

# Table of Contents

<b>Preface</b>	1
<b>Chapter 1: The Need for Cyber Intelligence</b>	7
<b>Need for cyber intelligence</b>	7
<b>The application of intelligence in the military</b>	9
Intel stories in history	9
The American Revolutionary War	10
Napoleon's use of intelligence	10
<b>Some types of intelligence</b>	11
HUMINT or human intelligence	11
IMINT or image intelligence	12
MASINT or measurement and signature intelligence	12
OSINT or open source intelligence	12
SIGINT or signals intelligence	13
COMINT or communications intelligence	13
ELINT or electronic intelligence	13
FISINT or foreign instrumentation signals intelligence	14
TECHINT or technical intelligence	14
MEDINT or medical intelligence	14
All source intelligence	15
<b>Intelligence drives operations</b>	16
Putting theory into practice isn't simple	20
<b>Understanding the maneuver warfare mentality</b>	23
Follow the process, the process will save you	23
What is maneuver warfare?	24
Tempo	24
The OODA Loop	26
Center of gravity and critical vulnerability	27
Surprise – creating and exploiting opportunity	28
Combined arms – collaboration	29
Flexibility	29
Decentralized command	29
<b>Summary</b>	30
<b>Chapter 2: Intelligence Development</b>	31
<b>The information hierarchy</b>	31
<b>Introduction to the intelligence cycle</b>	33
The intelligence cycle steps	34
Step 1 – Planning and direction	34
Requirements development	35
Requirements management	35

Directing the intelligence effort	36
Requirements satisfaction	37
Planning the intelligence support system	38
Step 2 – Collection	39
Step 3 – Processing	40
Step 4 – Analysis and Production	40
Step 5 – Dissemination	41
Methods	41
Channels	42
Modes	43
Dissemination architecture	43
Step 6 – Utilization	44
<b>Summary</b>	45
<b>Chapter 3: Integrating Cyber Intel, Security, and Operations</b>	47
<b>A different look at operations and security</b>	47
<b>Developing a strategic cyber intelligence capability</b>	48
Understanding our priorities	49
The business architecture	50
The data/application architecture	50
Technology architecture	50
Application of the architectures and cyber intelligence	50
A look at strategic cyber intelligence – level 1	52
<b>Introduction to operational security</b>	53
OPSEC step 1 – identify critical information	53
OPSEC step 2 – analysis of threats	54
OPSEC step 3 – analysis of vulnerabilities	54
OPSEC step 4 – assessment of risk	54
OPSEC step 5 – application of appropriate countermeasures	56
<b>OPSEC applicability in a business environment</b>	57
<b>Cyber intel program roles</b>	58
Strategic level – IT leadership	59
Strategic level – cyber intelligence program officer	59
Tactical level – IT leadership	60
Tactical level – cyber intelligence program manager	61
Operational level – IT leadership	62
Operational level – cyber intelligence analysts	62
<b>Summary</b>	63
<b>Chapter 4: Using Cyber Intelligence to Enable Active Defense</b>	65
<b>An introduction to Active Defense</b>	66
<b>Understanding the Cyber Kill Chain</b>	67
<b>General principles of Active Defense</b>	68
Active Defense – principle 1: annoyance	69
Active Defense – principle 2: attribution	69
<b>Enticement and entrapment in Active Defense</b>	70

Scenario A	70
Scenario B	71
<b>Types of Active Defense</b>	71
Types of Active Defense – manual	72
Types of Active Defense – automatic	72
<b>An application of tactical level Active Defense</b>	73
<b>Summary</b>	75
<b>Chapter 5: F3EAD for You and for Me</b>	77
<b>Understanding targeting</b>	78
<b>The F3EAD process</b>	82
<b>F3EAD in practice</b>	84
<b>F3EAD and the Cyber Kill Chain</b>	90
Cyber Kill Chain and OODA loop	90
Cyber Kill Chain and OPSEC	92
Cyber Kill Chain and the intelligence cycle	94
Cyber Kill Chain and F3EAD	95
<b>Application of F3EAD in the commercial space</b>	95
Limitations of F3EAD	96
<b>Summary</b>	97
<b>Chapter 6: Integrating Threat Intelligence and Operations</b>	99
<b>Understanding threat intelligence</b>	99
<b>Capability Maturity Model – threat intelligence overview</b>	102
Level 1 – threat intelligence collection capability	103
Phase initial	104
Example 1 – Open Threat Exchange – AlienVault	104
Example 2 - Twitter	111
Example 3 - Information Sharing and Analysis Centers	115
Example 4 - news alert notifications	116
Example 5 - Rich Site Summary feeds	117
Phase A	118
Example 1 - Cisco – GOSINT platform	120
Example 2 - The Malware Information Sharing Platform project	120
Phase B	120
Phase C	121
Level 2 – Threat Information Integration	122
Phase initial	123
Phase A	124
Categorization of items that are applicable to multiple teams	125
Phase B	125
Phase C	126
<b>Summary</b>	127
<b>Chapter 7: Creating the Collaboration Capability</b>	129
<b>Purpose of collaboration capability</b>	129
Formal communications	130

Informal communications	131
Communication and cyber intelligence process	131
Methods and tools for collaboration	133
Service level agreements and organizational level agreements	133
Responsible accountable supporting consulted informed matrix	134
Using key risk indicators	134
<b>Collaboration at the Strategic Level</b>	136
Executive support	138
Policies and procedures	138
Architecture	139
Understanding dependencies	139
Prioritized information	141
Intelligence aggregation	142
Intelligence reconciliation and presentation	143
<b>Collaboration at the Tactical Level</b>	145
Breaking down priority information requirements	145
Application of the theory	146
Theory versus reality	147
Creating the tactical dashboard	149
<b>Collaboration at the Operational Level</b>	152
<b>Summary</b>	154
<b>Chapter 8: The Security Stack</b>	155
<b>Purpose of integration – it's just my POV</b>	155
<b>Core security service basics</b>	156
<b>Security Operations Center</b>	158
The spider	159
Capabilities among teams	160
<b>Capability deep dive – Security Configuration Management</b>	161
Security Configuration Management – core processes	163
Security Configuration Management – Discovery and Detection	164
Security Configuration Management – Risk Mitigation	164
Security Configuration Management – Security State Analysis	165
Security Configuration Management – Data Exposure and Sharing	166
<b>Prelude – integrating like services</b>	168
<b>Integrating cyber intel from different services</b>	171
Overview – red team methodology	171
Red team – testing methods	172
White box	172
Gray box	172
Black box	172
Red team constraints	173
Red team – graphical representation	174
Data integration challenges	175
The end user perspective	175

The service level perspective – cyber intelligence – Data Exposure and Sharing	176
The SOC perspective	178
<b>Capability Maturity Model – InfoSec and cyber intel</b>	179
Capability Maturity Model - InfoSec and cyber intel – initial phase	180
Capability Maturity Model - InfoSec and cyber intel – Phase A	181
Capability Maturity Model - InfoSec and cyber intel – Phase B	182
Capability Maturity Model - InfoSec and cyber intel – Phase C	183
<b>Collaboration + Capability = Active Defense</b>	184
<b>Summary</b>	184
<b>Chapter 9: Driving Cyber Intel</b>	185
<b>The gap</b>	185
<b>Another set of eyes</b>	186
The logic	187
Event	188
Incident	189
Mapping events and incidents to InfoSec capabilities	189
<b>Capability Maturity Model – security awareness</b>	191
Capability Maturity Model - security awareness Phase - Initial	192
Capability Maturity Model - security awareness – Phase A	192
Capability Maturity Model - security awareness – Phase B	193
Capability Maturity Model - security awareness – Phase C	195
Capability Maturity Model - security awareness – Phase C +	196
Just another day part 1	197
<b>Summary</b>	198
<b>Chapter 10: Baselines and Anomalies</b>	201
<b>Setting up camp</b>	201
Baselines and anomalies	202
<b>Continuous monitoring – the challenge</b>	203
Part 1	203
Part 2	204
Part 3	206
<b>Capability Maturity Model – continuous monitoring overview</b>	207
Level 1 – phase A	208
Level 1 – phase B	209
Level 1 – phase C	210
<b>Capability Maturity Model – continuous monitoring level 2</b>	211
Scenario 1 – asset management/vulnerability scanning asset inventory	212
Phase initial	214
Information gathering	214
Developing possible solutions	215
Phase A	216
Procedure RASCI (example)	216
Phase B	216
Regional data centers	217
Local office environment	218

Phase C	218
Scenario 2 – security awareness/continuous monitoring/IT helpdesk	220
Phase initial	221
Information gathering	222
Developing possible solutions	223
Phase A	223
Procedure RASCI (example)	224
Phase B and C – sample questions	224
Just another day part 2	225
<b>Summary</b>	227
<b>Chapter 11: Putting Out the Fires</b>	229
<b>Quick review</b>	229
<b>Overview – incident response</b>	230
Preparation and prevention	231
Detection and analysis	232
Containment, eradication, and recovery	232
Post-incident activity	232
Incident response process and F3EAD integration	233
Intelligence process tie-in	234
<b>Capability Maturity Model – incident response</b>	235
Initial phase	235
Phase A	235
Phase B	236
Phase C	238
<b>Summary</b>	240
<b>Chapter 12: Vulnerability Management</b>	241
<b>A quick recap</b>	242
<b>The Common Vulnerability Scoring System calculator</b>	243
Base metric group	243
Temporal metric group	245
Environmental metric group	245
CVSS base scoring	246
Metrics madness	247
<b>Vulnerability management overview</b>	247
<b>Capability Maturity Model: vulnerability management – scanning</b>	249
Initial phase	250
Phase A	252
Phase B	253
Phase C	254
<b>Capability Maturity Model: vulnerability management – reporting</b>	255
Initial phase	255
Phase A	257
Phase B	258
Phase C	259

<b>Capability Maturity Model: vulnerability management – fix</b>	259
Initial phase	261
Phase A	262
Phase B	263
Phase C	265
<b>Summary</b>	267
<b>Chapter 13: Risky Business</b>	269
<b>Risk overview</b>	269
Treating risk	269
Risk tolerance and risk appetite	270
<b>Labeling things platinum, gold, silver, and copper</b>	271
Differentiating networks	272
<b>Taking a different look at risk</b>	272
Review of threat intelligence integration	273
Capability Maturity Model: risk phase – initial	274
Improving risk reporting part 1	275
Capability Maturity Model: risk phase – final	276
Improving risk reporting part 2	277
Open source governance risk and compliance tools	278
Binary Risk Assessment	278
STREAM cyber risk platform	278
Practical threat analysis for information security experts	278
SimpleRisk	278
Security Officers Management and Analysis Project	279
<b>Summary</b>	279
<b>Chapter 14: Assigning Metrics</b>	281
<b>Security configuration management</b>	281
Developing the risk score	282
Working in key risk indicators	284
<b>Summary</b>	286
<b>Chapter 15: Wrapping Up</b>	287
<b>Just another day part 3</b>	287
<b>Lessons learned</b>	288
<b>Other Books You May Enjoy</b>	291
<b>Index</b>	295

---