Index

A
access router (AR) 228, 241
access service authoriser (ASA) 226
access service provider (ASP) 226, 241
advanced persistent threat 88
air traffic controller 34
asymmetric warfare 31, 141-142
authentication, authorization and accounting (AAA) 241
authorization and bootstrapping information request (ABIREQ) 230
authorization and bootstrapping information response (ABIRES) 230
average residence time (AVR) 237

B
backward process 56, 59, 64
battlefield 30-31, 86-87, 138, 264
bootstrapping client identifier (BCID) 230
bootstrapping configuration agent (BCA) 230, 241

C
channel binding (CB) 232
Chebyshev Inequality 166, 171-172, 180
cognitive factors 129
cognitive Instance-based learning 125
collaboration services 40-41
collaborative situation awareness for decision making 29, 37, 355
command and control and situation awareness theory 29
commercial and military environments 29
common operating picture 30, 37-38, 40-41
complete learning cycle 130
comprehension 2-4, 32, 34, 39, 46, 72, 74, 79, 85, 98, 106-107, 114-115, 125-127, 130, 149, 200, 343
computation 39, 43, 49-50, 57, 69, 76, 110, 190, 269
computation process 49
counter network defense 1-2, 4-5, 7-8, 23, 49, 67, 71-81, 86, 88, 92, 122, 141, 161, 259-260, 284, 344, 355
counter network security 2, 8, 48, 105, 107, 109, 112, 116, 122, 260
crowd sourcing 37-38, 42
CSA-DM 37, 43
cyber analysts 30, 34
cyber c 30-37, 39, 41, 43
cyber command and control 29-30, 32, 35-36, 41, 43, 355
cyber doctrine 31
cyber-infrastructure 127-128
cybersecurity 46, 48, 68, 125-126, 138-139, 219
cyberspace 16, 29, 44, 74-75, 78-81, 115, 122, 140, 256, 259
cyber warriors 31

D
DARPA 99, 101, 162, 172-174, 179, 198, 296, 302-313, 315-318, 342
data collection services 38
data exfiltration 92
data mining 39, 83, 100, 150, 160, 167, 178-179, 184, 298, 316-318
decision-point nodes 88
defensive 21, 29, 48, 50-51, 55, 59-60, 67, 70, 95, 98, 151-154, 253-254, 291, 296
defensive and operational capabilities 29
degree of reliability 88
Index

detection and reporting of incidents and near-miss incidents 11
detection of malicious behavior 95
discrete time 51, 60
discrete-time dynamic evolutionary game 49
discrete-time stochastic control problem 48
   doctrinal aspects 31
dynamic host control protocol v6 (DHCPv6) 227
dynamic programming 48, 50, 53-55, 68-70

E
EAP extended master session key (EMSK) 229
EAP re-authentication protocol (ERP) 228
enterprise network 98, 102, 320, 322, 327, 330, 340
equilibrium analysis 51
   equilibrium approach 49
extensible authentication protocol (EAP) 221-222, 238-239, 241

F
Facebook 21
fast mobile IPv6 (FMIPv6) 222
field flight plan 34
forward process 56, 59, 62, 64
f-score 166, 173-174, 176-177, 180
fusion model 32, 161, 163

G
game theory 49, 68, 70, 287
guest OS 96

H
hacking 14, 16-17, 27, 94, 102, 154, 356
handover key response (HKResp) 231
handover key server (HKSS) 231
honeynet 98, 101-102
honeypot 102
human decision-making 87
human endeavor 86
human relations 10, 26
human resources security 13
human role and the theoretical relationship 20

I
importance of properly educating IT-users 13
information element (IE) 230
information key (IK) 231
information master key (IMK) 231
information security incident management 13, 17
information security policy 13, 25, 27-28
insider threat 11, 25
internalization of security policies 17
internet engineering task force (IETF) 222, 241
internet service provider (ISP) 195, 242
ISO 27001 15, 22
ISO 27002 15
IT abuse incidents 16
IT security 19, 23, 26, 101, 285, 348
IT systems 10, 12, 15, 28, 139, 249, 340

J
JDL 32, 74, 142, 147-148, 153, 155, 159, 161, 163-164
joint chiefs of staff and military service leadership 29
joint director’s laboratories 32

K
kinetic worlds 92
knowledge, attitudes and behaviour 18

L
local area network 89, 202, 293
logging host 89
long-term memory 34, 39-40, 46, 154

M
maritime domain awareness 30
McAfee 33
MDA 30
media independent handover function (MIHF) 225
media independent handover (MIH) 221-222
medium access control (MAC) 230, 239, 242
message integrity key (MIK) 231
military industrial complex 29-30
military operation 31, 104
mobile IPv6 (MIPv6) 222, 240
mobile node (MN) 222, 242
mobility service authorizer (MSA) 226, 242
mobility service provider (MSP) 226, 242
multi-player sequential decision making models 49

N
national cybersecurity 125
network access server (NAS) 224, 242
nominal stage 64
nonlinear objective functions 50
Norwegian Centre for Securing Information 21
Norwegian Computer Crime Survey 12, 15-16, 25-26
numerical experiment 48, 62
numerical stability 60

P
passive asset detection system 115
passive operating system fingerprint 115
point of attachment (PoA) 222, 226
probability of inertia 131, 136
protective monitoring 5, 105, 108-109, 113-114, 119, 252, 255, 258
protocol for carrying authentication for network access (PANA) 223, 240

Q
quality of service (QoS) 242

R
recognition-primed decision 76, 126
root master key (RMK) 229

S
sanctions and punishment 11, 15
Scandinavia 11
security awareness 10-11, 14, 16-18, 21, 28, 253
security controls 19
sensor fusion 163, 165-169, 176, 178-180, 254, 302-304, 309-311, 314, 318-319
service request identifier (SRID) 230
social networks 11, 21, 24
socio-technical theory 10-11, 15, 22-24, 72

T
the-need-to-know principle 11
threat to information security 10, 14
training in information security 12, 18, 23

U
unintentional threats 11
usage specific root key (USRK) 229

V
variable workload 117
voice over IP (VoIP) 222

W
wiki leaks 14
Windows Vista 12
WireShark 98-99