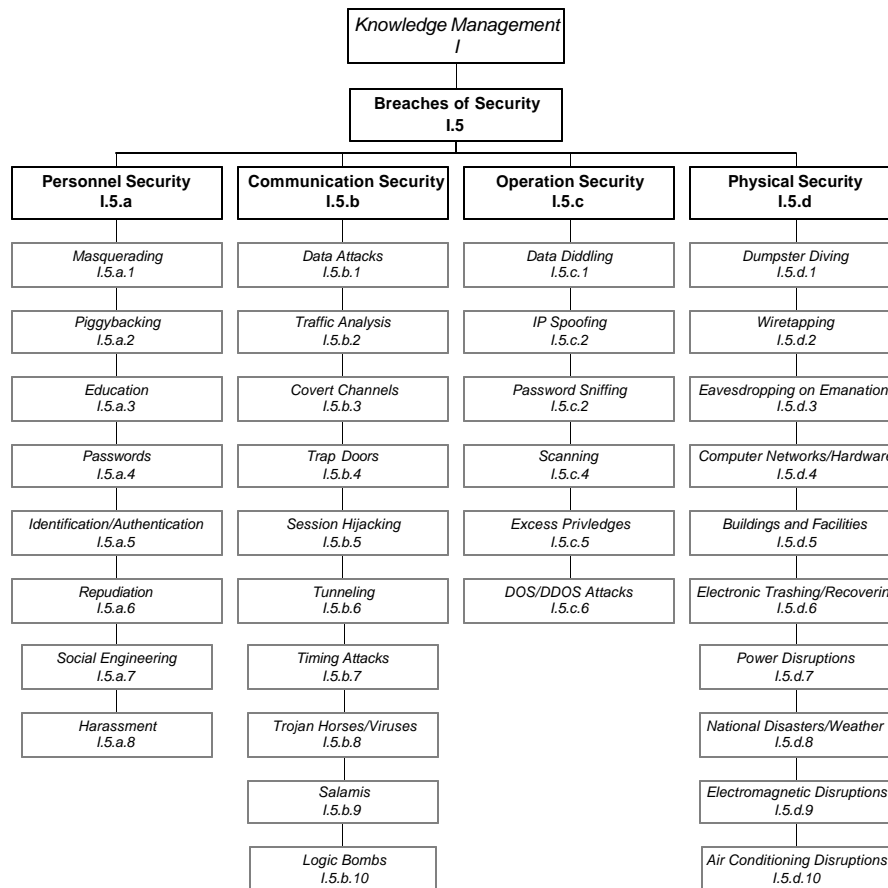


Figure 97: HHM Diagram (Head-topic: I.5)

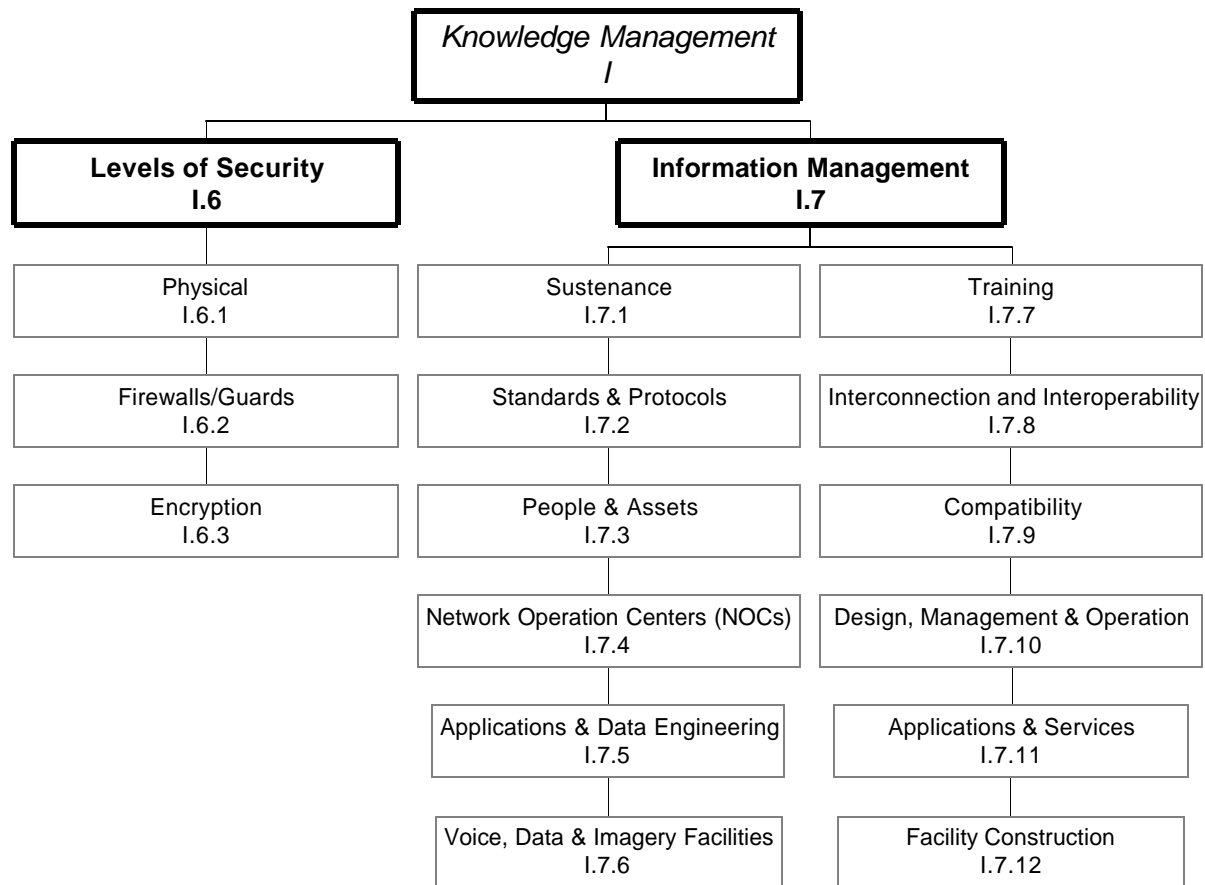


Figure 98: HHM Diagram (Head-topics: I.6 and I.7)

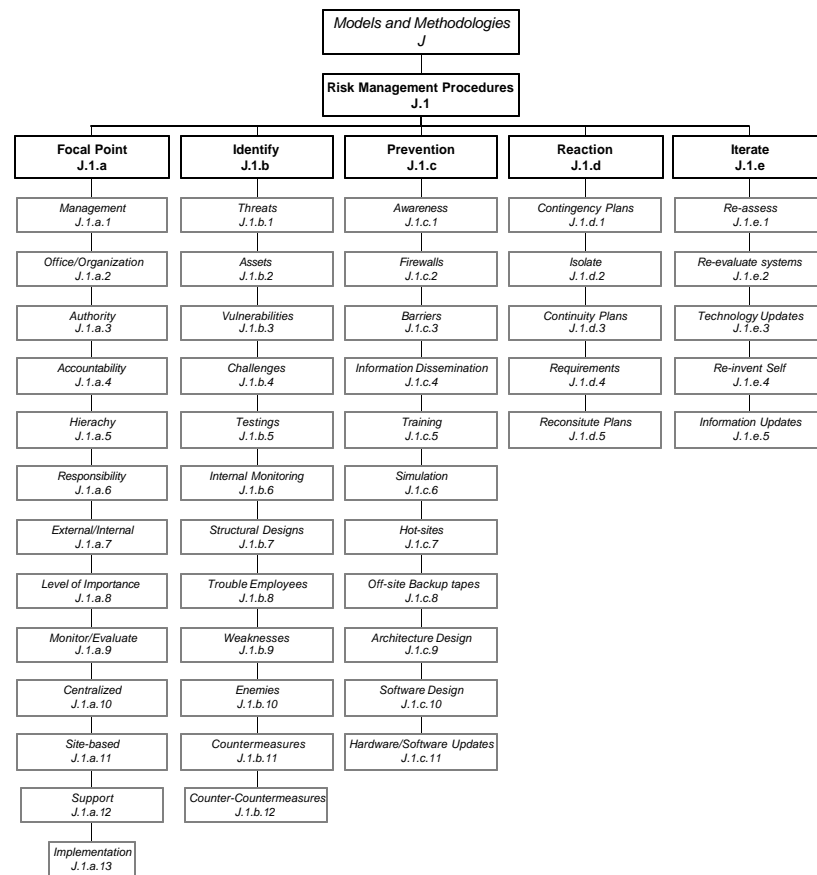


Figure 99: HHM Diagram (Head-topic: J.1)

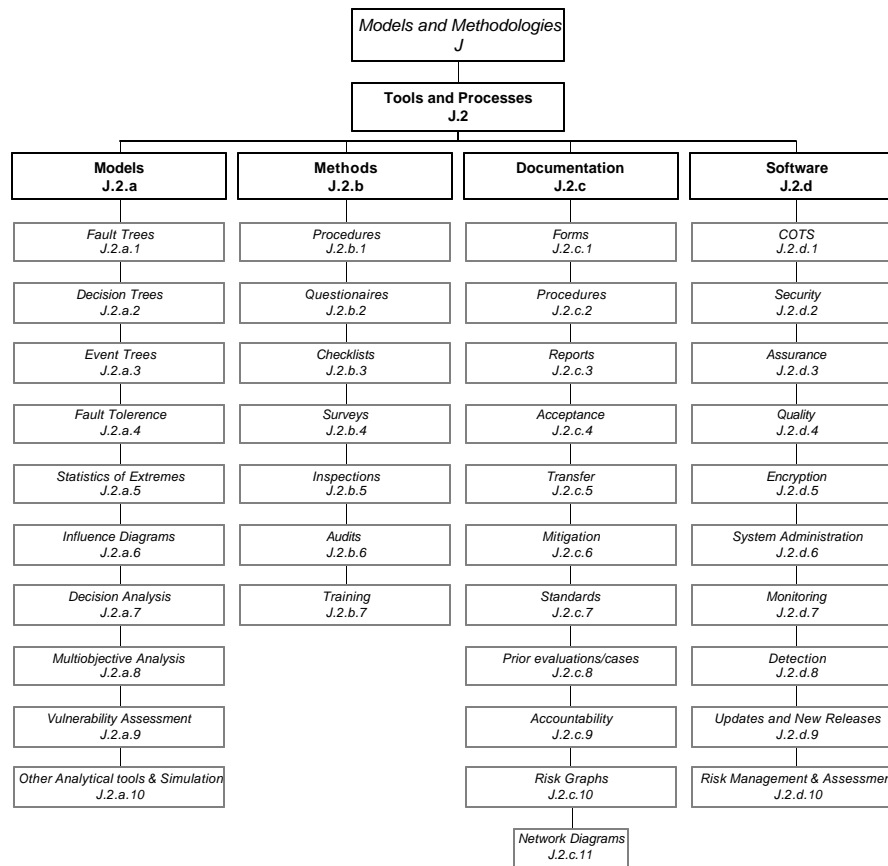


Figure 100: HHM Diagram (Head-topic: J.2)

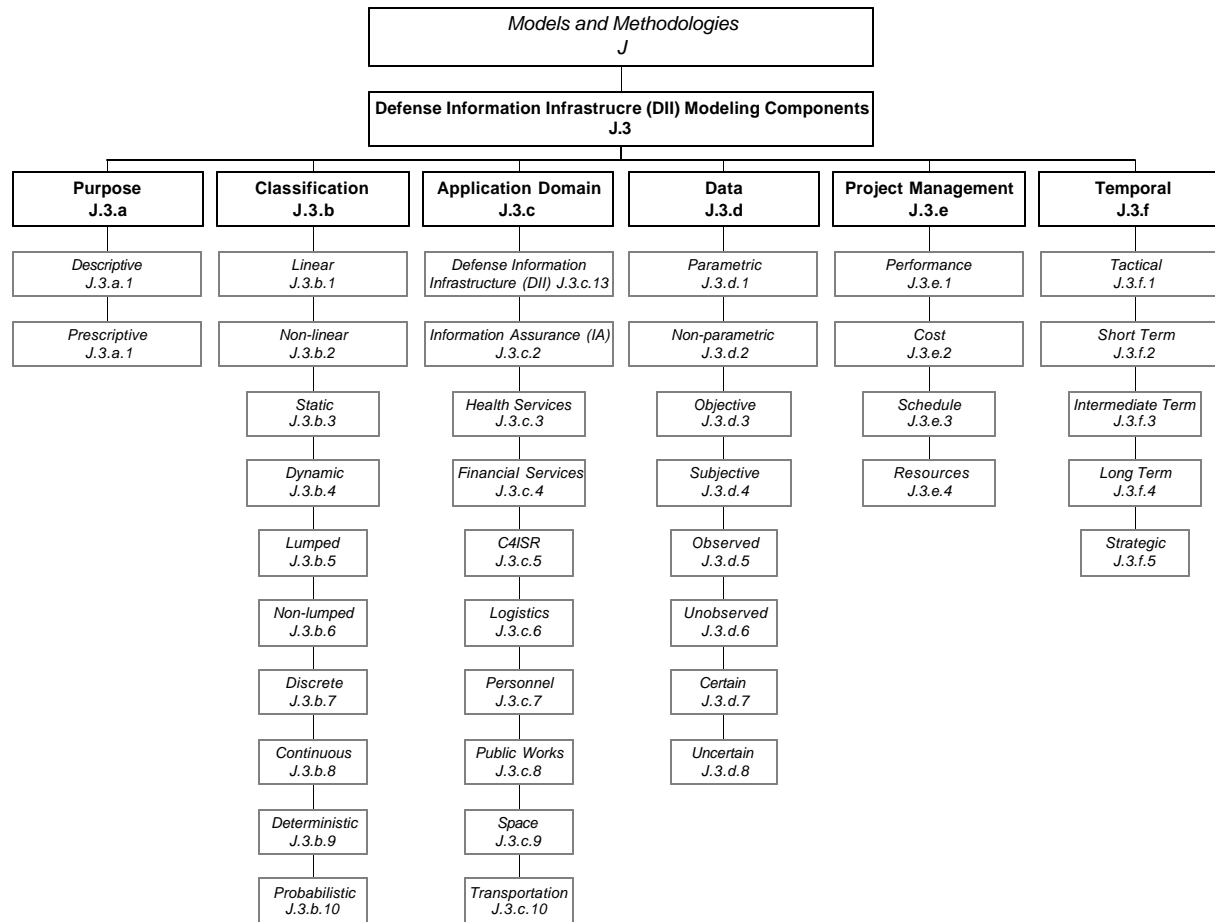


Figure 101: HHM Diagram (Head-topic: J.3a-J.3f)

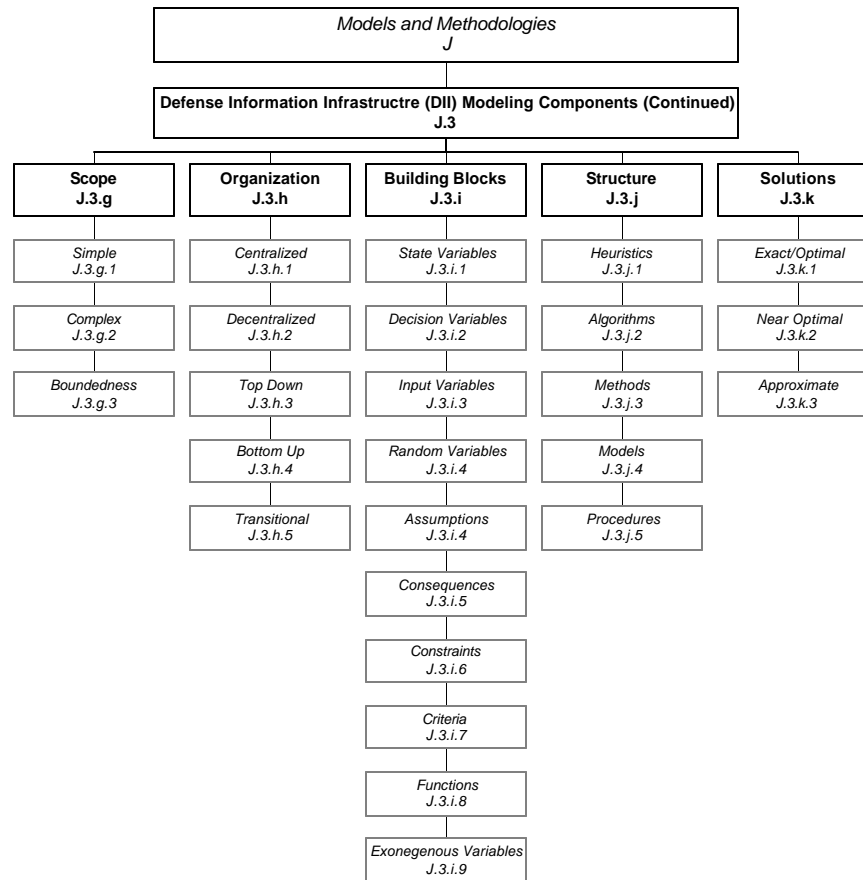


Figure 102: HHM Diagram (Head-topic: J.3g-J.3k)

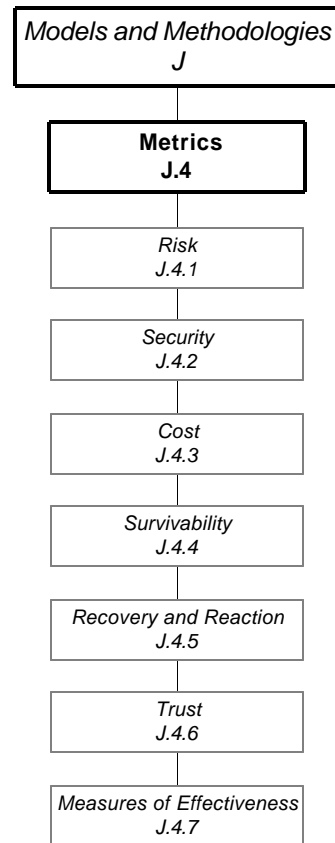


Figure 103: HHM Diagram (Head-topic: J.4)

Appendix C: IA Metric Definitions and Representations

Table 36 encapsulates the IA metrics, their definitions and representation. The table has four columns depicting the following attributes:

- *Column-one*: Represents the reference numbers for each IA metric.
- *Column-two*: Depicts the IA metric nomenclature.
- *Column-three*: Depicts a definition for each IA metric, which shows the conditions where the metric could be used.
- *Column-four*: Illustrates an equation or a representation for each metric that clearly shows the context and value of the metric.

#	IA Metric	Metric Definition	Equation or Representation
M.1	Algorithmic Efficiency	Reflects the complexity of the algorithm implemented to solve the problem.	<p>Defined as the Big-O Notation where O means on the order of [Fenton, 1997]. Algorithm efficiency is an excellent comparison metric.</p> <p>Examples of the worst case:</p> <ul style="list-style-type: none"> • Quick Sorting List Algorithm: $O(n \log(n))$. • Bubble Sorting Algorithm: $O(n^2)$. • Comparison Algorithms: $O(n^2)$.
M.2	Bit Error Rate (BER) [Whatis.com, 2001]	The percentage of bits that have errors relative to the total number of bits received in a transmission. The BER is an indication of the quantity of retransmission bits for a given transmission. BER is usually expressed as ten to a negative power [Whatis.com, 2001].	$BER = \frac{\sum_{i=1}^{\infty} Errors}{N}$ <p>, where</p> <ul style="list-style-type: none"> • Errors are the number of incorrect bits. • N is the total number of bits for a set transmission.
M.3	Buffering Factor	The number of components (i.e., security, authentication and authorization interfaces, gateway and proxy servers, and firewalls) in place that increases the difficulty and effort in gaining access to information storage and access points.	<p>Buffering Factor = $\sum_{i=1}^{\infty} (a_i) + \sum_{i=1}^{\infty} (b_i) + \sum_{i=1}^{\infty} (c_i) \dots$; where</p> <ul style="list-style-type: none"> • $i=1$ to n (n is a relative small number). • a_i is the first type of interface component. • b_i is the second type of interface component. • And so on.
M.4	Complexity (Coupling)	Coupling complexity is the number of lines (connections) entering and leaving a system or component [Jones, 1998].	<p>Complexity (Coupling) = length (fan-in * fan-out)²</p> <ul style="list-style-type: none"> • Length is may be measured by Lines of Code, length of connections or some other size metric. • Fan-in and fan-out are the measure of entering and leaving connections from the component.

M.5	<i>Complexity (Halstead)</i> [Jones, 1998]	The Halstead complexity metric (H) [Jones, 1998] is based on information theory and psychology and measures software complexity using number of operators and operands instead of length.	$H = n_1 \log_2 n_1 + n_2 \log_2 n_2$; where <ul style="list-style-type: none"> n_1 is the number of distinct operators in the software. n_2 is the number of distinct operands in the software.
M.6	<i>Complexity, Software (McCabe)</i> [Jones, 1998]	The McCabe software complexity metric measures the decision complexity within loops and conditional statements in software. The metric places the same weight on nested and un-nested loops.	McCabe Software Complexity = One more than the number of binary decisions for a proper program
M.7	<i>Complexity, Structure (McCabe)</i> [Jones, 1998]	The McCabe Cyclomatic Complexity Metric (M) [Jones, 1998] measures the number of linearly independent paths of a system.	$M = L - N + 2P$; where <ul style="list-style-type: none"> L is the number of links into and out of the system. N is the number of nodes or subcomponents of the system. P is the number of disconnected parts (if none then $P=1$).
M.8	<i>Confidentiality Levels</i>	The number of informational categorical divisions arranged for the purpose of segregating information away from unauthorized personnel.	Confidentiality Levels = # of unique information separation categories within an organization or system (e.g., secret, classified, unclassified).

M.9	<i>Coupling Interaction Index</i>	Measures the relationship between components and systems. A level and a scale (e.g., extremely high, low) represent the index. Extremely high corresponds to a system with large consequences but low occurrence probabilities. Low corresponds to a system with small consequences but moderate to high occurrence probabilities. These relationships are indicated with a coupling interaction index. Tight coupling systems have very little slack between them. Loose coupling systems have flexibility between them. Linear interactions are those expected production or maintenance sequences that are visible even if unplanned. Complex interactions are unfamiliar or unplanned sequences that are not visible or not immediately comprehended [Perrow, 1999].	<p><u>Index:</u></p> <ul style="list-style-type: none"> • <i>Extremely High:</i> Tight, Complex (e.g., space, aircraft and nuclear operations). • <i>High:</i> Loose, Complex (e.g., military functions and missions). • <i>Moderate:</i> Tight, Linear (e.g., power grids, and dam operations). • <i>Low:</i> Loose, Linear (e.g., Assembly line productions).
M.10	<i>Cryptographic Work Factor (Number)</i>	Number of operations required to break a cryptographic system [Nichols, 1999].	Quantitative number usually written as 2^n . Where n is the number of bits contained in the cryptographic key. The higher the number, the longer it takes to break the key structure.

M.11	<i>Cryptographic Work Factor (Time)</i>	The amount of time it takes to break a cryptographic system.	<p>Temporal number related to number of system operations used to break a cryptographic key structure. For example, the amount of time to break a 40, 56, 64 and 128-bit key for 1995, 2000, and 2005 (predicted based on Moore's Law) is listed below, respectively [Erkomaa, 1998].</p> <ul style="list-style-type: none"> • 40-bit: 68 hours, 8.6 minutes, 1.07 minutes. • 56-bit: 7.4 weeks, 6.5 days, 19 hours. • 64-bit: 36.7 years, 4.6 years, 6.9 months. • 128-bit: 6.7×10^{17} millennia, 8.4×10^{16} millennia, and 1.1×10^{16} millennia. <p>The Data Encryption Standard (DES) algorithm uses a 56-bit key and was broken by a distributed network in 22 hours [Stallings, 1999].</p>
------	---	--	--

M.12	Data Immunity	The probability that the information from a system is correct and can be validated.	<ul style="list-style-type: none"> • <i>Probability (0.00 to 0.25)</i>: The information is from an un-trusted source. Interaction with the system has never been executed prior to this time. There is no system or policy in place to validate or verify the receiving user or system. • <i>Probability (0.26 to 0.50)</i>: The information is from a fairly un-trusted source. Interaction with the system has been executed a few times or on an irregular basis. There is no system or policy in place to validate or verify the receiving user or system. • <i>Probability (0.51 to 0.75)</i>: The information is from a trusted source confirmed with the use of technology or policy. Interaction with the system is executed on a fairly regular basis. There is a system or policy in place to validate or verify the receiving user or system. • <i>Probability (0.76 to 1.00)</i>: The information is from a trusted source and transactions are executed on a daily basis. There is technology or a policy in place to validate or verify the receiving user or system, which is constantly upgraded and maintained.
M.13	Data Transfer/Access Rate	The rate of bits that can be transferred or accessed on a system per second.	<p>Date Rate = $\frac{N}{T}$; where</p> <ul style="list-style-type: none"> • N is the number of bits for a specific interval of time (T).

M.14	Defect Density Measure	This measure is used to determine the reliability growth of a system during the design phase [Dhillon, 1999]. This metric requires the generation of defect severity categories and must possess some ambiguity.	$q_{cd} = \sum_{i=1}^a \frac{N_i}{L}; \text{ where}$ <ul style="list-style-type: none"> • θ_{cd} is the cumulative defect ratio for design. • α is the total number of reviews. • N_i is the total number of unique defects, at or above a give severity level, discovered in the i^{th} design review. • L is the number of source lines of design statement express in thousands (non-commented and commented lines).
M.15	Defect Density per Line of Code (LOC) [Humphrey, 1989]	The number of defects (i.e., the improper program conditions resulting from an error related to improper program packaging or handling) per 1000 lines of source code [Humphrey, 1989].	$\text{Defects(LOC)} = \frac{\sum_{i=1}^{\infty} (\text{Defects Detected})}{\sum_{i=1}^{\infty} (\text{Total Software Length (LOC)})}$ $\text{LOC} = \text{NCLOC} + \text{CLOC}$ <ul style="list-style-type: none"> • NCLOC is non-commented lines of code. • CLOC is commented lines of code.
M.16	Detectability	Refers to the likelihood that the system recognizes the initial events of a failure or attack before damage to the system.	Probability (Detectability)= (Event Detected Damage will Occur)
M.17	Duration of Effects	The total range of time of the consequences related to an IA incident.	Duration of the Effect = (Initial Consequences Detected(t_0))- (Consequence are eliminated or mitigated(t_n)) where, <ul style="list-style-type: none"> • T_0 is the time when the initial negative event leading to a consequence is noticed. • T_n is the time when the consequence from the negative event is eliminated or mitigated.

M.18	Effort	The formula represents Boehm's effort model, which states that the effort required to develop a software system (measured by E in person months) is related to size (measured by S in thousands of delivered source states) [Fenton, 1996].	$E = aS^b$; where <ul style="list-style-type: none"> • a and b parameters are determined by the type of software system developed. • Examples of a and b constants [Fenton, 2000] <ul style="list-style-type: none"> - Organic Systems: $a=2.4$, $b=1.05$ - Organic Systems: $a=3.0$, $b=1.12$ - Organic Systems: $a=3.6$, $b=1.20$
M.19	Expected Effect on Adversary's Decisionmaking Abilities	A categorical representation of the measure of consequence due to an organization's countermeasures prior to a system attack. For example, by increasing the level of security for equipment and personnel or increasing the amount of detection capabilities through technological advances, an organization can impact purposely or inadvertently an adversary's decisionmaking cycle.	<p><i>High:</i> Adversary decisionmaking capabilities are diminished and show a considerable delay in execution.</p> <p><i>Medium:</i> Adversary decisionmaking capabilities are degraded in some manner and show a minor delay in execution.</p> <p><i>Low:</i> Adversary decisionmaking capabilities are not impacted and show no delay in execution.</p>
M.20	Expected Value of Risk	The sum of the product of the probabilities and their associated random variable values.	$E[X] = \int_0^{\infty} xp(x)dx$; where <ul style="list-style-type: none"> • x is a random variable. • $p(x)$ is the probability density function.

M.21	Failure Rate	The number of failures (i.e., a malfunction of a user's installation, which may result from a bug, incorrect installation, communication interruption, a hardware fault, etc. [Humphrey, 1989]) per unit of measure for an integrated system or circuit. In this metric example, failure rates are measured in failures per million hours.	$I = p_L p_Q (C_1 p_T + C_2 p_E) p_P$; where <ul style="list-style-type: none"> π_L is a learning factor (process maturity). π_Q is a quality factor (testing process). π_T is a temperature factor (device technology: operating temperature and power dissipation, etc.). π_E is an environmental factor (harshness). C_1 and C_2 are complexity factors. <p>Typical values for all variables are found in Johnson [1989].</p>
M.22	Fault Location Coverage	The measure of a system's ability to detect and locate a specific fault or failure given that a fault exists [Johnson, 1989].	Coverage = Probability (Fault Recovery Fault Existence)
M.23	Frequency of Failure (Unconditional Failure Intensity)	The number of failures detected in a system per unit time given that the component was as good as new at time zero [Whatis.com, 2001].	$\text{Failure Frequency} = \frac{\sum_{i=1}^{\infty} (X_i)}{\text{Time(Interval)}} ;$ <p>where</p> <ul style="list-style-type: none"> X_i is the sum of the failures detected in the system.
M.24	Hamming Distance	The distance between any two binary strings representing the number of differences in which information differs. For example, the binary strings 0001 and 1001 have a hamming distance of 1. The measure gives insight into error detection and correction, and information integrity [Fenton, 1996].	<p>Hamming Distance = The difference in the bit arrangement of Transmission A and Transmission A'.</p> <ul style="list-style-type: none"> Transmission A is the original transmission sequence and Transmission A' is the changed transmission sequence if any has occurred.

M.25	Hardness	<p>A categorical measure of the difficulty in partially or fully penetrating a system. The metric is modeled after the Mohs hardness scale used for minerals. Five minerals from the 10 standard minerals were used to represent computer system hardness.</p>	<p><i>Talc (Hardness Level 1):</i> The product or service has not been tested, validated and verified by any independent agency and any claims representing the difficulty of penetrating the product or service with harmful intent is untrustworthy. In the lifetime (i.e., being used in the marketplace) of the product or service, there have been several documented penetrations.</p> <p><i>Gypsum (Hardness Level 2):</i> The product or service has not been tested, validated and verified by any independent agency and any claims representing the difficulty of penetrating the product or service with harmful intent is untrustworthy. In the lifetime of the product or service, there have been numerous (more than 5) documented penetrations.</p> <p><i>Quartz (Hardness Level 3):</i> The product or service was tested, validated and verified by one independent agency to the difficulty of penetrating the product or service with harmful intent. In the lifetime of the product or service, there have been a few (2-5) documented penetrations and measures to fix the vulnerabilities were actively taken.</p> <p><i>Topaz (Hardness Level 4):</i> The product or service was tested, validated and verified by more than two independent agencies to the difficulty of penetrating the product or service with harmful intent. In the lifetime of the product or service, there is one documented penetration and measures to fix current and future vulnerabilities were actively taken.</p> <p><i>Diamond (Hardness Level 5):</i> Tested, Validated and Verified by more than three independent agencies (each agency is represented by Academia, Industry and the Federal Government) to the difficulty of penetrating the product or service with harmful intent. In the lifetime of the product or service, there were zero documented penetrations.</p>
------	----------	--	---

M.26	Hazard Function	<p>The probability for failure at a specified time, given that it survived to that time (t). [McCormick, 1981]. Hazard function (h(t)) is expressed failures per unit time and may be related to the Survivor function (S(t)) by a probability density function (f(t)) [Leemis, 1995].</p>	$I(t) = -\frac{1}{R(T)} \frac{dR(t)}{dt}; \text{ where}$ <ul style="list-style-type: none"> • $\lambda(t)$ is the hazard rate • $R(T)$ is the reliability function expressed by $R(T) = e^{-\int_0^t I(t) dt}$ $S(t) = e^{-(I t)^k}; \quad t \geq 0$ $f(t) = I k (I k)^{k-1} e^{-(I t)^k}; \quad t \geq 0$ $h(t) = \frac{f(t)}{S(t)} = I k (I k)^{k-1}; \quad t \geq 0$ <ul style="list-style-type: none"> • λ is the positive scale parameter. • κ is the positive shape parameter.
M.27	Hurdle Rate	<p>The minimum rate of return (ROI) that proposed investments is expected to achieve in improving productivity [Putnam, 1992].</p>	$ROI = \frac{(Cost\ reduction - Investment)}{(Investment) * (\#\ of\ years)};$ <ul style="list-style-type: none"> • This model ignores the time cost of money.
M.28	IA Personnel Trained	<p>The percent of trained personnel on IA related subjects above a described threshold set by an organization.</p>	$IA\ Trained\ Personnel = \frac{\sum_{i=1}^N (X_i)}{N} * 100; \text{ where}$ <ul style="list-style-type: none"> • N is the total number of personnel in the organization. • X_i is the number of personnel trained in IA tasks, process or functions defined by the organization.

M.29	<i>Incident Occurrence</i>	The frequency of similar incidents that transpire in a described range of time.	$\text{Incident Occurance} = \frac{\sum_{i=1}^{\infty} (X_i)}{\text{Time}} ; \text{ where}$ <ul style="list-style-type: none"> • X_i is the number of similar incidents within a specified timeframe.
M.30	<i>Incident Recovery Time</i>	The amount of time it takes a system to recuperate its processes or components to its original level of performance.	Recovery Time = Time (T_f) when system is equal to or above "normal" operational threshold minus Time (T_0) when system has fallen below set operational threshold.
M.31	<i>Incident Response Time</i>	The amount of time it takes a system to identify and respond to an incident by processing the type, level and severity of the incident and taking appropriate measures to correct the faults, vulnerabilities, failures and damages.	ResponseTime = Time (T_f) - Time (T_0) ; where <ul style="list-style-type: none"> • T_f is the final time when the appropriate measures are completed. • T_0 is the initial time of identifying and responding.
M.32	<i>Information Corruption Rate</i>	The amount of bits per unit time for a system to accidentally destroy, degrade and corrupt information residing on the system within the context of ordinary use.	$\text{Corruption Rate} = \frac{\text{Number of Corrupted Bits}}{\text{Time(Interval)}}$

M.33	Information Entropy	<p>A measure of uncertainty ($h(x_i)$) to each random value x_i, then the total uncertainty ($H(x)$) is the lack of knowledge, or the disorder in the space of the variable X. Entropy is related to the concepts of uncertainty, surprise, and predictability. A less probable event gives us more surprise, less predictability but after the event occurs there is an increase in the amount of information to the user [Kasobov, 2000]. Entropy is measured in time and gives the user an understanding of information loss or gain based on received information. Intrusion detection and sensor information or lack of information equates to some entropy and value of the information. Information Entropy can be used to measure uncertainty, rate of information acquisition and selecting criterion for the choice of probability distributions [Preuber, 1997]</p>	$H(x) = -\sum_{i=1}^n p_i (\log(p_i)) = -\sum_{i=1}^n p_i (\log_2(p_i)) =$ $H(x) = \sum_{i=1}^n (\log_2(N))$ $\text{Network Performance} = \left(\frac{H_{T(\text{prior})} - H_{T(\text{Posterior})}}{H_{T(\text{prior})}} \right) * 100$ $P(x) = \text{Predictability} = 2^{-H(x)}$ $\text{Information Loss Curve (Entropy)} = -\ln(t^2)$ <p>where</p> <ul style="list-style-type: none"> • P_i is the probability of the event and can be related to N (Number of Occurrences). • Preuber [1997] discusses Network Performance and related variables. • Willis [2000] discusses information loss curve concept. <p><u>Shannon entropy:</u></p> <ol style="list-style-type: none"> 1. No information <ul style="list-style-type: none"> • Lots of order • Shannon entropy small 2. Potentially lots of information <ul style="list-style-type: none"> • Disorder • Shannon entropy high
M.34	Information Timeliness	<p>The difference in the amount of time it takes for information to be requested and received by a user or system.</p>	<p>Timeliness =</p> $\text{Requested Time } (T_q) - \text{Received Time } (T_r)$

M.35	Information Value	The net worth of information or information system by relating its value to the age of information, and the effort and cost of constructing, protecting, storing and rebuilding the information.	<p><i>Information Value</i> = $A + C + E$; where</p> <ul style="list-style-type: none"> • A is the cost representing the age of the information. Cost of storing the information, and the sensitivity of the information. • C is the cost of constructing, protecting and storing the information. • E is the cost of effort (man-hours or man-years) to construct, protect and store the information.
M.36	Information Value Levels	A categorical depiction of the net worth of the effects and consequences of losing information or information systems [NSA, 1999].	<p><i>Level 1</i>: Violation of the information protection policy would have negligible adverse effects or consequences.</p> <p><i>Level 2</i>: Violation of the information protection policy would adversely affect and/or cause minimal damage to the security, safety, financial posture, and/or infrastructure of the organization.</p> <p><i>Level 3</i>: Violation of the information protection policy would cause some damage to the security, safety, financial posture, and/or infrastructure of the organization.</p> <p><i>Level 4</i>: Violation of the information protection policy would cause serious damage to the security, safety, financial posture, and/or infrastructure of the organization.</p> <p><i>Level 5</i>: Violation of the information protection policy would cause exceptionally grave damage to the security, safety, financial posture, and/or infrastructure of the organization.</p>

M.37	<i>Lifecycle Costs (LCC)</i> [Dhillon, 1999]	Lifecycle costs of a system are represented by several unique inputs. There are three general models discussed in Dhillon [1999], which estimate the lifetime cost of a system.	$LCC = RC + NRC$ $LCC = RDC + PCC + OSC + DC ; \text{ where}$ $LCC = IC + OC + FC$ <ul style="list-style-type: none"> • RC is recurring cost consisting of maintenance, operating, support, labor and inventory costs. • NRC is non-recurring costs consisting of training, procurement, management, support, transportation, research and development, test equipment, installation, etc. • RDC is research and development costs consisting of software, management, engineering design, evaluation, etc. • PCC is production and construction cost. • OSC is operation and support cost consisting of distribution, product operation, sustaining logistic support costs. • DC is disposal cost and is expressed by an equation in Dhillon [1999]. • The third model is made up by three major components consisting of initial costs (IC), operating cost (OC) and failure cost (FC). Each component is expressed by an equation in Dhillon [1999].
M.38	<i>Likelihood of Gaining Access to System</i>	The probability that a system is penetrated through any entry point. Event trees are an excellent means to calculate the system access likelihood.	$\text{Access probability} = P(\text{The system is penetrated})$
M.39	<i>Lost Information Percentage</i>	The ratio of missing, stolen or corrupted bytes of information over the total number of bytes of information for a particular system.	$\text{Lost Information} = \frac{\text{Number of Bits Lost}}{\text{Total Number of Bits Stored}}$

M.40	Manpower Utilization Rate	The number of people utilized for a defined project. Measured in man-months per month, or man-years per year. Manpower buildup follows a Rayleigh distribution. [Putnam, 1992]	$y = K(1 - e^{-at^2})$; where $y' = 2Kat(e^{-at^2})$ <ul style="list-style-type: none"> y is the cumulative effort. y' is the effort per time period (Man-months per month). K is the total effort to the end of project (i.e., recovery project after an accident, attack or failure). t is the elapsed from the start of the cycle. a is the shape parameter that governs the rate at which the curve approaches peak manpower.
M.41	Mean Effort to Reach Target	The average amount of force used by an adversary to maneuver through the shortest path of a system. The mean effort is measured in time and the adversary's intentions are to control the system to cause failure, vulnerability with the system, organization or mission or to extract information.	$Mean\ Effort\ (Target) = \frac{\sum(\#\ of\ time\ units)}{N}$; where <ul style="list-style-type: none"> Unit time can be measured in seconds, minutes, hours, etc. The units must be consistent throughout the measurement. N is total number of times the experiment is run on a particular system.
M.42	Mean Time Between Failures (MTBF) [Storey, 1996]	The functional life of an item divided by the total number of failures during that time [Storey, 1996].	$MTBF = MTTF(I^{-1}) + MTTR(m^{-1})$ If $\lambda(t)$ and $\mu(t)$ are constant and $\lambda \ll \mu$. <ul style="list-style-type: none"> This also assumes that the system has random repairs and no repairs after a failure.

M.43	Mean Time to Failures (MTTF) [Storey, 1996]	The expected time that a system will operate before the first failure occurs. Availability is the MTTF divided by the sum of the MTTF and the mean time to repair (MTTR). [Storey, 1996]	$MTTF(I^{-1}) = E(T) = \int_0^{\infty} e^{-I t} dt = \frac{1}{I};$ where <ul style="list-style-type: none"> λ is the failure rate of a component or system. $E(T)$ is the expected value.
M.44	Mean Time to Human Error (MTTHE) [Dhillon, 1999]	The expected mean time of a human error occurrence related to the human performance reliability function [Dhillon, 1999]. The MTTHE equation can be used with any known distribution function but data indicates the Weibull, gamma, and lognormal distributions fit the human error data quite well.	$MTTHE = \int_0^{\infty} R_h(t) dt = \int_0^{\infty} \exp \left[- \int_0^t I(t) dt \right] dt;$ where <ul style="list-style-type: none"> R_h is the human performance reliability. t is measured in time (usually in hours). $\lambda(t)$ is the error rate per hour.
M.45	Mean Time to Repair (MTTR) [Storey, 1996]	The average time taken to repair a system which has failed and return the system to operational status [Storey, 1996].	$MTTR(\mu^{-1}) = \frac{1}{\mu} = \frac{\sum_{j=1}^k I_j T_j}{\sum_{j=1}^k I_j};$ where <ul style="list-style-type: none"> μ^{-1} is the average repair rate. λ_j is the constant failure rate of unit j; for $j=1, 2, 3, \dots, k$. k is the total number of units. T_j is the corrective maintenance or repair time required to repair unit j; for $j=1, 2, 3, \dots, k$.
M.46	Mission Time	The measure of time at which the reliability of a system falls below the level r indicated by a user [Johnson, 1989].	$MT[r] = \frac{-\ln(r)}{I};$ where <ul style="list-style-type: none"> λ is the constant failure rate r is the threshold reliability measured in time.

M.47	<i>Natural Disaster Detection Likelihood</i>	The probability that a system or user identifies a failure, or fault given a natural disaster (e.g., wind, hurricane, tornado, rain) occurs. Event trees are an excellent means to calculate this likelihood.	<i>Disaster Probability</i> = $P(\text{Failure or Fault is Detected} \mid \text{A Natural Disaster Occurs})$
M.48	<i>Number of Access Points per System (Permeability)</i>	The amount of system back door, entry and exit points. The number of attack paths to target and/or critical failure points within a system. The metric is a measure of the permeability of the total system.	<i>Permeability</i> = # of Access Points (Entry and Exit)
M.49	<i>Number of Dissimilar Systems</i>	Homogeneous systems imply that component systems share vulnerabilities [Trust, 1999]. Having dissimilar systems increases the likelihood of organizational operability when certain vulnerabilities are exploited.	The number of dissimilar systems in a given information network providing similar services (e.g., common and control, database storage, information retrieval).
M.50	<i>Number of Documented Risks</i>	The number of documented risks for a given system, process or organization using a systematic and comprehensive tool (e.g., Hierarchical holographic Modeling). This is a subjective measurement of the risk an organization can potentially manage or mitigate.	<i>Documented Risks</i> = # of identified risks for a particular system or process.
M.51	<i>Number of Eradicated Viruses</i>	The amount of viruses eradicated from systems within an organization divided by the total number of systems.	$\text{Eradicated Viruses} = \frac{\text{Number of Eradicated Viruses}}{\text{Total Number of Systems}}$
M.52	<i>Number of Parallel Security Mechanisms</i>	The number of parallel security mechanism in the total system. Parallel mechanism provides more reliability, availability, security and redundancy over serial mechanisms.	<i>Parallel Security Mechanisms</i> = # of parallel mechanisms within a specified system.
M.53	<i>Number of Serial Security Mechanisms</i>	The number of serial security mechanism in the total system. Serial mechanism provides less reliability, availability, security and redundancy over parallel mechanisms.	<i>Serial Security Mechanisms</i> = # of serial mechanisms within a specified system.


M.54	Outage-Index Metric	The outage-index metric (I(O)) characterizes a telecommunications outage by incorporating service, duration and magnitude weights [Snow, 2000].	$I(O) = \sum_{j=1}^N W_{s_j} W_{d_j} W_{m_j} ; \text{ where}$ <ul style="list-style-type: none"> • j-1,.....,N are the service impacted by the outage, W_s=Service Weight, W_d=Duration Weight, and W_m=Magnitude Weight. • Magnitude Weights range from 0.00 to 16.67. Magnitude weights must also be multiplied by a Time Factor (TF) which range from 0.00 to 2.50: <ul style="list-style-type: none"> - TF=1.00 for daytime - TF=0.3 for evening - TF=0.2 for weekends, and - TF=0.1 for late night
M.55	Performability	The probability that a system operates at equal to or above a set threshold at a specific instant of time. It may also represent the probability that a number of processors or components are available or that a component will accomplish a specific mission or task at time t. This measure differs from reliability by focusing on the likelihood that a subset of functions is performed correctly [Johnson, 1989].	Performability = Probability (The system is operating at a set threshold at time t)
M.56	Personnel Turnover Rate	The rate personnel in an organization leave or are added to an organization for a specified period of time. This does not include personnel reductions based on organizational restructuring.	$\text{Personnel Turnover Rate } (T_f - T_0) = \frac{\text{Personnel Leaving Organization}}{\text{Total Number of Personnel in the Organization}} * 100 ;$ <ul style="list-style-type: none"> • $(T_f - T_0)$ is the period of time considered.

M.57	<i>Predicted Number of Faults</i>	The number of faults predicted (B) in a program is based on Halstead's belief that software complexity is based on the number of operators and operands [Bryan, 1998].	$B = \frac{(n_1 + n_2) \log(n_1 + n_2)}{3000}; \text{ where}$ <ul style="list-style-type: none"> • n_1 is the number of distinct operators in the software. • n_2 is the number of distinct operands in the software.
M.58	<i>Potential Effect (Type I Error)</i>	The probability of rejecting truthful information based on some set conditions. This equates to a false negative reading. An example is a Army unit rejecting information on enemy targets and designating them as friendly forces.	<i>Potential Effect (Type I Error) Probability=</i> Probability (Rejecting the Information and the Information is True)
M.59	<i>Potential Effect (Type II Error)</i>	The probability of accepting false information on some set conditions. This equates to a false positive reading. An example is a unit accepts information on tripped sensors and increases the security of the unit even though the sensor information is incorrect. This has less harm to an organization compared to a Type I Error.	<i>Potential Effect (Type II Error) Probability=</i> Probability (Accepting the Information and the Information is False)
M.60	<i>Processing Time for Reconfiguration</i>	The amount of time it takes for a system to arrange the appropriate hardware components, software processes or user manual tasks to respond to a failure or attack.	Processing Time (Reconfiguration) = Time (T_f) - Time (T_0) ; where <ul style="list-style-type: none"> • T_f is the final time when the appropriate reconfiguration measures are completed. • T_0 is the initial time of reconfiguration.

M.61	<i>Processing Time for System Update</i>	The amount of time it takes for a system or process to identify, request, receive and then process an update in order to fix a vulnerability or security flaw.	<p>ProcessingTime (Update)= Time (T_f) - Time (T_0) ; where</p> <ul style="list-style-type: none"> T_f is the final time when the update is complete. T_0 is the initial time of starting to update the system or process to identify, request, receive and then process a vulnerability or security type update.
M.62	<i>Recovery Operational Percentage (24-hours)</i>	The operational percentage regained within 24-hours, after critical functions or operations are degraded from failures, faults or attacks on a system. It is critical for an organization to become fully operational after an IA incident.	$\text{Recovery \%} = \frac{\text{Percent regained in 24 - hours}}{\text{Original Operating Percentage}}$
M.63	<i>Redundancy Ratio</i>	The amount of hardware, software, or information that the system operationally requires divided by the amount of non-redundant entities that perform the same function [Johnson, 1989].	<p>Redundancy Ratio = $\frac{H_r}{H_{nr}}; \frac{S_r}{S_{nr}}; \frac{I_r}{I_{nr}}$; where</p> <ul style="list-style-type: none"> H_r and H_{nr} is amount of Redundant Hardware and Non-redundant Hardware, respectively. S_r and S_{nr} is amount of Redundant Software and Non-redundant Software, respectively. I_r and I_{nr} is amount of Redundant Information (Bits) and Non-redundant Information (Bits), respectively.
M.64	<i>Repair Rate Function</i>	The function measures the rate in which a system or components are repaired after faults or failures are noted by the system or user. The repair rate is measured in units of repairs per unit of time.	<p>Repair Rate = $\frac{1}{N_{nr}(t)} \frac{dN_r(t)}{dt}$; where</p> <ul style="list-style-type: none"> $dN_r(t)$ is the derivative of $N_r(t)$, which is the rate at which component are repaired at time t. $N_{nr}(t)$ is the amount of un-repaired systems at time t.

M.65	Resource Availability	The percentage of an essential resource (i.e., time, personnel, information, cost, system components) remaining after an incident. This can also represent the amount of a resource consumed for a given process (e.g., personnel for virus eradication or time for incident response procedures).	Resource Availability = $\frac{\text{Current Resource Percentage}}{\text{Resource Percentage Prior to Incident}} * 100$
M.66	Risk Leverage	The difference between the risk exposure before reduction and risk exposure after reduction over the cost of risk reduction [Pfleege, 2000]. Risk exposure is the probability that an event will occur multiplied cost of the event occurring.	Risk Leverage = $\frac{\text{Risk Exposure before Reduction} - \text{Risk Exposure after Reduction}}{\text{Cost of Risk Reduction}}$
M.67	Risk Severity Classification	A matrix that defines frequency verses consequences. Frequency is depicted by five classes (frequent, probable, occasional, remote, and improbable) and four accident risk classes (A, B, C, and D), where A represents the most serious and D the least serious [Storey, 1996].	The two-dimensional matrix is illustrated in Figure 26. Each box depicts a cause and an effect for a specific risk. Other effect classifications include: catastrophic, critical, marginal and negligible. Other cause classifications include: moderate, occasional, remote, improbable, incredible, and impossible [Leveson, 1995]. The interpretation for the effect and cause classifications is organizational definitions.
M.68	Social Cost	A measure of the social costs of disabilities by placing a value on a human life. The National Safety Council places 6,000 days typically are selected to be equivalent to a fatality [McCormick, 1998]. This metric can be adapted to approximate the cost of having a critical system or infrastructure disabled from a failure or attack.	$\text{Total Social Cost} = NC(1+i)^t, \quad t < 6000$ $= NC(1+i)^{6000}, \quad t \geq 6000$ <p>where</p> <ul style="list-style-type: none"> • N is the number of individuals involved. • C is the cost of one disability day. • i is daily interest rate. • t is the time in consecutive days of disability.

M.69	<i>Software Capability Maturity Model</i>	<p>A categorical representation of the set of tools, methods, and practices used to produce a functional and quality software product. The five levels are initial, repeatable, defined, managed, and optimized, and represent an increasing order in formality [Humphrey, 1989].</p>	<ul style="list-style-type: none"> • <i>Level 1 (Initial)</i>: Few processes are defined and are sometimes chaotic in nature. • <i>Level 2 (Repeatable)</i>: Basic project management processes are established to track cost, schedule and functionality of the product. • <i>Level 3 (Defined)</i>: The engineering and management activities are documented, standardized and integrated into the organizational process. • <i>Level 4 (Managed)</i>: Measures of the process are collected and are quantitatively analyzed and understood. • <i>Level 5 (Optimized)</i>: Continuous process improvement using feedback mechanisms and data analysis.
------	---	---	---

M.70	Software Function and Feature Points	 <p>Focuses on the software problems within a product instead of the size of the product. Software engineering has measured the productivity and cost (effort of production and reliability) with lines of code (LOC) [Fenton, 1996]. The metric is called Non-Commented Single Lines of Code (NSLOC) but does not capture the complexity or the language level of the code [Miller, 1993] [Fenton, 1996].</p>	$Functional\ Points = \left[\begin{array}{l} (Wi)(\# \text{ of inputs}) + (Wo)(\# \text{ of outputs}) + \\ (Wq)(\# \text{ of inquiries}) + (Wf)(\# \text{ of files}) + \\ (We)(\# \text{ of external interfaces}) \end{array} \right] *$ <p>[Technical Complexity] [Adjustment]</p> <ul style="list-style-type: none"> • <i># of inputs</i>: Each user input providing distinct application-oriented data is counted; queries counted separately. • <i># of outputs</i>: Numbers of reports, screens, error messages, etc. • <i># of inquiries</i>: On-line request followed by an immediate response. • <i># of files</i>: number of master files. • <i># of external interfaces</i>: number of machine-readable interfaces (e.g., data files on tape or disk). • <i>Weighting factors (W)</i> are different for simple, average, complex system (e.g., average weights: 4, 5, 4, 10, and 7). • Technical Complexity Adjustment = <ul style="list-style-type: none"> - 0.65 + (0.01)(Total Degree of Influence) - Total Degree of Influence Parameters <ul style="list-style-type: none"> ▪ Not Present=0 ▪ Insignificant Influence=1 ▪ Moderate Influence=2 ▪ Average Influence=3 ▪ Significant Influence=4 ▪ Strong Influence, throughout=5
------	--------------------------------------	---	--

M.71	Software Vulnerabilities	This metric is based on Newman's Law, which states that the number of "bugs (faults)" of a software product increases as the square of the code size. Security vulnerabilities are approximately linear in the number of program bugs even though other flaws cause vulnerabilities [CS 551, 2001]	$\text{Vulnerabilities} = \sqrt{\text{Lines of Code (LOC)}}$ <ul style="list-style-type: none"> LOC includes non-commented and commented lines of code
M.72	Standard Stability Measure	A measure of the expected changes to the standard, product or service within the next five years [Newton et al., 1997].	<p><i>High:</i> No changes expected within the next five years.</p> <p><i>Medium:</i> Some changes expected within the next five years.</p> <p><i>Low:</i> Many changes expected within the next five years.</p>
M.73	Survivor Function	The function is a generality of reliability and is the probability that an item is functional at any time t [Leemis, 1995].	$S(t) = P[T \geq t]; \quad t \geq 0$ $S(t) = e^{-(\lambda t)^\kappa}; \quad t \geq 0$ <ul style="list-style-type: none"> Utilizing the Weibull Distribution. λ is the positive scale parameter. κ is the positive shape parameter.
M.74	System Design Adequacy (Effectiveness)	The capability of a system to perform satisfactory with in its specified operational environment [Habayeb, 1987]. The quantification of a system's design limitations, physical failures, and availability during operations. It is represented as a probability and is a function of readiness, reliability and design adequacy (performance) [Habayeb, 1987].	<p>System Design Adequacy = $(P_{da})(P_r)(P_{sr})$; where</p> <ul style="list-style-type: none"> The events may not be mutually exclusive and may or may not be statistically independent. P_{da} is system design adequacy, which is 1-P (System Design Limitation). P_r is reliability given system readiness (P_{sr}). P_r is based on operating within a specified period of time. P_{sr} is based on operating time, down time, free time, and availability.

M.75	System Flexibility (Diversity)	<p>The ability to expand, improve and adapt to an environment or circumstance. The operation of the system is performed in different ways in the hope that the same fault is not present in different implementations or the same vulnerability does not cascade throughout the system.</p>	<p><i>High:</i> The users can easily and readily adapt or reconfigure the components of the system to meet current threats or failures through at least two means: software, mechanical or electrical. The organization controls the flexibility of the system.</p> <p><i>Medium:</i> The users can adapt or reconfigure the components of the system to meet current threats or failures through only one mean: software, mechanical or electrical. The organization may control the flexibility of the system but vendor interaction may be required.</p> <p><i>Low:</i> The users cannot adapt or reconfigure the components of the system to meet current threats or failures. The organization has no control over the flexibility of the system and requires vendor interaction.</p>
M.76	System Integrity Levels	<p>Classifications of the ability of a system to detect faults in its own operation and inform a human operator or possibly take the necessary steps to correct the faults [Storey, 1996]. The highest functional requirement is class-1 and the lowest is class-5. These classes are modeled after the integrity levels for computer systems in German nuclear power plants.</p>	<p><i>Level 1:</i> Systems that release automatic actions for protection of human life and environment (i.e., data, components, interconnected systems). The ability to self-check and self-heal the entire system.</p> <p><i>Level 2:</i> Systems that protect only critical components and functions of the system and its environment. Possesses limited self-check and self-heal capabilities.</p> <p><i>Level 3:</i> Systems that protect only critical components or functions of the system and its environment. Possesses either a self-check or self-heal capability.</p> <p><i>Level 4:</i> Human operators monitor the integrity of the system by the use of alarms, screens and queries.</p> <p><i>Level 5:</i> Systems for simple requirements, which do not inform human operators or take appropriate actions after a fault is noted.</p>

M.77	System Maturity Level	The categorical measure depicting whether the system is fully developed.	<p><i>High:</i> Component or system is newly developed; many upgrades or fixes expected; not fully certified, tested, verified or validated by an independent organization. Probability of failures, faults and vulnerabilities is not probable.</p> <p><i>Medium:</i> Component or system is newly developed; many upgrades or fixes expected; not fully certified, tested, verified or validated by an independent organization. Probability of failures, faults and vulnerabilities is unlikely.</p> <p><i>Low:</i> Component or system is newly developed; many upgrades or fixes expected; not fully certified, tested, verified or validated by an independent organization. Probability of failures, faults and vulnerabilities is extremely likely.</p>
M.78	System Non-Repudiation	Non-repudiation is defined as the ability of the recipient of the transaction to prove to a third party that the sender sent a piece of information. In this context, system non-repudiation is the ability of a system to verify the origin of a transaction (piece of information or process) and that that the receiving system received the same transaction [AMS, 2001].	<p><i>High:</i> The user or system can prove that the sender transmitted the transaction and that the recipient received the same transaction. Both individuals can audit the transaction.</p> <p><i>Medium:</i> The user or system can prove that the sender transmitted the transaction or that the recipient received the same transaction. One individual can audit the transaction.</p> <p><i>Low:</i> The user or system cannot prove that the sender transmitted the transaction and that the recipient received the same transaction. Neither individual can audit the transaction.</p>
M.79	System Spoilage	Cost to fix post-release defects divided by the total project cost [Fenton, 1996].	$\frac{\text{Cost to fix "post - release" defects}}{\text{Total System Cost}} * 100$

M.80	System Value	This metric is based on Metcalfe's Law [CS 551, 2001], which states that the value of a network is the square of the number of users.	$\text{System Value} = \sqrt{\text{Number of Users}}$
M.81	Test Cost Factor	System or product testing is a very important consideration in assessing the success of a system, and is essential in minimizing the cost associated with testing. The test cost factor (TCF) [Storey, 1996] is a useful metric in measuring test expenditures.	$TCF = \frac{\text{Test Expenditure}}{\text{Test Expenditure} + \text{Design Expenditure}}$
M.82	Time to Assess Lost or Damaged Information	The time needed to calculate the quantity and worth of information lost or damaged directly after a failure or attack.	$\text{Time to Assess} = \text{Time } (T_f) - \text{Time } (T_0)$; where <ul style="list-style-type: none"> • T_f is the final time when all calculations to establish worth are completed. • T_0 is the initial time of reconfiguration.
M.83	Time to Withstand a Continuous Attack	The amount of time a system can resist the harmful effects of an attack or failure by using security measures, redundancy, reconfiguration measures, or detection mechanisms.	$\text{Time (Withstanding)} = \text{Time } (T_f) - \text{Time } (T_0)$; where <ul style="list-style-type: none"> • T_f is initial time when the effects on the system cause failure, loss of functionality or inoperability. • T_0 is the initial time of detected failures or attacks.
M.84	Unreliability	The probability that a component has not survived a specified time interval [Johnson, 1989]. Unreliability and reliability sum to 1.	$Q(t) = \frac{N_f(t)}{N} = \frac{N_f(t)}{N_0(t) + N_f(t)} = 1 - R(t);$ where <ul style="list-style-type: none"> • $N_f(t)$ is the number of components that failed at time t. • $N_0(t)$ is the number of components that are operational at time t. • N is the total number of components. • $R(t)$ is the reliability of the system.

M.85	Usability	Is the extent to which the product is convenient and practical to use [Fenton, 1996]. The metric is related to the notion of system user-friendliness and is predominately used in the context of software but has application in hardware and policy functions.	Usability = Probability (The user of a system does not experience a problem (e.g., failure, user interface fault) during a given interval of time under set conditions.
M.86	User-lost-erlangs (ULE) [Snow, 2000]	ULE is a logarithmic measure (e.g., Richter scale) of system survivability [Snow, 2000].	$ULE = \log_{10}(MD)$; where <ul style="list-style-type: none"> M is the magnitude of an outage (number of customers affected) and D is the duration of the outage (days).
M.87	Verification/Validation	Verification is the process of determining whether the output of a lifecycle phase fulfils the requirement specified by the previous phase. Validation is the process of confirming a system specification is appropriate and is consistent with the user requirements [Storey, 1996]. The metric uses the evaluation assurance levels (EAL) [Rycombe, 2001] from the common criteria levels to categorize the verification and validation of products.	<ul style="list-style-type: none"> EAL0: Product or System Failure. EAL1: Functionally tested. EAL2: Structurally tested. EAL3: Methodically tested and checked. EAL4: Methodically designed, tested, and reviewed. EAL5: Semi-formally designed and tested. EAL6: Semi-formally verified design and tested. EAL7: Formally verified design and tested.

Table 36: Information Assurance Metrics

Appendix D: IA Metric Characteristics

Table 37 has five columns to the right of the IA metric depicting the characteristics of the metric itself. The following abbreviations are used within Table 37: Lines of Code (LOC), Minute (Min), Second (Sec), and Return on Investment (ROI).

- Column-three: Represents a subjective assessment between the objective and a metric and the representation is flexible to meet the needs of an organization.
- Column-four: Measurement type is depicted as either fundamental or derived.
- Column-five: Measurement category is depicted as quantitative (QN), qualitative (QL) or temporal (TP).
- Column-six: Metric scale is depicted as nominal (N), interval (I), ordinal (O) or ratio (R) scales.
- Column-seven: Metric units correspond to building blocks of each IA metric (e.g., inches for length, bits per second for data rate).

#	IA Metric	Objective Association	Measurement Type	Metric Category	Metric Scale	Metric Units
M.1	Algorithmic Efficiency	Maintainability	Fundamental	QN	N	None
M.2	Bit Error Rate	Information Loss	Derived	QN	N	Bits/second
M.3	Buffering Factor	Security	Fundamental	QN	N	Component
M.4	Complexity	Redundancy	Fundamental	QN	N	None
M.5	Complexity (Halstead)	Reliability	Fundamental	QN	N	None
M.6	Complexity, Software (McCabe)	Reliability	Fundamental	QN	N	None
M.7	Complexity, Structure (McCabe)	Reliability	Fundamental	QN	N	Paths
M.8	Confidentiality Levels	Integrity	Fundamental	QN	N	Levels
M.9	Coupling Interaction Index	Extreme Events	Fundamental	QL	O	None
M.10	Cryptographic Work Factor (Number)	Security	Fundamental	QN	N	Keys
M.11	Cryptographic Work Factor (Time)	Security	Fundamental	TP	I	Years
M.12	Data Immunity	Integrity	Derived	QN	I	None
M.13	Data Transfer/Access Rate	Operability	Derived	QN	N	Bits/second
M.14	Defect Density Measure	Reliability	Derived	QL	R	Defects/LOC
M.15	Defect Density per Line of Code	Reliability	Fundamental	QL	R	Defects/LOC
M.16	Detectability	Survivability	Derived	QN	I	None
M.17	Duration of Effects	Surety	Derived	TP	I	Sec or Min
M.18	Effort	Cost	Fundamental	QN	N	Person*Months
M.19	Expected Effect on Adversary's Decisionmaking Abilities	Uncertainty	Derived	QL	O	None
M.20	Expected Value of Risk	Risk	Derived	QN	I	None
M.21	Failure Rate	Operability	Derived	QN	N	Failures
M.22	Fault Location Coverage	Survivability	Derived	QN	I	None
M.23	Frequency of Failure	Survivability	Derived	QN	N	Failures/Time
M.24	Hamming Distance	Information Loss	Derived	QN	N	Bits
M.25	Hardness	Survivability	Fundamental	QL	O	None
M.26	Hazard Function	Survivability	Derived	QN	I	None
M.27	Hurdle Rate	ROI	Fundamental	TP	I	(Year) ⁻¹
M.28	IA Personnel Trained	Situational Awareness	Fundamental	QN	N	People
M.29	Incident Occurrence	Surety	Derived	QN	N	Incident/time
M.30	Incident Recovery Time	Availability	Derived	TP	I	Sec or Min
M.31	Incident Response Time	Survivability	Derived	TP	I	Sec or Min
M.32	Information Corruption Rate	Integrity	Derived	QN	N	Bits/second

#	IA Metric	Objective Association	Measurement Type	Metric Category	Metric Scale	Metric Units
M.33	Information Entropy	Information Loss Uncertainty	Derived	TP	N	Time
M.34	Information Timeliness	Surety	Derived	TP	I	Sec or Min
M.35	Information Value	Cost	Derived	QN	N	Dollars
M.36	Information Value Levels	Cost	Derived	QL	O	None
M.37	Lifecycle Costs	Cost	Fundamental	QN	N	Dollars
M.38	Likelihood of Gaining Access to System	Security	Fundamental	QN	I	None
M.39	Lost Information Percentage	Information Loss	Derived	QL	R	None
M.40	Manpower Utilization Rate	Cost	Fundamental	QN	N	People
M.41	Mean Effort to Reach Target	Survivability	Fundamental	TP	I	Days
M.42	Mean Time Between Failures	Reliability	Fundamental	TP	I	Sec or Min
M.43	Mean Time to Failures	Reliability	Fundamental	TP	I	Sec or Min
M.44	Mean Time to Human Error	Reliability	Derived	TP	I	Sec or Min
M.45	Mean Time to Repair	Maintainability	Fundamental	TP	I	Sec or Min
M.46	Mission Time	Reliability	Derived	TP	I	Sec or Min
M.47	Natural Disaster Detection Likelihood	Survivability	Fundamental	QN	I	None
M.48	Number of Access Points per System (Permeability)	Security	Fundamental	QN	N	Access Points
M.49	Number of Dissimilar Operating Systems	Redundancy	Fundamental	QN	N	Operating Systems
M.50	Number of Documented Risks	Risk	Fundamental	QN	N	Risks
M.51	Number of Eradicated Viruses	Operability	Derived	QN	N	Viruses
M.52	Number of Parallel Security Mechanisms	Security	Fundamental	QN	N	Parallel Mechanisms
M.53	Number of Serial Security Mechanisms	Security	Fundamental	QN	N	Serial Mechanisms
M.54	Outage-Index Metric	Surety	Derived	QN	I	None
M.55	Performability	Surety	Derived	QN	I	None
M.56	Personnel Turnover Rate	Cost	Derived	QN	I	Percent
M.57	Predicted Number of Faults	Reliability	Fundamental	QN	N	Faults
M.58	Potential Effect (Type I Error)	Uncertainty	Derived	QN	I	None
M.59	Potential Effect (Type II Error)	Uncertainty	Derived	QN	I	None
M.60	Processing Time for Reconfiguration	Operability	Derived	TP	I	Minutes
M.61	Processing Time for System Update	Operability	Fundamental	TP	I	Seconds
M.62	Recovery Operational Percentage (24-hours)	Expected Damage	Derived	QN	R	None
M.63	Redundancy Ratio	Redundancy	Fundamental	QN	R	None
M.64	Repair Rate Function	Maintainability	Fundamental	QN	N	Systems/time

#	IA Metric	Objective Association	Measurement Type	Metric Category	Metric Scale	Metric Units
M.65	Resource Availability	Availability	Derived	QN	R	Percent
M.66	Risk Leverage	Extreme Events	Fundamental	QN	R	None
M.67	Risk Severity Classification	Risk	Fundamental	QL	O	None
M.68	Social Cost	Cost	Derived	QN	N	Dollars
M.69	Software Capability Maturity Model	Surety	Fundamental	QL	O	None
M.70	Software Function and Feature Points	Availability	Fundamental	QN	I	Function Points
M.71	Software Vulnerabilities	Operability	Fundamental	QN	N	Vulnerabilities
M.72	Standard Stability Measure	Cost	Fundamental	QL	O	None
M.73	Survivor Function	Reliability	Derived	QN	I	None
M.74	System Design Adequacy	Surety	Derived	QN	I	None
M.75	System Flexibility	Redundancy	Fundamental	QL	O	None
M.76	System Integrity Levels	Integrity	Fundamental	QL	O	None
M.77	System Maturity Level	Reliability	Fundamental	QL	O	None
M.78	System Non-Repudiation	Integrity	Fundamental	QL	O	None
M.79	System Spoilage	Cost	Fundamental	QL	R	Percent
M.80	System Value	Expected Damage	Fundamental	QN	N	Users
M.81	Test Cost Factor	Cost	Fundamental	QL	R	Dollars
M.82	Time to Assess Lost or Damaged Information	Cost	Derived	TP	I	Minutes
M.83	Time to Withstand a Continuous Attack	Survivability	Derived	TP	I	Minutes
M.84	Unreliability	Reliability	Derived	QN	I	None
M.85	Usability	Operability	Derived	QN	I	None
M.86	User-lost-erlangs	Survivability	Derived	QN	I	User*Days
M.87	Verification/Validation	Surety	Fundamental	QL	O	None

Table 37: Information Assurance Metric Characteristics

References

- "Command, Control, Communications, and Computers, Intelligence, Survivability and Reconnaissance (C4ISR)." Online. Internet. February 2000. Available: <http://www.dtic.mil/exercsec/adr97/chap23.html>.
- "Computer Almanac-Numbers about Computers." Online. Internet. May 2000. Available: <http://www.cs.cmu.edu/afs/cs.cmu.edu/user/barn/www/numbers.html>.
- "Crime in Cyberspace, First Draft of International Convention Released for Public Discussion." Online. Internet. August 2000. Available: <http://conventiaons.coe.int/treatv/en/projects/cybercrime.htm>.
- "Executive Order 12958 – Classified National Security Information." Online. Internet. August 2000. Available: <http://www.dss.mil/seclib/eo12958.htm>.
- "Hacking Threat to GCC." Online. Internet. January 2001. Available: <http://www.interactive-tech.com/hack.html>.
- "How to Eliminate the Ten Most Critical Internet Security Threats." Online. Internet. May 2000. Available: <http://www.sans.org/topten.htm>.
- "Information Assurance Description." Online. Internet. September 2000. Available: <http://portal.deskbook.osd.mil/irp/38.htm>.
- "Intelligence Resource Program." Online. Internet. May 2000. Available: <http://www.fas.org/irp/wwwinfo.html>.
- "Metrics Methodology Write-up." IASET Workshop. July 14, 1999. Online. Internet. December 2000. Available: <http://www.iaset.org/program.htm>.
- "Organization – Land Information Warfare Activity – INSCOM." Online. Internet. May 2000. Available: <http://www.fas.org/irp/agency/inscom/liwa/org.htm>.
- "Strategies: Firewalls and Security." Online. Internet. August 2000. Available: <http://www.school.com/on-line/in101s-4-3.htm>.
- "The History of Computer Crimes to Date – 2000." Online. Internet. May 2000. Available: <http://www.making-a-difference.org/computer-crime-chronicles.htm>.
- "The National Infrastructure Protection Center Information System Advisory 00-044." Online. Internet. May 2000. Available: <http://www.nipc.gov/advis00-044.htm>.
- "Threat Assessment." Information Warfare, Defense. Online. Internet. February 2000. Available: <http://cryptome.org/iwd-a.htm>.
- "Workplace Practices and Organizational Performance: No Easy Fixes." Online. Internet. August 2000. Available: <http://www.hrdc-drhc.gc.ca/arb/publications/bulletin/vol3n2/v3n2c7e.shtml>.

- Abrams, Marshall D. "NIMS Information Security Threat Methodology." MITRE Technical Report.
- Adams, Charlotte. "New Service Gauges for Virus Risk." Federal Computer Week 26 April 1999. Online. Internet. May 2000. Available: <http://208.20.97.5/ref/hottopics/security/background/few-virus-4-26-99.html>.
- Air Power Studies Centre. APSC Paper Number 47: Military Information Operations in a Conventional Warfare Environment. Commonwealth of Australia 1995. Online. Internet. March 2000. Available: <http://www.defense.gov.au/apsc/publish/paper47.htm>.
- Alberts, David S., John J. Garstka, and Frederick P. Stein. Network Centric Warfare. C4ISR Cooperative Research Program (CCRP). 1942.
- AMS Center for Advanced Technologies. "Sixty Security Building Block...Non-repudiation." Online. Internet. February 2001. Available: <http://www.amsinc.com/Amscat/Security%20Story/SecurityBldgBlock6.htm>.
- Anderson, Robert H. "Research and Development Initiatives Focused on Preventing, Detecting,, and Responding to Insider Misuse of Critical Defense Information System." Santa Monica, California. RAND Corporation, 1999.
- Anonymous. Maximum Security. 2nd ed. Sams Publishing. 1998.
- Ashkenas, Ron, Dave Ulrich, Todd Jick, and Steve Kerr. The Boundaryless Organization. Jossey-Bass Inc., San Francisco, California, 1995.
- Associated Press. "Credit Card Machines Paralyzed by Y2K." Online. Internet. January 2001. Available: <http://www.usatoday.com/life/cyber/tech/review/crg754.htm>.
- Bennett, Bob, Senator. Hearing: Y2K Response, Recovery and Cyber-Reconstitution: Understanding the Role of the Information Coordination Center. 29 July 1999. Online. Internet. May 2000. Available: <http://www.senate.gov/~y2k/hearings/990729/st990729bennett.htm>.
- Berard, Edward, V. "Metrics for Object-oriented Software Engineering." Online. Internet. January 2001. Available: <http://www.toa.com/pub/moose.htm>.
- Burton, Katharine J. Captain, USN. "Defense-wide Information Assurance Program (DIAP)." DoD DIAP Briefing, 1999.
- Campbell, William H. Lieutenant General, USA. Director for Command, Control, Communications, and Computers (DISC4). Hearing on Information Superiority and Information Assurance. Online. Internet. May 2000. Available: <http://www.house.gov/hasc/testomony/106thcongress/00-03-08campbell.htm>.
- Carnegie Mellon, Software Engineering Institute. Detecting Signs of Intrusion. Security Improvement Module (CMU/SEI-SIM-001). August 1997.

- Carnegie Mellon, Software Engineering Institute. Simplex in a Hostile Communications Environment: The Coordinated Prototype. Technical Report (CMU/SEI-99-TR-016). August 1999.
- CERT Coordination Center. The Information Assurance Research Institute: IA Science & Engineering for the 21st Century. 1999. Draft. Software Engineering Institute. Online. Internet. March 2000. Available: <http://www.cert.org>.
- Chankong, Vira, and Yacov Y. Haimes. Multiobjective Decision Making, Theory and Methodology. North Holland, New York, 1983.
- Christensen, John. "Bracing for guerrilla warfare in cyberspace." CNN Interactive, April 6, 1999. Online. Internet. June 2000. Available: <http://cnn.com/TECH/specials/hackers/cyberterror>.
- Clark, Drew. "Pentagon hit by Major Cyber Attacks." National Journals: Technology Daily. Online. Internet. May 2000. Available: <http://www.govexec.com/dailyfed/0399/030899b3.htm>.
- Clark, Richard D. "Implementation of PDD 63 through Project Matrix." Critical Infrastructure Assurance Office. Online. Internet. September 2000. Available: http://www.ciao.gov/Matrix/RC_Memo.htm.
- Collins, James C. and Jerry I. Porras. Built to Last. HarperCollins Publishers, Inc., New York, 1997.
- Computer Emergency Response Team/Coordination Center (CERT/CC) Report, Articles and Presentations. Online. Available. September 2000. <http://www.cert.org/van/reports.html>.
- Computer Science 551, "Security and Privacy on the Internet." Professor David Evans. University of Virginia. September-December 2000. Online. Available. March 2001. <http://www.cert.org/van/reports.html>.
- Computer Science and Telecommunications Board National Research Council. The Digital Dilemma, Intellectual Property in the Information Age. National Academy Press, Washington, D.C, 2000.
- Computer Security Institute (CSI) and Federal Bureau of Investigations (FBI), 1999 Survey US Corporations Losing Millions from Security Breaches.
- Computer Security Institute (CSI) and Federal Bureau of Investigations (FBI), Issues and Trends: 2000, CSI/FBI Computer Crime and Security Survey (22 Mar 2000). Online. Internet. May 2000. Available: http://www.gocsi.com/prelea_000321.htm.
- Craft, Rickard L. and Gregory D. Wyss. Sandia National Laboratories. "Toward a Science-Based Approach to Information Assurance." Online. Internet. September 2000. Available: <http://www.sandia.org>.

- Cramer, Myron L. Dr. "Measuring the Value of Information." Presented at InfoWAR Conference, 1997. Online. Internet. December 2000. Available: <http://iw.windermeregroup.com/Papers/infoval.html>.
- Curtis, Bill, William E. Hefley, and Sally Miller. "Overview of the People Capability Maturity Model." CMU/SEI-95-MM-01. September 1995.
- Cyber Conference. "Carnegie Mellon University Center Cyber Summit." July 24-25 2000. Pittsburgh, PA.
- Deane, Joel. "VicodinES Manifesto: 'Infect the world'." ZDNet News, April 1, 1999. Online. Internet. June 2000. Available: <http://www.zdnet.com/adnn/stories/news/0,4586,2235046,00.html>.
- Defense Science Board. Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D). November 1996. Online. Internet. March 2000. Available: <http://www.aci.net/kalliste/iwdmain.htm>.
- Deswarte, Yves. "Contribution of Quantitative Security Evaluation of Intrusion Detection." Online. Internet. December 2000. Available: http://www.zurich.ibm.com/pub/Other/RAID/Prog_RAID98/Full_Papers/deswarte_slides.html/index.htm.
- Dhillon, B. S. Design Reliability: Fundamentals and Applications. CRC Press LLC. Boca Raton, Florida, 1999.
- DiCenso, David J. Major USAF Retired. "IW Cyberlaw." Online. Internet. May 2000. Available: <http://www.airpower.makwell.af.mil/airchronicles/apj/apj99/sum99/discenso.html>.
- Dombroski, Matthew. "A Risk-based Decision Support Methodology for Operations Other Than War (OOTW)." University of Virginia. April 2001.
- Donahue, William J., Lieutenant General. "Information Assurance in the New Millennium." Online. Internet. May 2000. Available: <http://public.afca.scott.af.mil/public/00jan/jan01.html>.
- Douglas, Mary. Social Research Perspectives. Russell Sage Foundation. 1985.
- EDS. "EDS Total Information Assurance Life Cycle Support." Online. Internet. August 2000. Available: <http://www.eds-gov.com/Solutions/ia/lifecycle.asp>.
- Ellis, Susan. "Cyberthreat: Protecting US Information Networks (Interview with Dr. Jeffrey Hunker, Director of CIAO)." Online. Internet. June 2000. Available: <http://www.ncs/telcomnews/98-3/article2.html>.
- Engst, Adam, C. Internet Starter Kit, Macmillan Computer Publishing, Indianapolis, IN, 1996.

- Erkomaa, Liisa. "Secure Socket Layer and Transport Layer Security." Online. Internet. February 2001. Available: <http://www.tml.hut.fi/Studies/Tik-110.350/1998/Essays/ssl.html>.
- Ezell, Barry C., Captain. "Risks of Cyber Attack to Supervisory Control and Data Acquisition for Water Supply." University of Virginia. May 1998.
- FAS Project. "White Paper on Information Infrastructure Assurance." Online. Internet. May 2000. Available: <http://china.si.umich.edu/spp/courses/744/misc.hyper/0209.html>.
- Federal Security. "Federal IT Security—The New Day Dawns." Online. Internet. June 2000. Available: http://www.gcn.com/research_results/12_8teg.html.
- Federation of American Scientists (FAS). "Framework for Estimating Security Costs." Online. Internet. June 2000. Available: <http://www.fas.org/sgp/spb/framework.html>.
- Fenton, Norman E. and Shari L. Pfleeger. Software Metrics: A Rigorous & Practical Approach, 2nd Edition. PWS Publishing Company, Boston, MA, 1997.
- Fenton, Norman. "Software Metrics for Control and Quality Assurance Course Overview." January 10 2000. Online. Internet. February 2001. Available: http://www.dcs.qmw.ac.uk/~norman/Courses/mod_903/slides/slides_2000/all_slides_2000_blue.
- Fisher, W. R., M. F. Doherty, and J. M. Douglas (1988). The interface between design and control 2: Process operability. *Industrial and Engineering Chemistry Research*.
- Fleming, Mike. "Information Assurance, Protecting and Defending Against Cyber-Attack." DARPA Briefing. 9 March 2000.
- Field Manual, FM 22-100 (Leadership). Preliminary Draft 2000. Online. Internet. February 2001. Available: <http://www.fm22-100.army.mil/>.
- Field Manual, FM 100-5 (Army Operations). Preliminary Draft 2000. Online. Internet. February 2001. Available: <http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/100-5/100-5toc.htm>.
- George Smith. An Electronic Pearl Harbor? Not Likely. *Issues in Science and Technology*, Fall 1998. 68-73.
- Global Technology Research. Intelligence-Based Threat Assessment Information Networks and Infrastructure. Online. Internet. March 2000. Available: http://www.aracnet.com/~kea/Papers/theat_whtie_paper.shtml.
- Grabowski, Martha and Karlene H. Roberts. "Risk Mitigation in Virtual Organizations." 4 June 1998. Online. Internet. August 2000. Available: <http://www.ascusc.org/jcmc/vol3/issue4/grabowski.html>.

- Habayeb, A. R. Systems Effectiveness. Pergamon Books Ltd, 1987.
- Haimes, Yacov Y. "Hierarchical Holographic Modeling." IEEE Transactions on Systems, Man, and Cybernetics. Volume 11, Issue 9, 1981.
- Haimes, Yacov Y. "Total Risk Management. Risk Analysis. Volume 11, Issue 2, 1991.
- Haimes, Yacov Y. Risk Modeling, Assessment and Management. John Wiley and Sons, Inc., New York, 1998.
- Haimes, Yacov Y. "Organizational Program within the Information Assurance Institute." 4 April 2000a.
- Haimes, Yacov Y. Leontief-Based Model of Risk in Complex Interconnected Infrastructures, January 6, 2000b. ASCE Journal of Infrastructure Systems.
- Haimes, Yacov. Y. "Institute for Integrated Information Assurance (IIIA)." Draft. April 11, 2000c.
- Haimes, Yacov Y., Stan Kaplan, and Paul Slovic. Quantitative Risk Analysis and the Affect Heuristic. January 10, 2001a, Draft Six.
- Haimes, Yacov Y., Thomas A. Longstaff, and Gregory A. Lamm "Balancing Promise and Risk to Information Assurance in Joint Vision 2020." Technical Report, Center for Risk Management, University of Virginia, 18 February 2001b.
- Haimes, Yacov Y., James H. Lambert, and Stan Kaplan. Risk Filtering and Ranking Method and Hierarchical Holographic Modeling. Center for Risk Management of Engineering Systems, University of Virginia. March 8, 2001c.
- Hamre, John J. Deputy Secretary of Defense. Statement to Congress on Information Assurance. Online. Internet. May 2000. Available: http://www.fas.org/irp/congress/1998_hr/98-06-11hamre.htm.
- Harris Corporation. "What is Information Assurance?" Online. Internet. September 2000. Available: <http://www.govcomm.harris.com/inforassurance/whatis.htm>.
- Henley, Ernest J. and Hiromitsu Kumamoto. Probabilistic Risk Assessment. The Institute of Electrical and Electronics Engineers, Inc., New York, 1992.
- Hissam, Scott and Daniel Plakosh. "COTS in the Real World: A Case Study in Risk Discovery and Repair." Carnegie Mellon Software Engineering Institute, Pittsburgh, PA, 1999.
- Humphrey, Watts S. Managing the Software Process. Addison-Wesley Publishing Company Inc., 1989.
- Icove, David, Karl Seger, and William Vonstorch. Computer Crime: A Crimefighter's Handbook. O'Reilly and Associates, Inc., 1995.

- Information Warfare Research Center (IWRCC). "Information Assurance Related Missions and Functions." Online. Internet. March 2000. Available: <http://www.terrorism.com/infowar/j6kdefense.html>.
- Jacquet, Jean-Phillippe and Alain Abran. "From Software Metrics to Software Measurement Methods: A Process Model." Proceedings of the 3^d International Software Engineering Standards Symposium (ISESS, 1997).
- John E. Gibson. How To Do A Systems Analysis and Systems Analyst Decalog. 1991.
- Johnson, Barry W. Design and Analysis of Fault Tolerant Digital Systems Addison-Wesley Publishing Company Inc., 1989.
- Johnson, Chris. "Visualizing the Relationship between Human Error and Organizational Failure." Department of Computing, University of Glasgow, Glasgow. Online. Internet. August 2000. Available: <http://www.dsc.gla.ac.uk/~johnson>.
- Johnson, Michael, Major, US Army, Land Information Warfare Activity (LIWA) Operations Officer. Personal Interview. 15 May 2000.
- Joint Military Intelligence College Foundation. "Knowledge Management." Defense Intelligence Journal. Volume 9, Number 1, Winter 2000.
- Jones, Byran. "Software Quality Assurance." October 11 1998. Online. Internet. February 2001. Available: http://www.comp.glam.ac.uk/pages/staff/bfjones/sqa/structural_testing/.
- Kaplan, S. and B. J. Garrick (1981). "On the Quantitative Definition of Risk," Risk Analysis Vol. 1, No. 1, pp. 11- 27.
- Kasabov, Nik. "Uncertainty in Data and Information." January 08 2000. Online. Internet. February 2001. Available: <http://divcom.otago.ac.nz/infosci/courses/INFO223/Lectures/7/sld007.htm>.
- Koller, Glenn R. Risk Modeling for Determining Value and Decision Making. CRC Press LCC. Boca Raton, Florida, 2000.
- Kontio, Jyrki. "The Riskit Method for Software Risk Management, version 1.00." Institute for Advanced Computer Studies and Department of Computer Science University of Maryland, 2000.
- Koob, Gary Dr. "Challenge: Assurance Metrics." DARPA/ITO. Online. Internet. December 2000. Available: <http://www.cs.utah.edu/~sjt/jto/metrics.html>.
- Kuhn, Richard D. "Sources of Failure in the Public Switched Telephone Network." National Institute of Standards and Technology, 1997.
- Lamm, Linda, M. J. "Develop Measures of Effectiveness and Deployment Optimization Rules for Networked Ground Sensors." University of Virginia. May 2001.

- Leemis, Lawrence M. Reliability. Prentice-Hall, Inc., 1995.
- Leveson, Nancy G. Safeware, System, Safety and Computers. Addison-Wesley Publishing Company, Inc., 1995.
- Lewis, Brian. "Information Warfare." Online. Internet. March 2000. Available: <http://www.fas.org/irp/eprint/snyder/infowarfare.htm>.
- Libicki, Martin. "Defending Cyberspace and Other Metaphors." Institute for National Strategic Studies. Online. Internet. June 2000. Available: http://www.infowar.com/MIL_C4I/Libicki/dcomcch00.html.
- London Press. "Cyber Attacks on Increase." Online. Internet. May 2000. Available: <http://www.mi2g.com>.
- Longstaff, Thomas and Yacov Y. Haimes. "A Holistic Roadmap for Carnegie Mellon Institute for Survivable Systems (CMISS)." August 10, 2000.
- Longstaff, Thomas, A., Carol A. Sledge, and Yacov Y. Haimes. COTS-Based Systems and the Risk to Information Assurance. Forth Draft. February 6, 2001.
- Lonstaff, Thomas A., Clyde Chittister, Rich Pethia, and Yacov Y. Haimes. "Are We Forgetting the Risks of Information Technology?" Computer. IEEE Computer Society. December 2000.
- Lowrance, W. W. Of Acceptable Risk, William Kaufmann, Lost Altos, CA. 1976.
- Management Analytics. "Is Information Assurance an Unsolvable Problem?" Online. Internet. June 2000. Available: <http://www.all.net/books/iwar/unsolvable.html>.
- McCormick, Norman J. Reliability and Risk Analysis. Academic Press, Inc., 1981.
- McCullagh, Declan. "Cyber Crime has Bugs." Online. Internet. August 2000. Available: <http://www.wired.com/news/print/0,1294,36047,00.html>.
- Military Critical Technologies (MCT). "Part III: Developing Critical Technologies." October 2000. Online. Internet. February 2001. Available: <http://www.dtic.mil/mctl/>.
- Miller, William D. "Systems Engineering Metrics." System Engineering: A Competitive Edge in the Changing World. Proceedings of the 4th Annual International Symposium of the National Council on Systems Engineering, Volume I. August 10-12, 1994. San Jose, CA: 787-789.
- Minihan, Kenneth A. Lieutenant General, USA. Director, National Security Agency (NSA). Defending the National Against Cyber Attack: Information Assurance in the Global Environment. Online. Internet. May 2000. Available: <http://www.usinfo.state.gov/journals/itps/1198/ijpe/pj48min.htm>.
- MITRE Corporation. "The Threat to America's Critical Infrastructures." Online. Internet. May 2000. Available: <http://www.mitre.org/support/papers/>.

- Morgan, M. Granger, Florig, H. Keith, Michael L. DeKay, and Paul Fischbeck. Categorizing Risks for Risk Ranking. Risk Analysis, Volume 20, No. 1, 2000. 49-57.
- National Academy Press. "The Digital Dilemma, Intellectual Property in the Information Age." National Academy Press, Washington, D.C. 2000.
- National Cooperative Education Statistics System. "Safeguarding your Technology." Online. Internet. March 2000. Available: <http://nces.ed.gov/pubs98/safetech/>.
- National Research Council (US). Committee on Information Systems. Trust in Cyberspace. National Academy Press, 1999.
- National Security Agency (NSA). Information Assurance Technical Framework. Computer File at National Defense University Library, Fort McNair, Virginia. 1999.
- National Security Telecommunications Advisory Committee, Information Assurance Task Force. Electric Power Risk Assessment. Nov 1997.
- Newton, Judith, Elizabeth Fong, and Tom Rhodes. "A Taxonomy for Retrieval of Standards Information on the World Wide Web." Online. Internet. February 2001. Available: <http://www.computer.org/proceedings/meta97/papers/jnewton/jnewton.htm>.
- Nichols, Randall K., Raniel J. Ryan, Julie J. Ryan, William E. Baugh. Defending your Digital Assets. McGraw-Hill Companies, 2000.
- Nitzbers, Sam. "The Cyber Battlefield-Is this the Setting for the Ultimate World War?" IEEE International Symposium on Technology and Society 1997.
- Noach, David. "Computer Viruses Cost \$12 Billion in 1999." Online. Internet. May 2000. Available: <http://public.afca.scott.af.mil/public/00jan/jan01.html>.
- Norton, Darcy R. and Anne Marie Willhite. "Establish a Baseline Assessment to Manage Risks Using Risk Matrix. MITRE Corporation.
- Nuclear Regulatory Commission (NRC). "Fault-tree Handbook." Prepared by Vesely, W. E., F. F. Goldberg, N. H. Roberts, and D. F. Haasl. NRC Report Number NUREG-0492. January 1981.
- OSCAM Approach to O and S Cost. Online. Internet. February 2001. Available: <http://www.oscamtools.com/Modleing%Approach.htm>.
- Parker, Donn B. Fighting Computer Crime. John Wiley and Sons, Inc., 1998.
- Payne, Shirley C, University of Virginia, Director for Security Coordination and External Relations. Personal Interview. 15 April 2001.
- Perrow, Charles. Normal Accidents. Princeton University Press. 1999.

- Pfleeger, Shari L. "Risky Business: What we have yet to Learn about Software Risk Management." Systems/Software, Inc., Washington, D.C. Online. Internet. February 2001. Available: <http://ftp.cs.umd.edu/users/sharip/mswe607/risks.htm>.
- Poller, Alan. "Cyber Crime Comes to Washington." Information Systems Security Guide September 1998. Online. Internet. May 2000. <http://www.gov.exec.com/features/0998/0998sup1.htm>.
- Power, Richard. Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace. Que Corporation, 2000.
- President's Commission on Critical Infrastructure Protection. PCCIP Summary Report (October 23, 1997). Online. Internet. May 2000. Available: <http://www.pccip.gov/summary.html>.
- President's Commission on Critical Infrastructure Protection. Report Summary, 1999. Online. Internet. May 2000. Available: <http://www.pccip.ncr.gov/summary.html>.
- Preuber, Heike. "Shannon's Entropy." Online. Internet. June 2000. Available: <http://sellensr.me.queensu.ca/preusser/diplomar/node10.html>.
- Putnam, Lawrence H. and Ware Myers. Measures for Excellence. PTR Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1992.
- Rai, Gulshan, Dr., Dr. R. K. Dubash, and Dr. A. K. Chakravarti. "Computer Related Crimes." Online. Internet. May 2000. Available: <http://www.mit.gov.in/crime.htm>.
- Randell, Brian, Laprie, Jean-Claude, and Algirdas Azizienis. "Fundamental Concepts of Dependability." 1992.
- Richard Pethia, Manager, Trustworthy Systems Program and CERT Coordination Center Software Engineering Institute Carnegie Mellon University. Statement to US Senate on Governmental Affairs, June 5, 1996. Online. Internet. May 2000. Available: http://www.cert.org/congressional_testimony_Pethia96.html.
- Roberts, Fred S. Measurement Theory, Encyclopedia of Mathematics and its Applications. Addison-Wesley Publishing Company, Reading, Massachusetts, 1979.
- Robinson, Paul C., Woodard, Joan B., and Samuel G. Varnado. Critical Infrastructure: Interlinked and Vulnerable. Issues in Science and Technology, Fall 1998. 61-67.
- Rycombe Corporation. "Common Criteria." Online. Internet. February 2001. Available: <http://www.rycombe.com/cc.htm>.
- Saydjari, Sami O. "Information Assurance." DARPA Briefing. Online. Internet. May 2000. Available: <http://www.darpa.mil/iso/ia/>.
- Schalestock, Barbara, Deputy LIWA, US Army, Land Information Warfare Activity (LIWA) Operations Officer. Personal Interview. 15 May 2000.

- Schwartau, Winn. "Infrastructure Is Us." Online. Internet. March 2000. Available: <http://www.inforsecuritymag.com/jun99/Infrastruc.htm>.
- Schwartau, Winn. "It's About Time: The Metric for Information Security." (1999) Online. Internet. November 2000. Available: <http://www.shockwavewriters.com/Lectures/WS/themetricfor IS.htm>.
- Schweber, Von E. "The Land of the Lost." PC Week, pg. 102, October 27, 1997.
- Shanahan, Stephen W., Lieutenant Colonel and Lieutenant Colonel Garry J. Beavers. "Information Operations in Bosnia." Online. Internet. May 2000. Available: <http://www-cgsc.army.mil/milrev/english/novdec97/shanahan.htm>.
- Sibley, K. "Data Recovery: How Safe is Your Business." Computing Canada, Volume 23, Number 21. October 1997.
- Skroch, Michael, Program Manager, Information Assurance Science and Engineering Tools (IASSET). "Development of a Science-Based Approach for Information Assurance." Online. Internet. September 2000. Available: <http://www.darpa.mil/iso/iaset/iaset.htm>.
- Snow, A., "A Survivability Metric For Telecommunications: Insights and Shortcomings." 1998 Information Survivability Workshop - ISW'98 IEEE Computer Society, Orlando, FL October 1998 135-138.
- Stallings, William. Cryptography and Network Security, Principles and Practice. Second Edition. Prentice Hall, Upper Saddle River, New Jersey, 1999.
- Stang, David J. Ph. D. "The Computer Virus Problem." Online. Internet. May 2000. Available: <http://www.sevenlocks.com/virushelp/wpoverviewofthevirusproblem.htm>.
- Stephenson, Peter. "Managing Intrusions." Executive White Paper. Netigy Corporation, 1999.
- Stevens, S. S. Mathematics, measurement and psychophysics. In S. S. Stevens (ed.), Handbook of Experimental Psychology. John Wiley & Sons, Inc., New York, 1951.
- Story, Neil. Safety-Critical Computer Systems. Addison Wesley Longman, Inc., New York, 1996.
- Strategic Research Division (SVP Division). A 1992 survey of 450 Fortune 1000 companies. Online. Internet. May 2000. Available: <http://www.lakeviewtech.com/solution/highavailability/hadefined.asp>.
- Strategic, Departmental, and Operational IEW Operations. FM 34-37. Preliminary Draft 2000. Online. Internet. June 2000. Available: <http://www.fas.org/irp/doddir/army/fm34-37/toc.htm>.
- Sullivan, Bob. "Cyberwar: The Threat of Chaos." Online. Internet. May 2000. Available: <http://www.msnbc.com/news/295227.asp?cp1=1>.

- Sunbelt-Software, "Computer Security Facts and Statistics." Online. Internet. May 2000. Available: http://www.sunbelt-software.com/security_and_stat.htm.
- Survivability/Lethality Analysis Directorate. Information Warfare Analysis. Online. Internet. May 2000. Available: http://web.arl.mil/services/infor_analysis.html.
- Tanenbaum, Andrew S. Computer Networks, 3rd Edition. Prentice Hall PTR, New Jersey, 1996.
- Tomlinson, Christine. Reconceptualizing Industrial Human Error. Insight, Vol 3, Issue 1, April 2000. 19-67.
- Tritak, John S. and Michael A. Vatis. Statements to Judiciary Subcommittee in the US Senate on Technology, Terrorism, and Government Information, October 6, 1999. "Critical Information Infrastructure Protection: the Threat is Real".
- Tulsiani, Vijay. "Reliability-Based Management of River Navigation System." University of Virginia. January 1996.
- Tulsiani, Vijay. "Risk, Multiple Objectives, and Fault-Tree Analyses – A Unified Framework." University of Virginia. May 1989.
- United States General Accounting Office. DoD's Information Assurance Efforts. June 11, 1998. GAO/NSIAD 98-132R. Online. Internet. February 2000. Available: <http://www.fas.org/irp/gao/nsiad-98132.htm>.
- United States General Accounting Office. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. Chapter Report, May 22, 1996. GAO/AIMD 96-84. Online. Internet. February 2000. Available: <http://www.fas.org/irp/gao/aim96084.htm>.
- US Navy GPOJWF. *Joint Doctrine for Information Operations*. Joint Publication 3-13, Joint Chiefs of Staff Publication, Joint Warfare Center, October 1998.
- VincodinES (Hacker Nickname). "Theory of Better File Virus Distribution." Online. Internet. August 2000. Available: <http://www.zdnet.com/zdnnet/special/essay.html>.
- Vinson, D. R. and C. Georgakis (1996). The design of operable processes using plant-wide, steady-state measures. Technical Report 23, CPMC, Lehigh University.
- Walczak, Paul LTC, Project Manager for Information Assurance, US Army Research Lab. "Information Survivability for the Digitized Land Force." Online. Internet. September 2000. Available: http://www.cert.org/research/isw98/all_the_papers/no40.html.
- Wass de Czege, Huba, Brigadier General, US Army Retired. "New Paradigm Tactics: The rapid evolution of Army tactical capabilities and methods." Online. Internet. May 2000. Available: <http://www.ida.org/DIVISIONS/sctr/cpof/Huba%20Papers%20-%20New%20Paradigm%20Tactics%20P1.DOC>.

Wentz, Larry K. "C4ISR Systems and Services." Online. Internet. August 2000.
Available: http://call.army.mil/call/spc_prod/ccrp/lessons/bosch11a.htm.

Whatis.com. "IT Specific Encyclopedia." Online. Internet. February 2001. Available:
<http://whatis.techtarget.com>.

Willis, John B. Major and Lieutenant Colonel Mark J. Davis. "Design of the
Reconnaissance, Surveillance, and Target Acquisition Squadron for the US Army's
Brigade Combat Team." United States Military Academy, 2000.

Woodard, John L., Lieutenant General, USAF, Director for Command, Control
Communications and Computer Systems, Joint Staff. "Information Assurance
through Defense in Depth." February 2000.