

# Contents

<b>Foreword</b>	<b>1</b>
<b>Preface</b>	<b>5</b>
<b>Introduction</b>	<b>9</b>
<b>I Key concepts</b>	<b>13</b>
<b>1 Information and intelligence</b>	<b>15</b>
1.1 Introduction . . . . .	15
1.2 Intelligence . . . . .	16
1.3 Intelligence gathering disciplines . . . . .	18
1.4 Information Operations . . . . .	20
1.5 Psychological Operations . . . . .	23
1.6 Critical infrastructures . . . . .	26
1.7 Tactics, techniques and procedures . . . . .	27
1.8 Words of Estimative Probability . . . . .	28
<b>2 Cyberspace</b>	<b>31</b>
2.1 Introduction . . . . .	31
2.2 Cyberspace . . . . .	32
2.3 Cyber intelligence . . . . .	35

2.4	Tactics, techniques and procedures in cyberspace . . . . .	38
2.5	Cyberspace Operations . . . . .	39
2.6	Threat actors in cyberspace . . . . .	41
2.7	Nation–state actors . . . . .	42
2.8	Advanced Persistent Threats . . . . .	45
2.9	Cyberspace and critical infrastructures . . . . .	47
2.10	MITRE ATT&CK . . . . .	48
2.11	DISARM . . . . .	50
<b>II</b>	<b>Russia, security and intelligence</b>	<b>53</b>
<b>3</b>	<b>Russia</b>	<b>55</b>
3.1	Introduction . . . . .	55
3.2	Russia and security . . . . .	57
3.3	Russia and intelligence . . . . .	59
3.4	Russia and defense . . . . .	61
3.5	Russia and cyberspace . . . . .	63
3.6	Russia and information warfare . . . . .	64
3.7	Active measures . . . . .	66
3.8	Russian information needs . . . . .	69
3.9	Vladimir PUTIN . . . . .	74
<b>4</b>	<b>The Russian cyber intelligence community</b>	<b>77</b>
4.1	Introduction . . . . .	77
4.2	FAPSI . . . . .	78
4.3	FSB: <i>Federal'naya Sluzhba Bezopasnosti</i> . . . . .	79
4.4	SVR: <i>Sluzhba Vneshney Razvedki</i> . . . . .	82
4.5	FSO: <i>Federal'naya Sluzhba Okhrani</i> . . . . .	83
4.6	GRU: <i>Glavnoye Razvedyvatelnoye Upravlenie</i> . . . . .	85

4.7	APT groups . . . . .	87
<b>5</b>	<b>The Russian cyber intelligence ecosystem</b>	<b>91</b>
5.1	Introduction . . . . .	91
5.2	Private companies . . . . .	94
5.3	Web brigades . . . . .	96
5.4	Patriotic hackers . . . . .	97
5.5	Cyber crime . . . . .	100
<b>III</b>	<b>GRU: <i>Glavnoye razvedyvatel'noye upravleniye</i></b>	<b>105</b>
<b>6</b>	<b>GRU: <i>Glavnoye razvedyvatel'noye upravleniye</i></b>	<b>107</b>
6.1	Introduction . . . . .	107
6.2	The roots . . . . .	111
6.3	Leadership and structure . . . . .	113
6.4	Activities and operations . . . . .	120
6.5	The GRU mindset . . . . .	123
6.6	The traitors: defectors and double agents . . . . .	124
6.7	GRU SIGINT . . . . .	126
6.8	GRU Information Operations . . . . .	130
6.9	The GRU in the media . . . . .	131
<b>7</b>	<b>2018: <i>annus horribilis</i></b>	<b>133</b>
7.1	Introduction . . . . .	133
7.2	July 2018 . . . . .	135
7.3	September 2018 . . . . .	137
7.4	October 2018 . . . . .	139
7.4.1	Holland . . . . .	139
7.4.2	UK . . . . .	140
7.4.3	USA . . . . .	140

7.4.4	Canada . . . . .	142
7.5	2018 was a bad year . . . . .	143
7.6	The 2018 targets . . . . .	144
7.6.1	USA 2016 Elections . . . . .	145
7.6.2	Novichok . . . . .	146
7.6.3	Doping in sport . . . . .	147
7.6.4	MH17 . . . . .	147
7.6.5	Ukraine . . . . .	148
7.7	Questions and conspiracies . . . . .	149
7.8	The 2018 aftermath . . . . .	151
7.9	Conclusions . . . . .	152
<b>IV</b>	<b>The GRU in cyberspace</b>	<b>155</b>
<b>8</b>	<b>The units</b>	<b>157</b>
8.1	Introduction . . . . .	157
8.2	Military Unit 26165 . . . . .	158
8.3	Military Unit 74455 . . . . .	161
8.4	Military Unit 29155 . . . . .	164
8.5	Military Unit 54777 . . . . .	166
8.6	Military Unit 55111 . . . . .	168
8.7	Military Unit 36360 . . . . .	170
8.8	Military Unit 11135 . . . . .	172
8.9	Other relevant GRU units . . . . .	172
8.10	Conclusions . . . . .	174
<b>9</b>	<b>APT groups</b>	<b>177</b>
9.1	Introduction . . . . .	177
9.2	APT28 . . . . .	179

9.3	Sandworm Team . . . . .	182
9.4	Ember Bear . . . . .	185
9.5	Saint Bear . . . . .	186
9.6	Laundry Bear . . . . .	187
<b>10</b>	<b>Beyond the GRU</b>	<b>191</b>
10.1	Introduction . . . . .	191
10.2	State actors: Russian intelligence agencies . . . . .	192
10.3	State actors: Russian Ministry of Defense . . . . .	193
10.4	Non-state actors: private companies . . . . .	195
10.5	Non-state actors: web brigades . . . . .	198
10.6	Non-state actors: criminal gangs . . . . .	199
10.7	Non-state actors: patriotic hackers . . . . .	200
10.8	Non-state actors: cyber proxies . . . . .	201
<b>11</b>	<b>Tactics and techniques</b>	<b>203</b>
11.1	Introduction . . . . .	203
11.2	Reconnaissance . . . . .	205
11.3	Resource development . . . . .	207
11.4	Initial access . . . . .	208
11.5	Execution . . . . .	209
11.6	Persistence . . . . .	210
11.7	Privilege escalation . . . . .	211
11.8	Defense evasion . . . . .	212
11.9	Credential access . . . . .	213
11.10	Discovery . . . . .	213
11.11	Lateral movement . . . . .	214
11.12	Collection . . . . .	215
11.13	Command and Control . . . . .	215
11.14	Exfiltration . . . . .	216

11.15	Impact . . . . .	217
11.16	Close access . . . . .	218
11.17	Deception . . . . .	220
11.18	OPSEC . . . . .	222
11.19	PSYOP tactics and techniques . . . . .	225
<b>12</b>	<b>The arsenal</b>	<b>229</b>
12.1	Introduction . . . . .	229
12.2	Infrastructure . . . . .	230
12.3	Tools . . . . .	232
12.4	Malware . . . . .	234
12.5	Exploits . . . . .	236
12.6	Identities . . . . .	238
12.7	Conclusions . . . . .	238
<b>13</b>	<b>Capabilities + targets = operations</b>	<b>241</b>
13.1	Introduction . . . . .	241
13.2	Capabilities . . . . .	242
13.3	Target countries . . . . .	244
13.4	Target sectors . . . . .	248
13.5	Operations . . . . .	252
<b>V</b>	<b>Final notes</b>	<b>257</b>
<b>14</b>	<b>Yes, but... how?</b>	<b>259</b>
14.1	Introduction . . . . .	259
14.2	Intelligence gathering . . . . .	260
14.3	Open source information gathering . . . . .	262
14.4	Threat characterization . . . . .	263
14.5	Threat detection . . . . .	265

14.6	Conclusions . . . . .	267
<b>15</b>	<b>So long, and thanks for all the fish</b>	<b>269</b>
15.1	To get started . . . . .	269
15.2	Things within and beyond cyberspace . . . . .	270
15.3	Russia: much more than intelligence . . . . .	271
15.4	The badass guys who act . . . . .	272
15.5	Acting in cyberspace . . . . .	272
15.6	Concluding . . . . .	273
15.7	From now on . . . . .	274
15.8	So long... . . . . .	275
<b>VI</b>	<b>Appendices</b>	<b>277</b>
<b>A</b>	<b>The GRU in Spain</b>	<b>279</b>
<b>B</b>	<b>MITRE ATT&amp;CK GRU tactics and techniques</b>	<b>285</b>
B.1	Reconnaissance . . . . .	285
B.2	Resource development . . . . .	286
B.3	Initial access . . . . .	287
B.4	Execution . . . . .	288
B.5	Persistence . . . . .	289
B.6	Privilege escalation . . . . .	290
B.7	Defense evasion . . . . .	291
B.8	Credential access . . . . .	293
B.9	Discovery . . . . .	294
B.10	Lateral movement . . . . .	294
B.11	Collection . . . . .	295
B.12	Command and Control . . . . .	296
B.13	Exfiltration . . . . .	297

B.14 Impact . . . . .	297
<b>C Acronyms</b>	<b>299</b>
<b>Bibliography</b>	<b>303</b>
<b>Index</b>	<b>367</b>