

Index

Note: Page numbers followed by *f* or *t* indicate material in figures or tables, respectively.

A

access control list (ACL), 283
 ACLU. *See* American Civil Liberties Union
 act on objectives phase, Cyber Kill Chain, 114
 active defense, 289–290
 active response, 291–292
 darknet, 290
 honeynets, 290, 291*f*
 honeypot, 290, 291*f*
 active response, 291–292
 activists, 161
 Anonymous, 172–173
 Estonia, 171
 SEA, 171–172
 adaptive chosen plaintext, 227
 administrative privileges, 186
 Advanced Encryption Standard (AES), 221
 advanced persistent threats (APTs), 101, 114, 258
 characteristics of, 102
 CSSC's goals, 343
 life cycle, 341*f*
 motivations
 activism, 103–104
 cybercrime and corporate espionage, 103
 military/political, 103
 tradecraft
 malware, 105
 social engineering and phishing, 105
 strategic web compromises, 105
 zero-day attacks, 104
 advanced tools and training of cyberwarfare, 351–352
 AES. *See* Advanced Encryption Standard
 AFCERT. *See* Air Force's Computer Emergency Response Team
 air domain of warfare, 13
 Air Forces Cyber, 43
 airmen, cyber tips to, 331
 alliances and partnerships, 346–347

ambush techniques, 8
 American Civil Liberties Union (ACLU), 164
 American Revolution, 8
 AMS. *See* Assignments Management System
 Analysis and Production phase, 78
 Analyzer activity, 142
 ancient warfare, 9
 Anonymous, 7, 37–38, 37*f*, 172–173
 anti-malware packages, 202
 anti-malware software, 251, 259
 failure of, 260
 anti-malware technologies, 203
 antiexploitation features, implementing, 186
 antivirus (AV) file reputation services, 186
 ANY/ANY rule, 281
 application-aware firewalls, 281
 application whitelisting, 186
 APTs. *See* advanced persistent threats
Art of War (Sun Tzu), 32
 Assignments Management System (AMS), 324
 Associated Press (AP) Twitter account, 32
 asymmetric ciphers, 215–219
 scaling, 216*t*
 asymmetric cyberwarfare, military targets in, 32–33
 asymmetric encryption, 215
 asymmetric warfare, 28
 attack delivery mechanisms, 109
 attackers in cyberwarfare, 241, 298, 306
 Aurora attacks, 38–39, 260
 authentication, 210, 218
 and authorization systems, 201
 authenticity, 182
 authority, 125–127
 availability, 182, 191, 305–307

B

backups, 307
 baiting attack, 133
 baseline configuration, 187
 basic input/output system (BIOS), 251
 behavior-based anti-malware capabilities, 203

behavior-based detection system, 285
 Bell-LaPadula model, 297
 BGP. *See* Border Gateway Protocol
 Biba model, 297
 BIOS. *See* basic input/output system
 Bitcoin, 235
 black box penetration testing, 265
 black-hat hackers, 174
 blacklisting, 261, 263–264, 263f
 bomba, 214
 bombe, 11, 215
 Border Gateway Protocol (BGP), 279
 British Defense Doctrine, 321
 brute-force attack, 227
 buffer overflow, 111

C

C-I-A triad, 182f, 191
 C2 phase. *See* Command and Control (C2) phase of Cyber Kill Chain
 CA. *See* certificate authority
 Caesar cipher, 9
 Caesar, Julius, 9, 209, 210
 Careto, 154
 CCD COE. *See* Cooperative Cyber Defence Centre of Excellence
 Central Intelligence Agency (CIA), 80
 central management systems, 256–257
 centralized protection capabilities, 349
 certificate authority (CA), 224
 certification, testing technique, 264
 changing threat model
 historical hacking, 97
 modern hacking
 focused attacks, 100–101
 opportunistic attacks, 98–99
 semi-targeted attacks, 99–100
 checksums, 210, 212
 Cheney, Richard, 249, 349
 China, cyberattack on Google, 38–39
 chosen plaintext, 227
 Churchill, Winston, 11
 C4I. *See* Command, Control, Communications, Computers, and Intelligence
 CIA. *See* Central Intelligence Agency
 Cialdini, Robert, 121
 CIL. *See* critical information list
 ciphers, 211–212
 ciphertext, 211, 227
 civilian infrastructure, 54, 66–69, 67f

classification, data, 295
 clone phishing, 131
 clothes, symbols of power, 126
 cloud computing, 59
 CMRS. *See* Continuous Monitoring and Risk Scoring
 CNA. *See* computer network attack
 CND. *See* computer network defense
 CNE. *See* computer network exploitation
 CNO. *See* computer network operations
 code, 211
 code-breaking technology, 195
 Code Red worm, 146–147
 coercion, motivation of spies, 81
 cold war, 12
 Collection phase of intelligence cycle, 77
 collection plan, preparation of, 77
 COMINT. *See* communications intelligence
 Command and Control (C2) phase of Cyber Kill Chain, 112–113
 Command, Control, Communications, Computers, and Intelligence (C4I), 248, 278
 commitment and consistency principle, 123–124
 Common Access Card (CAC), 225
 Common Criteria, 185
 Common Criteria Protection Profile, 185
 communications intelligence (COMINT), 83
 communications targets, conventional warfare, 29
 computer network attack (CNA), 17, 25, 225–226
 computer network defenders, 351
 computer network defense (CND), 18, 25, 189–190, 224–225
 computer network defense (CND) strategies, 177–178
 designing a modern
 dynamic defense, 196–198
 risk and threats, 198–199
 secure networks, 199–205
 computer network exploitation (CNE), 18
 computer network operations (CNO), 148
 concentric castles, 180f
 conduct of attacks and indiscriminate means, 68–69
 “Confidence in Cyberspace” guide, 186
 confidentiality, 182, 191, 210, 218
 configuration baseline, selecting, 204
 configuration management systems, 257, 265
 configuration standards, 256
 consumer-grade operating systems, 236
 content filtering, 134–135
 continuous low-level warfare, 344
 Continuous Monitoring and Risk Scoring (CMRS), 303
 continuous threats to systems and networks, 344f

- continuous warfare, systems and networks, 344f
- control, laws of war, 60
- Control System Security Center (CSSC), 343, 346
- Controlled Unclassified Information (CUI), 297
- conventional warfare, 26, 28, 322
 - goal of, 27
 - military targets in, 28–30
- Cooperative Cyber Defence Centre of Excellence (CCD COE), 57, 346
- corporations, 160
 - industrial espionage, 169
 - and intelligence agencies, 170
- countermeasure implementation, 23
- CPI. *See* Critical Program Information
- critical information, identification of, 22
- critical information list (CIL), 22
- Critical Program Information (CPI), 297
- cryptanalysis, 84, 226
- cryptocurrency, 339
- cryptographers, 10
- cryptographic hash, 222
- cryptographic systems, 229
 - computer network attack and, 225–226
 - computer network defense and, 224–225
 - defeating attacks on, 229–231
 - defense in depth using, 230–231
- cryptography, 202, 207–210, 232
 - asymmetric ciphers, 215–219
 - attacking, 226–227
 - brute-force, 227
 - ciphers and encryption, 211–212
 - cryptographic concepts, 210–211
 - in cyberwar. *See* cyberwar
 - goals of, 211
 - hash life cycle, 223
 - hashing and message digests, 222
 - modern cryptosystems, 220–221
 - symmetric ciphers, 212–215, 214f
- Cryptolocker, 231, 234–235
- Cryptome*, 165, 166
- cryptosystem, 211
- CSSC. *See* Control System Security Center
- Cuban Missile Crisis, 12, 86
- CUI. *See* Controlled Unclassified Information
- cyber domain, 13
 - exploring, 14–16
- Cyber Kill Chain®, 106
 - act on objectives phase, 114
 - Command and Control phase, 112–113
 - Deliver phase, 109–110
 - Exploit phase, 110–111
 - Install phase, 111–112
 - Reconnaissance phase, 106–108
 - steps, 106
 - Weaponize phase, 108–109
- cyber operations, organizing for, 326–329, 326f, 328f
 - U.S. Cyber Command (USCYBERCOM), 329–330
 - U.S. Strategic Command (USSTRATCOM), 329
- cyber ranges, advanced training on, 351
- cyber tips, to airmen, 331
- cyberattackers, 5, 55, 56
 - Amnesty International targeted by, 163
 - U.S. Air Force targeted by, 324
- cybercrime, 103
 - in Romania, 168
- cyberespionage, 5
- cyberhygiene, 252, 253
- cyberintelligence, 33
- cybersecurity threats, 15
- Cyberspace Policy Review, 348
- cyberspace, weaponizing. *See* weaponizing cyberspace
- cybertargets, in unconventional warfare, 32
- cyberwarfare, 5, 25–26, 207–208
 - combatants in
 - guerrilla cyberwarriors and insurrectionists, 43–45
 - individuals and small groups, 45–46
 - military forces, 42–43
 - components in, 293
 - concept of, 4
 - creation of, 178
 - cryptography in, 224
 - Common Access Cards, 225
 - computer network defense and cryptographic systems, 224–225
 - defenders in, 270, 291, 293, 345
 - defined, 5
 - ethics and, 70–71
 - future of, 335–336
 - vs. guerrilla warfare and traditional warfare, 47–49, 48t
 - information operations, techniques of, 16f
 - intelligence support to, 87–88
 - and kinetic warfare, integrating, 345
 - likelihood of, 6–7
 - and military doctrine, 317–331
 - NGOs in
 - aid groups, 165–166
 - diplomatic organizations, 166
 - religious organizations, 167

cyberwarfare, *continued*
 and nonstate actors
 APTs, 340–343
 attack tools, analysis of, 337
 continuous warfare, 343–345
 Langner's analysis, 339
 roles of, 163–165
 pillars of, 330
 terminology of, 7
 cyberwarfare law
 civilians and infrastructure, 66
 conduct of attacks and indiscriminate means,
 68–69
 military use of Internet, 67
 prohibited targets, 67–68
 control, 60
 espionage, treachery, and ruses, 69
 jurisdiction, 58–59
 kinetic warfare context, 55–56
 neutrality, 69–70
 responsibility, 60–63
 self-defense, 65–66
 United Nations, 66
 sovereignty, 58
 Tallinn Manual, 57
 use of force, 63, 64*f*
 measuring force, 63–64
 threats of force, 65
 cyberwarfare reconnaissance process, 107
 cyberwarfare targets, 33–34
 nontraditional, 36
 industrial espionage, 38–40
 military cyberattacks, 40–41
 political activism and hacktivism, 37–38
 against traditional military targets
 Flame malware, 36
 Iran vs. U.S. drones, 34–35, 35*f*
 Serbia and Kosovo, 36
 cyberwarfare technologies and techniques, 232
 cyberwarriors, 33, 109

D

damage containment, 186
 darknet, 290
 DARPA. *See* U.S. Defense Advanced Research
 Projects Agency
 data at rest, 309
 data availability, 305–307
 data center eavesdropping, 90
 data classification, 295–297, 296*f*
 data creation, 309
 Data Encryption Standard (DES), 220
 Data Execution Prevention (DEP), 111
 data in motion, 309
 data integrity, 210, 218, 305, 306
 data labeling, 309–310
 Data Lifecycle Management (DLM), 308–310
 data loss prevention (DLP) systems, 119,
 298–302
 data spills, 298–299
 deployment challenges, 302
 encryption and data loss, 303–305
 at network boundary, 301*f*
 on workstation, 302*f*
 data loss response, 312–313
 data retention and disposal, 308
 DLM, 308–310
 drives and media management, 310–311
 DRM, 310
 data security tools, using, 298
 data spillage events, 298
 Dearlove, Richard, 12
 DEC. *See* Digital Equipment Corporation
 declassified, 296
 decryption process, 209
 defenders in cyberwar, 210, 345
 defending data, 293–294
 classification, 295–297
 data loss
 and prevention, 298–305
 response, 312–313
 integrity and availability, 305–307
 retention and disposal, 308–311
 defense against malware, 202–203
 defense in depth, 178
 in endpoint security, 253
 defense-in-depth strategies, 177–178
 changes in technology, 195–196
 CND strategy, designing a modern
 dynamic defense, 196–198
 risk and threats, 198–199
 secure networks, 199–205
 computer network defense, 189–190
 Department of Defense, 189
 for endpoints, 251, 252*f*
 human factors, 194–195
 neglecting layers, 191–192
 NSA people, technology, and operations defense
 strategy, 183–188
 system administrators, 193–194

Defense Information Systems Agency (DISA), 277, 299
 CMRS, 303
 Defense Information Systems Network (DISN), 278
 Defense Intelligence Agency (DIA), 80
 Defense Logistics Agency, 299
 defenses, 230
 against attacks on encryption, 236–237
 defensive cryptography, 231–232
 defensive cyberwar, future of, 352
 defensive cyberwarfare, supporting, 88
 defensive information operations, 15–16
 degausser, 311
 Deliver phase of Cyber Kill Chain, 109–110
 demilitarized zone (DMZ), 112
 denial of service (DoS) attacks, 37
 DEP. *See* Data Execution Prevention
 Department of the Navy CND defense-in-depth strategy, 190*f*
Der Spiegel newspaper, 90
 DES. *See* Data Encryption Standard
 detection, dangers of, 285
 device integrity, 186
 DIA. *See* Defense Intelligence Agency
 DIACAP. *See* DoD's Information Assurance Certification and Accreditation Process
 DigiNotar, 226
 digital certificates, 224, 226
 Digital Equipment Corporation (DEC), 97
 digital rights management (DRM), 310
 directness, measuring force, 63
 DISA. *See* Defense Information Systems Agency
 discovery DLP systems, 300
 DISN. *See* Defense Information Systems Network
 Dissemination phase, 78, 79*f*
 distributed control systems, 245, 245*f*
 DJIA. *See* Dow Jones Industrial Average
 DLM. *See* Data Lifecycle Management
 DLP systems. *See* data loss prevention systems
 DMZ. *See* demilitarized zone
 DNI. *See* United States Director of National Intelligence
 doctrine, military, 319
 DoD. *See* U.S. Department of Defense
 DoD *Strategy for Operating in Cyberspace*, 14
 DoD's Information Assurance Certification and Accreditation Process (DIACAP), 273, 274
 domains, 187
 of warfare, 13–14, 14*f*
 Doodle Labs, 119
 DoS attacks. *See* denial of service attacks

Dow Jones Industrial Average (DJIA), 32
 downgraded data, 296
 drive destruction, 312
 drive encryption, 224, 225
 DRM. *See* digital rights management
 drone platforms, 246–247
 Dual Elliptic Curve cryptographic system, 229
 dumpster diving, 132
 Duqu, 152, 153*f*
 dynamic defense, 196–198

E

e-mail messages, 135
 Echelon program, 89
 economy of force, 320
 EEs. *See* essential elements of information
 ego, motivation of spies, 81
 electro-optical intelligence, 87
 electronic attack, 19
 electronic intelligence (ELINT), 83
 electronic protect, 19
 electronic warfare, 18–19
 Eligible Receiver, 139, 144
 ELINT. *See* electronic intelligence
 embassy personnel in foreign countries, 81
 embedded systems, 248–249
 enclaves, 199
 encryption, 209–212, 260–261, 303, 304*f*, 305*t*
 algorithms, 228
 end-to-end encryption, 237
 endpoint security
 defense in depth, 253
 design, 203
 endpoint switches, 283
 endpoint system, 240–242
 attacking, 250
 protecting, 251–252
 anti-malware and antivirus, 258–259
 awareness, 258
 blacklisting, 263–264, 263*f*
 central management systems, 256–257
 configuration standards, 256
 encryption, 260–261
 network protection, 259
 physical security, 254
 policy, 254–255, 255*f*
 procedures, 255–256, 255*f*
 testing, 264–265
 U.S. Department of Defense strategy, 252–253
 whitelisting, 261–263, 262*f*

endpoint system, *continued*
 types of, 242
 computers, 242–243
 embedded systems, 248–249
 ICS. *See* industrial control system (ICS)
 military systems, 246–248
 mobile devices, 243
 Enigma device, 10–11, 10*f*, 213–215
 enterprise device, 282
 espionage acts, 69
 essential elements of information (EEIs), 76, 78
 ethics and cyberwarfare, 70–71
 Exploit phase of Cyber Kill Chain, 110–111

F

F-22 Raptors, 248
 Facebook, 17, 38, 67, 67*f*, 170, 336
 factoring, 215
 fake cellular towers, 287
 fake wireless networks, 287
 FBI. *See* Federal Bureau of Investigation
 FBIS. *See* Foreign Broadcast Information Service
 Federal Bureau of Investigation (FBI), 80
 Federal Information Processing Standard (FIPS), 220
 Federal Risk and Authorization Management Program (FedRAMP), 350
 file encryption, 224, 226
 financial intelligence (FININT), 90
 Financial Services Information Sharing and Analysis Center (FS-ISAC), 346
 FININT. *See* financial intelligence
 FIPS. *See* Federal Information Processing Standard
 firewalls, 200, 280, 283
 application-aware, 281
 handling, 282*f*
 packet filter, 280
 routers and switches, 282–283
 stateful packet inspection, 281
 firmware, 251
 1st Information Operations Command, 43
 FISINT. *See* foreign instrumentation signals intelligence
 Flame malware, 35, 35*f*, 36, 152–153
 flash memory, 311
 flash plug-in, 192
 Fleet Cyber Command, 43
 floppy disks, 311
 focused attacks, 100–101
 For Official Use Only (FOUO), 297
 Foreign Broadcast Information Service (FBIS), 85

foreign instrumentation signals intelligence (FISINT), 84, 87
Foreign Policy magazine, 18
 FOUO. *See* For Official Use Only
 FOXACID, 153
 frequency intelligence, 87
 friendly military forces, 81
Frontline, 143
 FS-ISAC. *See* Financial Services Information Sharing and Analysis Center
 Future Force Warrior design, 242

G

GAO. *See* Government Accountability Office
 Geneva Conventions, 30, 54, 62, 66, 67
 GEOINT. *See* geospatial intelligence
 geophysical intelligence, 87
 geospatial intelligence (GEOINT), 85–86
 German World War II Enigma device, 195
 Global Positioning System (GPS), 34, 35*f*, 246
 Goldwater-Nichols Act, 321
 Google, 17, 38–39, 85, 90, 151, 169, 170, 226, 228, 243, 246, 350
 Government Accountability Office (GAO), 327
 government agencies, 293
 GPS. *See* Global Positioning System
 gray-hat hackers, 174
Guardian newspaper, 89
 guerrilla cyberwarriors, 43–45
 guerrilla warfare, 28
 vs. traditional warfare and cyberwarfare, 47–49, 48*t*

H

hackers, 174
 hacking
 historical, 97
 modern
 focused attacks, 100–101
 opportunistic attacks, 98–99
 semi-targeted attacks, 99–100
 hacktivism, 37–38
 hacktivist, 339
 Hague Conventions, 31
 Hanssen, Robert, 82
 hard drives, 311
 hash life cycle, 223
 hashes, 195, 212, 222, 225, 226
 Health Information Trust Alliance (HITRUST), 346
 Heartbleed bug, 228

heuristic-based anti-malware capabilities, 203
 heuristic-based detection, 285
 heuristics, 259
 Hewlett-Packard (HP), 130
 HITRUST. *See* Health Information Trust Alliance
 HMI. *See* Human Machine Interface
 honeynets, 290, 291f
 honeypot, 290, 291f
 Honker Union, 145
 host-based DLP systems, 300
 host-based software firewalls, 282
 host intrusion prevention system (HIPS) rules, 187
 hostile military forces, 81
 HP. *See* Hewlett-Packard
 human intelligence (HUMINT), 80–82, 83f
 Human Machine Interface (HMI), 245
 humans, weak link, 119–120
 HUMINT. *See* human intelligence
 Hunter Industries, 120

I

ICBMs. *See* intercontinental ballistic missiles
 ICJ. *See* International Court of Justice
 ICS. *See* industrial control system
 ideology, motivation of spies, 81
 IDSs. *See* intrusion detection systems
 imagery intelligence (IMINT), 85
 immediacy, measuring force, 63
 in-place encryption, 202
 in-transit encryption, 202
 indicators, 22
 indiscriminate attacks, conduct of attacks and, 68–69
 individual motivations for cyberwarfare, 173
 industrial control system (ICS), 244–245
 distributed control systems, 245, 245f
 PLCs, 245–246
 SCADA systems, 244, 244f
 industrial espionage, 38–40, 169
 influence, as weapon, 121–122, 122f
 authority, 125–127
 commitment and consistency, principle of, 123–124
 liking, principle of, 127–128
 reciprocity, 122–123
 scarcity principle, 128–129
 social proof, 125
Influence: Science and Practice (Cialdini), 121
 information, 4, 79, 79f
 in armed conflict, role of, 9–12
 information assurance, 273
 Information Assurance defense-in-depth strategy, 185

Information Assurance designs, 189
 Information Assurance Directorate (IAD) of the
 National Security Agency, 185
 Information Assurance Support Environment, 309
 Information Enterprise strategic plan for
 2010–2012, 304
 information operations, 7
 categories of, 14–15
 techniques, 16–17
 CNA, 17
 CND, 18
 countermeasure implementation, 23
 critical information, identification of, 22
 electronic warfare, 18–19
 intelligence gathering, 18
 military deception, 20
 OPSEC, 20, 21f
 PSYOPs, 19–20
 risk assessment, 23
 threat analysis, 22
 vulnerability analysis, 22
Information Operations Roadmap, 17
 information operations, targets of, 41–42, 41t
 information sharing, 258
 information technology (IT), 3–4
 information warfare, 7, 16
 InfraGard, 346
 infrastructure
 civilian, 54, 66–69, 67f
 cyberwar and, 350
 targets, conventional warfare, 29
 initial training, 134
 Install phase of Cyber Kill Chain, 111–112
 insurrectionists, 43–45
 integrity, 182, 191, 305, 306
 intelligence activities, media reporting on, 89
 data center eavesdropping, 90
 “Follow the Money,” 90
 Quantum program, 90–91
 intelligence agencies, 87
 intelligence architecture, development of, 77
 intelligence community, 76f
 intelligence cycle, 75–76, 76f, 79f
 intelligence disciplines, 80
 GEOINT, 85–86
 HUMINT, 80–82, 83f
 MASINT, 87
 OSINT, 84–85
 SIGINT, 83–84
 intelligence gathering, 18, 25

intelligence operations, 75
 Analysis and Production phase, 78
 case studies, 89–91
 Collection phase, 77
 Dissemination phase, 78, 79*f*
 intelligence cycle, 75–76, 76*f*
 Planning and Direction phase, 76–77
 Processing and Exploitation phase, 77–78
 intelligence requirements, 76–77
 intelligence support, to cyberwarfare, 87–88
 intercontinental ballistic missiles (ICBMs), 87
 international agreement on cyberlaw, 352
 International Court of Justice (ICJ), 55, 61
 International Governmental Organizations, 66
 international law
 and cyberwarfare, 347–348
 and kinetic warfare, 53–55
 international organized crime, 159
 International Telecommunication Union (ITU), 166
 Internet, 32, 270, 283
 network and telecommunications infrastructure, 26
 Internet-accessible systems, 194
 Internet of Things, 348
 intrusion detection systems (IDSs), 201, 285
 intrusion prevention systems (IPs), 201, 285
 invasiveness, measuring force, 63
 IPSs. *See* intrusion prevention systems
 IPv4, 283
 Iran and U.S. drones, 34–35, 35*f*
 Iraq war, 12, 41
 irregular warfare, 322
 IT. *See* information technology
 ITU. *See* International Telecommunication Union

J

Joint Publication 2.0: *Joint Intelligence*, 76
 Joint Task Force for Computer Network
 Defense, 189
 jurisdiction, 58–59
jus ad bellum law, 54
jus in bello law, 55, 66
 JWICS. *See* TC/SCI IP Data

K

Kennedy, John F., 12
 Kerckhoffs's principle, 222
 key distribution, 213
 key, encryption, 211
 key pair, 219
 key space, 211

Keyworth, George, 130
 kill chain, 106
 kinetic warfare
 defined, 53
 integrating cyberwar and, 345
 international law and, 53–55
 legal review and legality of actions, 55
 kinetic warfare context, cyberwarfare in, 55–56
 kinetic warfare law in cyber context, 56
 known plaintext, 227
 Kosovo, U.S. cyberwar strike, 36

L

land domain of warfare, 13
 LANs. *See* local area networks
 large-scale catastrophic cyberattacks, 6
 large-scale commodity cloud computing, 350
 Law Enforcement Sensitive (LES), 297
 laws of war, 31
 leakers, 174–175
 legal authority, 126
 legitimacy, 321
 LES. *See* Law Enforcement Sensitive
 Lieber Code in 1863, 31
 likelihood of cyberwar, 6–7
 liking principle, 127–128
 local area networks (LANs), 270
 LOIC. *See* Low Orbit Ion Cannon
 long-haul infrastructure, 278
 Low Orbit Ion Cannon (LOIC), 46

M

MAC. *See* Mission Assurance Categories
 magnetic media, 311
 malware, 105, 343
 defense against, 202–203
 encryption, 231–232
 maneuver, principles of war, 320
 MASINT. *See* measurement and signature
 intelligence
 mass, principles of war, 320
 materials intelligence, 87
 MD5, 222, 223
 mean time between failure (MTBF), 311
 measurable damage, measuring force, 63
 measurement and signature intelligence
 (MASINT), 84, 87
 measuring force, 63–64
 medical devices, 249
 meet-in-the-middle attack, 221

mercenaries, 61–63, 62*f*
 message digests, 210, 212, 222
 metadata, 89, 309
 military, 5. *See also* U.S. military
 character, measuring force, 64
 information operations, 7
 infrastructure, 54
 planners, 13, 14
 PSYOPs, roles for, 19
 use of Internet, civilians and, 67
 military asset, information as, 4
 military cyberattacks, on nontraditional
 cyberwarfare targets, 40–41
 military deception, 20
 military doctrine, 317, 319
 war, principles of, 319–321
 warfare
 forms of, 322–323
 levels of, 323, 325, 325*f*
 military forces, 42–43
 Military Information Support Operations (MISO), 19
 military research targets, conventional warfare, 29
 military targets, 27–28
 acceptable targets, treaties, and international
 law, 30–31
 in asymmetric cyberwarfare, 32–33
 in conventional warfare, 28–30
 total cyberwarfare, 33
 in unconventional warfare, 32
 MISO. *See* Military Information Support Operations
 mission assurance, 267, 272–274
 network operational procedures, 275–276
 surviving attacks, 275
 Mission Assurance Categories (MAC), 273
 Mitnick, Kevin, 121
 mobile devices, 243, 348
 modern computer network defense strategies, 196
 modern cryptosystems, 220
 AES, 221
 DES, 220
 RSA, 221
 3DES, 220–221
 modern hacking
 focused attacks, 100–101
 opportunistic attacks, 98–99
 semi-targeted attacks, 99–100
 modern malware concealment techniques, 203
 moles, 80
 money, motivation of spies, 81
 monitoring, CND environment, 201

Moonlight Maze, 143–145
 motivations of spies, 81
 MTBF. *See* mean time between failure

N

NAC. *See* network access control
 NASA. *See* National Aeronautics and Space Administration
 NAT. *See* network address translation
 nation-states, 28, 236
 National Aeronautics and Space Administration (NASA), 141
 National Geospatial-Intelligence Agency (NGA), 86
 National Institute of Standards and Technology (NIST), 295
 network security boundaries, 284*f*
 risk management process, 274*f*
 National Security Agency's Information Assurance Directorate (IAD), 186–188
National Security Strategy (2010), 15
 national sovereignty, 58
 NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), 57
 Naval Network Warfare Command, 43
 network access control (NAC), 280
 network address translation (NAT), 283
 network admissions control (NAC), 200
 network attacks, 343
 network-based DLP systems, 300
 network boundary, DLP at, 301*f*
 network-connected devices, 350
 network defense, 267–268
 active defense, 289–292
 defense technologies. *See* network defense technologies
 in depth, 178, 269–272
 integration of, 350
 mission assurance, 272–276
 security design, 276–278
 network defense technologies, 278
 and devices, 200–201
 IDSs, 285
 IPs, 285
 NAC, 280
 network security boundaries, 283–284
 physical network protection, 286–287
 protocols, 279
 Security Event and Information Management Systems, 286
 wireless network security, 287–289

network design, 349
 network-edge firewalls, 344
 network enclave admission process, 200f
 network enclaves and properties, 199–201
 network firewalls. *See* firewalls
 network flows, 202
 network management, 288–289
 network operational procedures, 275–276
 network protocols, 279
 network security boundaries, 283–284
 VLAN, 284
 network traffic monitoring, 201
 networks, continuous threats to systems and, 344f
 neutrality in kinetic warfare, 69–70
New York Times Co. v. United States, 161
 NGA. *See* National Geospatial-Intelligence Agency
 NGOs. *See* nongovernmental organizations
 9/11 attacks, 65, 66
 NIPRNet. *See* SBU IP Data
 NIST. *See* National Institute of Standards
 and Technology
 NIST Risk Management Framework (RMF), 273
 non-cyberwar attackers, 241
 nongovernmental organizations (NGOs), 159
 cyberwar. *See* cyberwar, NGOs in
 nonstate actors, 159
 nonkinetic warfare, 53
 nonrepudiation, 182, 210, 218
 nonstate actors, 7
 corporations, 160
 individuals and media, 161–162
 NGOs, 159
 organized crime, 160
 and responsibility, 61
 right of self-defense against, 65
 roles of, cyberwar in
 critics, 164–165
 participants, 164
 targets, 163
 terrorists and activists, 161
 nontraditional cyberwarfare targets, 36
 industrial espionage, 38–40
 military cyberattacks, 40–41
 political activism and hacktivism, 37–38
 nuclear intelligence, 87

O

Obama, Barack, 15–16
 objective, principles of war, 319
 objective territorial jurisdiction, 59

offensive cryptography
 Cryptolocker, 234–235
 Zeus, 232–234
 offensive cyberwarfare, supporting, 88
 offensive information operations, 15
 offensive, principles of war, 320
 Omega, 37
 one-time passwords, 192
 ongoing awareness programs, 134
 Open Source Center (OSC), 85
 open source intelligence (OSINT), 84–85
 OpenSSL encryption package, 271
 Operation Aurora, 151–152
 Operation Bodyguard, 21
 Operation Buckshot Yankee, 254
 Operation Ultra, 21
 operational level of warfare, 323
 operations security (OPSEC), 20, 21f
 opportunistic attack, 98–99
 OPSEC. *See* operations security
 optical media, 311
 organ (of a nation-state), 61
 organization procedures for endpoint defense in depth,
 255–256, 255f
 organizational authority, 126
 organized crime
 nonstate actors, 160
 ransomware, 167, 168f
 in Romania, crime cyberspace activities, 168
 OSC. *See* Open Source Center
 OSINT. *See* open source intelligence
 overhead imagery, 85

P

packet filter firewalls, 280
 Panda Security, 344
 patch management, 257
 PBS *Frontline* investigation, 143
 penetration testing, 135, 265
Pentagon Papers, 161
 People's Liberation Army (PLA), 148
 Percy, Hugh, 8
 perseverance, principles of war, 321
 phishing, tools of social engineer, 131–132, 131f
 “phone home” capabilities, 276
 physical network design, 278
 physical network protection, 286–287
 physical security, 254
 designs, 204–205
 physical separation, 284

PIRs. *See* priority intelligence requirements
 pivot, 192
 PKI. *See* public key algorithms
 PLA. *See* People's Liberation Army
 plaintext, 211
 Planning and Direction phase of intelligence, 76–77
 PLCs. *See* programmable logic controllers
 Poison Ivy, 149
 policy, 254–255, 255*f*
 political activism, 37–38
 port scanning tests systems, 264
 Powell, Colin, 86, 86*f*
 power, symbols of, 126–127
 POWs. *See* prisoners of war
 pretexting, tools of social engineer, 129–130
 Principles of Joint Operations, 321
 priority intelligence requirements (PIRs), 76
 prisoners of war (POWs), 81
 Processing and Exploitation phase, 77–78
 programmable logic controllers (PLCs), 245–246
 proprietary networks, 270
 proxies and gateways, 201
 PSS. *See* Public Safety Sensitive
 psychological operations (PSYOPs), 19–20, 28, 120
 public key algorithms, 215
 public key encryption, 216
 public key infrastructure (PKI), 185, 224, 226
 Public Safety Sensitive (PSS), 297

Q

quantum cryptography, 237
 Quantum program, 90–91

R

radar intelligence (RADINT), 87
 rainbow tables, 195, 223
 ransomware, 167
 RAT. *See* remote access trojan
 RC-135 Rivet Joint aircraft, 84, 84*f*
 real-time operating system (RTOS), 245
 reciprocity, 122–123
 Reconnaissance phase, 108, 109, 120
 Red Cell, 265
 red team, 265
 redacting, 296
 redundancy, 307
 refresher training, 134
 registration authority (RA), 224
 related key attacks, 227
 remote access systems, 283

remote access trojan (RAT), 111, 112
 remote platforms, 246–247
 remote telemetry units, 244
 responsibility, cyberwarfare law, 60–61
 restraint, principles of war, 321
 right of self-defense, against nonstate actors, 65
 risks, defined, 199
 “Robin Sage” operation, 135–136
 Romania, cybercrime activities, 168
 routers, 282, 283
 RSA, 221, 229
 RTOS. *See* real-time operating system
 rulesets, 280
 ruse, 69

S

salting, 223
 sanitizing, 296
 SANS critical controls, 188*t*
 SANS NetWars CyberCity environment, 351
 Saudi Arabian ARAMCO, 39–41
 SBU. *See* Sensitive But Unclassified
 SBU IP Data, 277
 SCADA systems. *See* supervisory control and data acquisition systems
 Scampi Systems, 119
 scarcity principle, 128–129
 Schwartz, Winn, 141
 SCI. *See* sensitive compartmented information
 script kiddies, 95
 SEA. *See* Syrian Electronic Army
 sea domain of warfare, 13
 Secret IP Data, 277
 secure networks, 199–205
 Secure Sockets Layer (SSL), 279
 secure Web traffic (SSL/TLS), 202
 Security Event and Information Management Systems, 286
 Security Event Managers (SEMs), 286
 Security Information and Event Management (SIEM) systems, 201, 286
 Security Information Monitors (SIMs), 286
 security, principles of war, 320
 self-defending hosts, 197
 self-defending networks, 197, 289, 290, 352
 self-defense, 65–66
 semi-targeted attack, 99–100
 SEMs. *See* Security Event Managers
 Senior Suter program, 149–150
 Sensitive But Unclassified (SBU), 296

sensitive compartmented information (SCI), 277

Sensitive Security Information (SSI), 296

Serbia, U.S. cyberwar strike, 36

SET. *See* Social-Engineer Toolkit

severity, measuring force, 63

SHA, 222

Shamoon malware, 39–41

side-channel attacks, 260

SIEM. *See* Security Information and Event Management

Siemens Simatic S7-300 PLC's firmware, 251

signals intelligence (SIGINT), 83–84

signature-based detection, 259, 285

signature-based systems, 203

simplicity, principles of war, 320

SIMs. *See* Security Information Monitors

simulations, 265

single unit retrieval format (SURF), 324

SIPRNet. *See* Secret IP Data

688th Cyberspace Wing, 43

67th Network Warfare Wing, 43

Skype, cyberattacks, 145

Snowden, Edward, 6, 17, 74, 89, 161, 164, 174, 175, 193, 276

social authority, 126

Social-Engineer Toolkit (SET), 132, 132f

social engineering, 117, 120, 228

- case study in, 135–136
- defending against, 133
 - content filtering, 134–135
 - incident reporting and response, 134
 - penetration testing, 135
 - security awareness and education, 133–134

social engineers, 117, 118

- commitment and consistency, principle of, 124
- tools of
 - baiting attack, 133
 - phishing, 131–132, 131f
 - pretexting, 129–130

social media, impact of, 32

social proof, 125

software and application logs, 201

software-defined network, 197

software improvements, advantage of, 187

software testing, 264

Solar Sunrise, 141–143

solid state drives (SSDs), 311

sovereignty, 58

space domain of warfare, 13

spear phishing attack, 131

spies, motivations of, 81

SQL Slammer, 147

SSDs. *See* solid state drives

SSI. *See* Sensitive Security Information

SSL. *See* Secure Sockets Layer

Stakkato, 148–149

star fort, 180, 181f

stateful packet inspection firewalls, 281

steganalysis tools, 219

steganography, 219

strategic level of warfare, 323

strategic web compromises, 105

Stuxnet, 8, 55, 140, 150–151, 194, 195, 240, 243, 269

subjective territorial jurisdiction, 59

substitution cipher, 215

supervisory control and data acquisition (SCADA) systems, 244, 244f, 246

supply chain targets, conventional warfare, 29

SURF. *See* single unit retrieval format

surprise, principles of war, 320

switches, 282–283

Symantec antivirus, 259

symmetric ciphers, 212–213, 214f

- Enigma device, 213–215
- scaling, 212t, 213

Syrian Electronic Army (SEA), 32, 38, 38f, 104, 171–172

system monitoring, 201

T

tactical level of warfare, 323

Tailored Access Organization (TAO), 18

Taliban Web site, 32

Tallinn Manual on the International Law Applicable to Cyber Warfare, 30, 57, 63, 68

TAO. *See* Tailored Access Organization

tapes, 311

targets

- and combatants
 - cyberwarfare targets. *See* cyberwarfare targets
 - traditional military targets. *See* military targets
 - U.S. cyberwar doctrine, 25
- prohibited, 67–68

TC/SCI IP Data, 277

technical network defenses, 200

telephone metadata, 89

terrorists, 161
 anonymous, 172–173
 Estonia, 171
 SEA, 171–172
 testing, 264–265
 The Jester, 45–46, 46f
 The Onion Router (TOR), 288
 Th3j35ter. *See* The Jester
 Thomas Ryan of Provide Security, 135
 threat analysis, 22
 threats, 199
 of force, 65
 tiger teams, 265
 Titan Rain, 148
 titles, symbols of power, 126
 TLS. *See* Transport Layer Security
 TOR. *See* The Onion Router
 total cyberwarfare, 33
 total warfare, 28
 TPM chip. *See* Trusted Platform Module chip
 TRACFIN, 90
 traditional information security operations, 177
 traditional warfare, 322
 vs. guerrilla warfare and cyberwarfare, 47–49, 48t
 traitors, 80
 Transport Layer Security (TLS), 224,
 226, 279
 trappings of power, 127
 treachery, 69
 Triple DES (3DES), 220–221
 trusted administrator's system, 193f
 Trusted Platform Module (TPM) chip, 260
 Twitter, 32, 38, 67, 171, 336
 two-factor authentication software, 192

U

U-2 Dragon Lady aircraft, 85, 86f
 UK GCHQ. *See* United Kingdom Government
 Communications Headquarters
 unconventional warfare, 28
 United Kingdom Government Communications
 Headquarters (UK GCHQ), 288
 United Nations Charter and foundational
 documents, 54
 United Nations Security Council, 86, 86f
 United States Director of National Intelligence
 (DNI), 5
 unity of command, principles of war, 320
 university computer systems, 142
 update management, 257

U.S. Air Force
 Air Forces Cyber, 43
 Computer Emergency Response Team
 (AFCERT), 141
 cyberattack on Assignments Management
 System, 324
 and IMINT, 85, 86f
 and SIGINT, 84f
 Solar Sunrise attacks, 141
 U.S. Army
 Army Field Manual, 19
 Cyber Command, 43
 Intelligence and Security Command, 43
 US-CERT's defense-in-depth strategy, 181f
 U.S. Computer Emergency Readiness Team, 180
 U.S. Cyber Command (USCYBERCOM), 14, 42–43,
 42f, 327, 329–330
 U.S. Cyberspace Policy Review, 346, 347
 U.S. cyberwar strike, Serbia and Kosovo, 36
 U.S. Defense Advanced Research Projects Agency
 (DARPA), 349
 U.S. Defense Information Systems Agency (DISA), 277
 U.S. Department of Defense (DoD), 13, 189, 199, 225,
 267, 271, 293, 327, 329
 Information Assurance Support Environment, 309
 Information Enterprise strategic plan, 304
 strategy, 252–253
 U.S. Marine Corps, 13
 Cyberspace Command, 43
 U.S. military, 19
 basic data life cycle, 308, 308f
 U.S. National Security Agency (NSA), 6, 12, 83, 161,
 167, 189, 220, 229, 256, 268, 271, 287,
 296, 299, 326
 in-depth strategy, 272, 272f
 strategies, mapping, 188t
 weaponizing cyberspace, 147
 U.S. Navy
 bombe machine, 11, 11f
 Cyber Defense Operations Command, 43
 Naval Network Warfare Command, 43
 U.S. Space Command (USSPACECOM), 189
 U.S. Strategic Command (USSTRATCOM), 329
 USB thumb drives, 311
 USCYBERCOM. *See* U.S. Cyber Command
 use of force, 63, 64f
 measuring force, 63–64
 threats of force, 65
 user- and system-contextual awareness, 197
 USSTRATCOM. *See* U.S. Strategic Command

V

virtual LAN (VLAN), 200, 284
 virtual private networks (VPNs), 119, 152, 200, 201, 225, 226, 289
 virtualization, 307
 VLAN. *See* virtual LAN
 VLAN hopping attacks, 284
 VPNs. *See* virtual private networks
 vulnerabilities, 343
 vulnerability analysis, 22
 vulnerability scanning, 265

W

WANs. *See* wide area networks
 war games, 265
 war, principles of, 319–321
 warfare
 domains of, 13–14, 14*f*
 forms of, 322–323
 levels of, 323, 325, 325*f*
 types of, 28
 watering hole attacks, 105
 Weaponize phase of Cyber Kill Chain, 108–109
 weaponizing cryptography
 defensive cryptography, 231–232
 offensive cryptography, 232–235
 weaponizing cyberspace, 139–140
 1990s, early attacks, 141
 Honker Union, 145
 Moonlight Maze, 143–145
 Solar Sunrise, 141–143
 Stuxnet and twenty-first century, 150–151
 Careto, 154
 Duqu, 152, 153*f*
 Flame, 152–153
 FOXACID, 153
 Operation Aurora, 151–152

2000s, worm turns, 145
 Code Red, 146–147
 Poison Ivy, 149
 Senior Suter, 149–150
 SQL Slammer, 147
 Stakkato, 148–149
 Titan Rain, 148
 weapons of mass destruction (WMD), 12
 weapons systems, 247
 Web content filtering, 135
 Web Domain Name System (DNS)
 reputation, 187
 Web site, 303
 Web traffic, 300
 whaling attacks, 131
 whistleblowers, 174–175
 white box penetration testing, 265
 white-hat hackers, 174
 whitelisting, 261–263, 262*f*
 capabilities, 203
 wide area networks (WANs), 270
 window of vulnerability, 104
 wireless access points, 283
 wireless network security, 287
 remote access and administration, 288–289
 WMD. *See* weapons of mass destruction
 workstation-to-workstation
 communications, 186
 World of Warcraft (WoW),
 steganography, 219
 World War II, 10–11
 worm (malicious code), 146
 WoW. *See* World of Warcraft

Z

zero-day attacks, 104
 zero-day vulnerabilities, 17, 187
 Zeus Trojan, 232–234, 234*f*