Stuxnet case study, 149–150
tactical decisions, 127
Axiom Attacker, 41–43

B
backdoors, 24
bad luck
as attacker friction, 81
as defender friction, 92
Bash, 2014 flaw, 88
battle damage assessment (BDA), 111
BDA (battle damage assessment), 111
Belgacom, GCHQ’s reported hack, 9
bidirectional access, 35
Bit9, 145
Blaster Worm, 88
botnets, 8
Rustock, 62
TDL4 rootkit, 79
bugs, 84

C
capability diffusion, 116–117
case studies
APT1, 162–164
Axiom, 164–165
DragonFly, 159–160
Flame, 154–157
Gauss, 157–159
Red October, 160–162
Stuxnet, 148–154
CERTs (Computer Emergency Response Teams), 119
China
alleged theft of Patriot Missile system, 7
APT1 group, 10, 162–164
Axiom group, 164–165
Chinese Great Firewall, 84
and Rustock botnet decapitation, 62
and “The Magnet of Threats,” 78
travelling in, 143
xFocus, 88
cloud-based security, 143–145
CNA (Computer Network Attack), 2–3
non-kinetic, 2, 3, 7–9, 11, 26
CND (Computer Network Defense), 2, 3
CNE (Computer Network Exploitation), 2, 3–4. See also espionage
first principles, 12
access, 12, 27–37
economy, 12, 37–41
humanity, 12, 17–18
operations, 4–11
directed collection, 7
duration, importance of, 11
life cycle, 18–27
non-kinetic CNA, 7–9
objectives, 5–10
positionial access, 9–10
strategic access, 9
strategic collection, 6
principles, 12–14
themes, 14–15
U.S. Department of Defense definition, 3
CNO (Computer Network Operations), 3
complexity
as attacker friction, 74–75
as defender friction, 89–91
Computer Emergency Response Teams (CERTs), 119
Computer Network Attack. See CNA
Computer Network Defense (CND), 2, 3
Computer Network Exploitation. See CNE
Computer Network Operations (CNO), 3
Conficker worm, 61, 79
constraints, 49, 50, 137
application whitelisting, 138–139
of economy, 37–41
network posture, 68–69
time, 69–70
cooperation principle, 12
cross-site-scripting (XSS) attacks, 31–32

D
data classification systems, 136
data exfiltration prevention, 50
data loss prevention, 50
DDOS attacks, 8
deadlocks, 84
deous life cycle, offensive, 49–51
defenders
access principle, 48–49
defensive life cycle, 49–51
economy principle, 51–53
frictions, 83–92
bad luck, 92
complexity, 89–91
flawed software, 84–86
inertia, 86–87
mistakes, 83–84
security community, 87–88
users, 91–92
humanity principle, 45–48
as unwitting helpers to attackers, 53
defensive strategy, 129–145
cloud-based security, 143–145
crafting, 135–143
failed tactics, 130–135
detection
e-mail attacks, 30–31
increasing cost of, 114–115
offensive operational life cycle, 26–27, 137
directed collection operations, 7
Distributed Denial of Service (DDOS) attacks, 8
diversity theme, 14–15, 102–103, 104–105, 109
DII hijacking, 138
DNS (domain name system), 32, 141–142
domain name hijacks, 32
DragonFly, 159–160
Duqu, 154
dynamic analysis, 116
Dynamic Internet Technology, 84
dynamism, 52
economy (first principle of CNE), 12, 13
attackers, 37–41
defenders, 51–53
Stuxnet case study, 149
tactical decisions, 126
efficiency, 70–71
Equation Group, 78, 103
espionage. See also CNE (Computer Network Exploitation)
APT1, 162–164
Axiom, 164–165
DragonFly, 159–160
Flame, 154–157
Gauss, 157–179
Red October, 160–162
exfiltration stage, offensive operational life cycle, 26, 53
expansion stage, offensive operational life cycle, 25–26, 53
exploitation. See CNE (Computer Network Exploitation)
exploitation expertise, 38
F
false asymmetries, 56–59
attrition, 57–59
cost, 56
firewalls, 34, 141, 159–160
first principles of CNE, 12
access, 12, 27–37, 48–49, 148–149
economy, 12, 13, 37–41, 51–53, 149
humanity, 12, 17–18, 45–48, 149
Flame, 154–157
focus asymmetry, 62
frictions
attacker frictions
bad luck, 81
complexity, 74–75
flawed tools, 75–77
mistakes, 74
other Attackers, 78–79
security community, 80–81
upgrades and updates, 77–78
defender frictions
bad luck, 92
complexity, 89–91
flawed tools, 84–86
inertia, 86–87
mistakes, 83–84
security community, 87–88
users, 91–92
definition of, 73
G
Gauss, 157–159
GCHQ, reported hack of Belgacom, 9
Google
Project Zero, 80
WebView, 87
Great Firewall, 84
Healthcare.gov, 90
Heartbleed bug, 67
honeypots, 63
hot-swappable tools, 125
humanity principle, 12
attackers, 17–18
defenders, 45–48
Stuxnet case study, 149
tactical decisions, 126
hypervisor-based rootkits, 144
I
iCloud, 85
iLOVEYOU virus, 30
inbound access, 27–29
incidence response companies, 51
Indexing Service, Microsoft Windows, 80
initial access stage, offensive operational lifecycle, 22–24, 53
initiative asymmetry, 61–62
innovation (CNE principle), 13, 98–101
defensive, 100–101
measuring, 99
offensive strategy questions, 123, 127
Stuxnet case study, 149
tactical decisions, 127
Internet
defined, 5
denying direct access, 141–142
NAT (network address translation), 57–59
iPhone App Store, 138
isolated networks, 35–36

K
kernel mode rootkit rewrites, 115
knowledge (CNE principle), 13, 95–96
offensive strategy questions, 122, 124
Stuxnet case study, 149
tactical decisions, 127

L
legitimate access, 28
liabilities, attacker, 110–112
life cycle of defensive operations, 49–51
life cycle of offensive operations, 18–27
detection, 26–27
exfiltration, 26
expansion, 25–26
initial access, 22–24
persistence, 24–25
targeting, 19–22
Linux
Bash flaw, 88
Shellshock vulnerability, 4
logging, 139–140
low-cost capabilities, 114
luck, bad
as attacker friction, 81
as defender friction, 92
LulzSec, 74

M
macros, Microsoft Office, 30
malicious code, 31, 34
Manageable Network Plan, 135–136
mass principle, 13
McRaven, William (Admiral), 105, 106
Microsoft
Alureon rootkit, 76
iLOVEYOU virus, 30
Office
e-mail attachments, 30
macros, 30
updates, 78
persistence, 24
positional access example, 10
Windows
Conficker worm, 61
Indexing Service, 80
SChannel flaw, 89–90
Windows Update, 155–157

mistakes
as attacker friction, 74
as defender friction, 83–84
Mitnick, Kevin, 33, 36
mobile transaction authentication numbers (mTAN), 28
modular frameworks, 124–126
Monsegur, Hector Xavier, 74
Morris worm, 29, 74
motivation asymmetry, 60–61
mTAN (mobile transaction authentication numbers), 28

N
NASDAQ, 2010 compromise, 22
NAT (network address translation), 57–59
network access
bidirectional, 35
inbound, 27–29
isolated networks, 35–36
outbound, 29–35
restricting, 34
network address translation (NAT), 57–59
network devices, 5
network segmentation and segregation, 139
networking expertise, 38–39
non-kinetic CNA, 2, 3
exfiltration requirements, 26
operations, 7–9, 11

O
obstruction, 49, 50, 137
offensive death cycle, 49–51
offensive strategy, 93–128
awareness principle, 97–98
crafting, 121–124
goals, 93–94
innovation principle, 98–101
knowledge principle, 95–96
modular frameworks, 124–126
operational security principle, 105–109
precaution principle, 101–105
program security principle, 110–121
tactical decisions, 126–127
OpenSSL, 67
Operation Aurora, 27
operational analysis expertise, 40
operational expertise, 40
operational security, 14, 105–109
exposure, minimizing, 106–107
measuring, 109
offensive strategy questions, 123–124, 127
reaction, controlling, 108–109
recognition, minimizing, 107–109
relative superiority and,
   105–106
Stuxnet case study, 151–153
tactical decisions, 127
operations, CNE, 4–11
directed collection, 7
duration, importance of, 11
life cycle, 18–27
non-kinetic CNA, 7–9
objectives, 5–10
positional access, 9–10
strategic access, 9
strategic collection, 6
opponent analysis, 101
outbound access, 29–35

P
parental control software, 33
password policies, 132–134
patching, 85–86, 88, 89
Patriot Missile System, China’s alleged
theft of, 7
pattern recognition, 107–108
penetration testing, 137
persistence stage, offensive operational life
cycle, 24–25, 53
personal security products, 33–34
phishing e-mails, 21–22, 159
plugin-based architecture, 124–126
Flame and, 154
Red October and, 161–162
pointy end of software, 65
positional access operations, 9–10
precaution (CNE principle), 13,
   101–105
offensive strategy questions, 123, 127
Stuxnet case study, 150–151
tactical decisions, 127
prevention, 49, 50, 51, 137
Principle of Least Privilege, 48–49
principles of CNE, 12–14
printers, 89
privacy, 49, 50, 51, 137
program security, 14, 110–121
Attacker liabilities, 110–112
costs, 112–120
measuring, 120–121
offensive strategy questions, 124, 127
Stuxnet case study, 153–154
tactical decisions, 127
Project Zero, Google, 80
proxy servers, 34

R
Rackspace, 144
Raytheon, directed collection operation
against, 7
Red October, 27, 160–162
redundancy, 14, 15, 102, 104, 121
Reed, Thomas, 148
relative superiority, 105–106
resources, technical, 41
responsible disclosure, 80
risk-based decisions, 52–53
rootkits
   Alureon, 76, 77
   kernel mode rewrites, 115
   Stuxnet, 151, 152, 154
   TDL4, 79
   ZeroAccess, 124
Russia, 8, 59, 119, 159, 161
Rustock botnet, 62

S
Sabu, 74
Saudi Aramco, 2012 Wiper malware attack, 9
SChannel flaw, 89–90
Schneier, Bruce, 89
security community
   as attacker friction, 80–81
   as defender friction, 87–88
segmentation, 139
segregation, 139
Seleznev, Roman Valerevich, 60
signature-based detection, 130–132
Snapchat, 29, 100
social engineering, 22, 33, 36, 95, 137
software development expertise, 39–40
Sony, 52, 74, 76, 93–94, 106, 130
South Korea, Wiper malware attack, 9
stealth threat, 14–15, 106–107, 130
strategic access operations, 9
strategic collection operations, 6
“Strategies to Mitigate Targeted Cyber
   Intrusions,” 137
strategy
   defensive, 129–145
      cloud-based security, 143–145
      crafting, 135–143
      failed tactics, 130–135
      defined, 93
   offensive, 93–94, 93–128
      awareness principle, 97–98
      crafting, 121–124
      goals, 93–94
      innovation principle, 98–101
      knowledge principle, 95–96
modular frameworks, 124–126
operational security principle, 105–109
precaution principle, 101–105
program security principle, 110–121
tactical decisions, 126–127
strong passwords, 132–134
Stuxnet, 8–9, 148–154
access principle, 148–149
awareness principle, 149–150
economy principle, 149
humanity principle, 149
innovation principle, 151
knowledge principle, 149
operational security principle, 151–153
precaution principle, 150–151
program security principle, 153–154
Subway sandwich chain, 2009 compromise, 21

T
Target retailer, 10, 84
targeting stage, offensive operational life
cycle, 19–22, 37–38, 49, 53
TDL4 rootkit, 79
technical resources, 41
themes of CNE, 14–15
TheMoon worm, 89
thumb drives, malicious, 32–33
time constraint
to attacker’s advantage, 37
to indeterminate advantage, 69–70
Track2, 60
ture asymmetries
to attacker’s advantage, 59–67
analysis of opponent, 64–65
effect of failure, 62–63
focus, 62
initiative, 61–62
knowledge of technology, 64
motivation, 60–61
rate of change, 66–67
tailored software, 65–66
to defender’s advantage, 67–69
network awareness, 68
network posture, 68–69
to indeterminate advantage, 69–71
Twenty Critical Security Controls for Effective
Cyber Defense, 135–136

U
unity of command, 12
updates, 77–78
upgrades, 77–78
users
as defender friction, 91–92
training, 134–134

V
vulnerabilities, reported by NIST, 23

W
watering hole attacks, 31
web domain whitelisting, 140–141
web proxy, authenticated, 141–142
website hijacks, 31–32
WebView, Google, 87
whitelisting
application whitelisting, 138–139
web domain whitelisting, 140–141
Windows
Conficker worm, 61
Indexing Service, 80
persistence, 24
SChannel flaw, 89–90
Windows Update, 155–157
Windows Update, 155–157
Wiper malware, 9
worms
Blaster, 88
Conficker, 61, 79
indiscriminate, 3–4
Morris, 29, 74
Stuxnet. See Stuxnet
TheMoon, 89

X
xFocus, 88
XSS (cross-site-scripting) attacks, 31–32

Z
ZeroAccess rootkit, 124
Zeus-in-the-middle (ZitMo), 28, 124