

## Contents

<b>1</b>	<b>Brief Review of Cyber Incidents</b>	<b>1</b>
1.1	Cyber's Emergence as an Issue	3
1.2	Estonia and Georgia – Militarization of Cyber	4
1.3	Conclusions	6
<b>2</b>	<b>Cyber Security – An Introduction to Assessment and Maturity Frameworks</b>	<b>9</b>
2.1	Assessment Frameworks	9
2.2	NIST 800 Risk Framework	9
2.2.1	Maturity Models	12
2.2.2	Use Cases/Scenarios	13
2.3	Cyber Insurance Approaches	14
2.3.1	An Introduction to Loss Estimate and Rate Evaluation for Cyber	17
2.4	Conclusions	17
2.5	Future Work	18
2.6	Questions	18
<b>3</b>	<b>Introduction to Cyber Modeling and Simulation (M&amp;S)</b>	<b>19</b>
3.1	One Approach to the Science of Cyber Security	19
3.2	Cyber Mission System Development Framework	21
3.3	Cyber Risk Bow-Tie: Likelihood to Consequence Model	21
3.4	Semantic Network Model of Cyberattack	22
3.5	Taxonomy of Cyber M&S	24
3.6	Cyber Security as a Linear System – Model Example	25
3.7	Conclusions	26
3.8	Questions	27
<b>4</b>	<b>Technical and Operational Scenarios</b>	<b>29</b>
4.1	Scenario Development	30
4.1.1	Technical Scenarios and Critical Security Controls (CSCs)	31

4.1.2	ARMOUR Operational Scenarios (Canada)	32
4.2	Cyber System Description for M&S	34
4.2.1	State Diagram Models/Scenarios of Cyberattacks	34
4.2.2	McCumber Model	35
4.2.3	Military Activity and Cyber Effects (MACE) Taxonomy	36
4.2.4	Cyber Operational Architecture Training System (COATS) Scenarios	37
4.3	Modeling and Simulation Hierarchy – Strategic Decision Making and Procurement Risk Evaluation	39
4.4	Conclusions	42
4.5	Questions	43
<b>5</b>	<b>Cyber Standards for Modeling and Simulation</b>	<b>45</b>
5.1	Cyber Modeling and Simulation Standards Background	46
5.2	An Introduction to Cyber Standards for Modeling and Simulation	47
5.2.1	MITRE’s (MITRE) Cyber Threat Information Standards	47
5.2.2	Cyber Operational Architecture Training System	49
5.2.3	Levels of Conceptual Interoperability	50
5.3	Standards Overview – Cyber vs. Simulation	51
5.3.1	Simulation Interoperability Standards Organization (SISO) Standards	52
5.3.2	Cyber Standards	54
5.4	Conclusions	56
5.5	Questions	57
<b>6</b>	<b>Cyber Course of Action (COA) Strategies</b>	<b>59</b>
6.1	Cyber Course of Action (COA) Background	59
6.1.1	Effects-Based Cyber-COA Optimization Technology and Experiments (EBCOTE) Project	59
6.1.2	Crown Jewels Analysis	60
6.1.3	Cyber Mission Impact Assessment (CMIA) Tool	61
6.1.4	Analyzing Mission Impacts of Cyber Actions	63
6.2	Cyber Defense Measurables – Decision Support System (DSS) Evaluation Criteria	64
6.2.1	Visual Analytics	65
6.2.2	Managing Cyber Events	67
6.2.3	DSS COA and VV&A	68
6.3	Cyber Situational Awareness (SA)	68
6.3.1	Active and Passive Situational Awareness for Cyber	69
6.3.2	Cyber System Monitoring and Example Approaches	69
6.4	Cyber COAs and Decision Types	70
6.5	Conclusions	71

6.6	Further Considerations	72
6.7	Questions	72
<b>7</b>	<b>Cyber Computer-Assisted Exercise (CAX) and Situational Awareness (SA) via Cyber M&amp;S</b>	<b>75</b>
7.1	Training Type and Current Cyber Capabilities	77
7.2	Situational Awareness (SA) Background and Measures	78
7.3	Operational Cyber Domain and Training Considerations	79
7.4	Cyber Combined Arms Exercise (CAX) Environment Architecture	81
7.4.1	CAX Environment Architecture with Cyber Layer	82
7.4.2	Cyber Injections into Traditional CAX – Leveraging Constructive Simulation	84
7.4.3	Cyber CAX – Individual and Group Training	85
7.5	Conclusions	86
7.6	Future Work	87
7.7	Questions	87
<b>8</b>	<b>Cyber Model-Based Evaluation Background</b>	<b>89</b>
8.1	Emulators, Simulators, and Verification/Validation for Cyber System Description	89
8.2	Modeling Background	90
8.2.1	Cyber Simulators	91
8.2.2	Cyber Emulators	93
8.2.3	Emulator/Simulator Combinations for Cyber Systems	94
8.2.4	Verification, Validation, and Accreditation (VV&A)	96
8.3	Conclusions	99
8.4	Questions	100
<b>9</b>	<b>Cyber Modeling and Simulation and System Risk Analysis</b>	<b>101</b>
9.1	Background on Cyber System Risk Analysis	101
9.2	Introduction to using Modeling and Simulation for System Risk Analysis with Cyber Effects	104
9.3	General Business Enterprise Description Model	105
9.3.1	Translate Data to Knowledge	107
9.3.2	Understand the Enterprise	114
9.3.3	Sampling and Cyber Attack Rate Estimation	114
9.3.4	Finding Unknown Knowns – Success in Finding Improvised Explosive Device Example	116
9.4	Cyber Exploit Estimation	116
9.4.1	Enterprise Failure Estimation due to Cyber Effects	118
9.5	Countermeasures and Work Package Construction	120
9.6	Conclusions and Future Work	122
9.7	Questions	124

<b>10</b>	<b>Cyber Modeling &amp; Simulation (M&amp;S) for Test and Evaluation (T&amp;E)</b>	<b>125</b>
10.1	Background	125
10.2	Cyber Range Interoperability Standards (CRIS)	126
10.3	Cyber Range Event Process and Logical Range	127
10.4	Live, Virtual, and Constructive (LVC) for Cyber	130
10.4.1	Role of LVC in Capability Development	132
10.4.2	Use of LVC Simulations in Cyber Range Events	133
10.5	Applying the Logical Range Construct to System Under Test (SUT) Interaction	134
10.6	Conclusions	135
10.7	Questions	136
<b>11</b>	<b>Developing Model-Based Cyber Modeling and Simulation Frameworks</b>	<b>137</b>
11.1	Background	137
11.2	Model-Based Systems Engineering (MBSE) and System of Systems Description (Data Centric)	137
11.3	Knowledge-Based Systems Engineering (KBSE) for Cyber Simulation	138
11.3.1	DHS and SysML Modeling for Buildings (CEPHEID VARIABLE)	139
11.3.2	The Cyber Security Modeling Language (CySeMoL)	140
11.3.3	Cyber Attack Modeling and Impact Assessment Component (CAMIAC)	140
11.4	Architecture-Based Cyber System Optimization Framework	141
11.5	Conclusions	141
11.6	Questions	142
<b>12</b>	<b>Appendix: Cyber M&amp;S Supporting Data, Tools, and Techniques</b>	<b>143</b>
12.1	Cyber Modeling Considerations	143
12.1.1	Factors to Consider for Cyber Modeling	143
12.1.2	Lessons Learned from Physical Security	144
12.1.3	Cyber Threat Data Providers	146
12.1.4	Critical Security Controls (CSCs)	147
12.1.5	Situational Awareness Measures	147
12.2	Cyber Training Systems	148
12.2.1	Scalable Network Defense Trainer (NDT)	153
12.2.2	SELEX ES NetComm Simulation Environment (NCSE)	153
12.2.3	Example Cyber Tool Companies	154
12.3	Cyber-Related Patents and Applications	154
12.4	Conclusions	160
	<b>Bibliography</b>	<b>161</b>
	<b>Index</b>	<b>175</b>