

Index

Note: Page numbers followed by *b* indicate boxes, *f* indicate figures and *t* indicate tables.

A

Academia and Industry
 associations, 77–78
AccessData Certified Examiner
 (ACE), 241–242
Active threats, 45–46
Act of war
 cyberspace, 227
 and use of force, 222
Advanced Persistent Threat (APT),
 28, 175–176
Air Force approach, 167–168
Air Operation Center (AOC),
 40–41
American Registry for Internet
 Numbers (ARIN),
 107, 108
APT. *See* Advanced Persistent
 Threat (APT)
Army doctrine
 documentation plan, 162
 elicitation, 164
 emotional approach, 164
 false flag, 165
 file/dossier, 164
 general access attacks, 157–158
 good/bad cop, 164
 HUMINT collector, 162
 integrated approaches, 163, 163*f*
 targeted access attacks, 158–159
 witness statements, 164
 World War II, 163
Assault, attack process
 actual cyber warfare, 189
 computer system, 190*b*
 deception, 189
 degradation, 190
 denial attacks, 190
 destruction, 190
 and Ds activities, 189, 189*f*
 internal manipulation, 189
 panic and disruption, 189–190
 VoIP, 189

Assault tools
 attacking hardware, 130–131
 defense, 131
 description, 128
 software, 129
 system environment, 129–130
 system resources, 129
Attackers and sponsors, 171
Attack methodology
 botnet armies, 26
 cracking passwords, 26–27
 and DMZ, 21
 exploit phase, 27
 framework tools, 26
 kinetic and non-kinetic warfare,
 21–24
 malcode, 25
 mapping sample, 24–27
 recon phase, 25
 rootkit program, 25
 and SE, 27
 sniffer, 25
 vulnerability, 25
Attack process, CNA
 access, 186–187
 assault, 189–190
 description, 184–185, 184*f*
 different location, 185
 different phases, 192
 escalation, 187–188
 exfiltration, 188
 obfuscation, 191
 privilege escalation, 184–185
 reconnaissance, 185
 scanning, 186
 sustainment, 190–191
Attribution, 247, 268
Auditing, 196, 197, 261, 271
Authentication, 196–197
Authorization, 196–197
Autonomous actors
 attack systems, 216–217
 cyber activities, 219

cyber warfare, 215
defensive systems, 218
exploratory systems, 216
Intrusion Prevention Systems
 (IPSs), 215
malware, 215

B

Battle Damage Assessment (BDA),
 72
Blackhat hacker, 210
Black Swan event, 277, 278

C

CACs. *See* Common Access Cards
 (CACs)
CAE. *See* Center of Academic
 Excellence (CAE)
CALEA. *See* Communications
 Assistance to Law Enforcement
 Act (CALEA)
Canadian Cyber Incident Response
 Center (CCIRC), 94
Canadian Security Intelligence
 Service (CSISS), 94
Capability surprise, 278
CAS. *See* Close Air Support (CAS)
CATS. *See* Center for Asymmetric
 Threat Studies (CATS)
CCIRC. *See* Canadian Cyber Incident
 Response Center (CCIRC)
Center for Asymmetric Threat
 Studies (CATS), 64
Center for Strategic and
 International Studies (CSIS), 64
Center of Academic Excellence
 (CAE), 86
Certified Computer Crime
 Investigator (CCCI), 241–242
Certified Computer Examiner
 (CCE), 241–242
Certified Digital Forensic Examiner
 (CDFE), 241–242

- Certified Digital Media Collector (CDMC), 241–242
- Certified Electronic Evidence Collection Specialist Certification (CEECS), 241–242
- Certified Forensic Computer examiner (CFCE), 241–242
- Certified Information Systems Security Professional (CISSP®), 84
- Chief Financial Officer (CFO), 38–39
- Chief Information Officer (CIO) and FUD, 39
- security investment, 38–39
- Chinese doctrine, 65–67
- CIA. *See* Confidentiality, Integrity and Availability (CIA)
- CIKR. *See* Critical infrastructure and key resources (CIKR)
- CIO. *See* Chief Information Officer (CIO)
- CIP. *See* Critical Infrastructure Protection (CIP)
- CISSP®. *See* Certified Information Systems Security Professional (CISSP®)
- Client-side attack, 186–187
- Close Air Support (CAS), 72
- Cloud computing, 283, 284–285
- CNA. *See* Computer Network Attack (CNA)
- CNCI. *See* Comprehensive National Cybersecurity Initiative (CNCI)
- CNE. *See* Computer Network Exploitation (CNE)
- CNO. *See* Computer Network Operations (CNO)
- COBIT. *See* Control Objectives for Information and Related Technology (COBIT)
- Collateral damage, 253
- Commercial-off-the-shelf (COTS), 262, 287
- Common Access Cards (CACs), 186
- Communications Assistance to Law Enforcement Act (CALEA), 239
- Communications Security Establishment Canada (CSEC), 94
- Comprehensive National Cybersecurity Initiative (CNCI), 73
- Computer Emergency Readiness Team (CERT), 287
- Computer Emergency Response Team (CERT), 31
- Computer Network Attack (CNA) attack process (*see* Attack process, CNA)
- blackhat hackers, 181
- conventional attack, 181–182
- cyber era (*see* Waging war, cyber era)
- definition, 181
- individual attackers, 181
- random hackers, 181–182
- reactive and proactive actions, 191
- strategies and tactics, 192
- Computer Network Defense (CND) authentication, authorization and auditing, 196–197
- availability, 196
- and CIA, 204
- confidentiality, 195
- conventional warfare, 193
- cyber attacks (*see* Cyber attacks)
- data mining and pattern matching, 205
- definition, 193
- individual states, 194–195
- information, 194
- integrity, 195–196
- military leadership, 193
- pure cyber attack sense and non-nation-state, 194
- security awareness and training, 198–200
- Computer Network Exploitation (CNE) description, 169
- intelligence and CI, 170–171
- intelligence gathering activities, 169
- reconnaissance (*see* Reconnaissance process)
- sensitive information, 169
- surveillance, 174–178
- Computer Network Operations (CNO), 184, 267
- Confidentiality, integrity and availability (CIA), 189, 195–196
- Continuation of Operations Planning (COOP), 261–262
- Control Objectives for Information and related Technology (COBIT), 238, 261
- COOP. *See* Continuation of Operations Planning (COOP)
- Corporations, non-state actors
- cyber criminal, 207–208
- cyber warfare, 212, 218
- regular criminal activities, 211–212
- technical industry, 211
- COTS. *See* Commercial-off-the-shelf (COTS)
- Counterinsurgency (COIN), 72–73
- Counterintelligence (CI) army regulation, 167
- attackers and sponsors, 171
- cyber CI, 165
- cybersecurity, 166
- information gathered and activities, 165
- internal traps, 166–167
- sources, cyber attacks, 170–171
- tactical level actions, 165–166
- the U.S. strategy, 166, 166f
- Covert activity
- attack, physical access controls, 150
- eavesdropping, electromagnetic emissions, 149–150
- vandalism/denial of service, 150
- Crime Scene Investigation (CSI), 240
- Criminal law
- civil and tribunal laws, 233
- electronic discovery, 234–235
- evidence, 233
- subpoena, 233
- Criminal organizations
- attackers, 214–215
- cyber operations, 208
- identities, 215
- motivations, 215
- Critical infrastructure and key resources (CIKR), 14–15
- Critical Infrastructure Protection (CIP), 283
- CSEC. *See* Communications Security Establishment Canada (CSEC)
- CSI. *See* Crime Scene Investigation (CSI)
- CSIS. *See* Center for Strategic and International Studies (CSIS)
- CSISS. *See* Canadian Security Intelligence Service (CSISS)
- CSOC. *See* Cyber Security Operations Centre (CSOC)
- Cyber attacks
- defense in depth, 203–204
- and DRP, 203

- environments and monitoring, 200
- intrusion detection and prevention, 201–202
- policy and compliance, 200–201 and SCADA, 200
- sources, 170–171
- surveillance, data mining and pattern matching, 201
- vulnerability assessment and penetration testing, 202–203
- Cyber Command (CYBERCOM), 10, 91, 287
- Cybercrime, 1, 2
- Cyber doctrine
 - guidance and directives, 73–78
 - operations and exercises, 78–80
 - sample doctrine, 63–70
 - and TTPs, 70–73
 - the U.S. military, 53–63
- Cybersecurity challenges
 - audits, 271
 - deterrence, 271
 - insider threat, 272
 - issues, 272
 - military ROE, 271
 - mobile devices, 271
 - situational awareness, 272
 - stovepipes, 272
- Cybersecurity issues
 - categorization and relationships, challenges, 259, 259f
 - challenges, complexity level, 258
 - core, 268–271
 - organization, 267–268
 - people, 266–267
 - policy, 260
 - processes, 260–261
 - Senior System Security Engineer, 258
 - significants, 258–259
 - skills, 265–266
 - technical, 261–265
- Cyber Security Operations Centre (CSOC), 94, 95
- Cyberspace battlefield
 - cyber warfare, 35–41
 - fielding systems, 49–51
 - war-fighting domains, 41–45
- Cyberspace challenges
 - computer network operations, 257–258
 - concise review and taxonomy, 258
 - the CTO's office CyberAssure™ program, 257
 - cybersecurity challenges (see Cybersecurity challenges)
 - cybersecurity issues (see Cybersecurity issues)
 - DARPA, 273
 - DHS, 273
 - DoD, 273
 - DoE, 273
 - DoJ, 273
 - DoS, 273
 - national and international debate, 274
 - NIST, 273
 - significant effort, 273–274
 - technical issues, 273
 - the U.S. Congress, 257, 272
- Cyber timeline, 291–295
- Cyber threatscape
 - ARPANET, 19
 - attackers, 27–30
 - attack methodology, 21–27
 - and CIP, 33
 - corporate assets, 33
 - defenders and attackers, network, 20–21
 - defense-in-depth, 30–33
 - designed map, 21, 22f
 - DoD, 19–20
 - F-35 Joint Strike Fighter program, 20
 - hackers, 20
 - targeted capabilities, 33
- Cyber time, 280
- Cyber warfare
 - America's information dominance tools, 3
 - art of war, 4
 - battlefront, 1
 - biometric and nanotechnology, 285
 - the Black Swan, 277
 - Buckshot Yankee, 11
 - capability surprise, 278
 - China, 13
 - CIKR and DHS, 14–15
 - CIP/SCADA vulnerabilities, 284
 - and CNN, 281
 - code word programs, 11–12
 - cold war, 16
 - constant headlines, 1
 - corporate networks and cloud computing, 284–285
 - and COTS, 287
 - countries and non-nation state actors, 280–281
 - criminal acts, 10–11
 - critical infrastructure, cyber attacks, 14–15, 15f, 280
 - the Cuckoo's Egg, 1–2
 - cyber arms control, 7–9
 - cyber conflicts, 287
 - cybercrime, 283–284
 - Cyber Pearl Harbor and 9/11 attacks, 281
 - cyberspace, electronics and electromagnetic spectrum, 4
 - cyber strategy and power, 6–7
 - cyber surprise framework, management, 278–279, 279t
 - and DARPA, 287
 - debate, 13–14
 - description, 288
 - and DHS, 287
 - and DIME, 281
 - and DoD, 3–4, 3f, 15
 - economic issues, 13
 - Eligible Receiver, 11
 - Estonian government, 12
 - the Fugitive Game, 1–2
 - Georgia, 12
 - Google, 13
 - Internet, 4, 16
 - "Israeli Elite Strike Force", 12–13
 - Kaspersky Lab, 282
 - Law Enforcement Agencies, 285
 - long-term evolution and sudden paradigm shifts, 277
 - Moonlight Maze, 11
 - Morris worm, 280
 - national leadership, the U.S., 2
 - national level leaders, 286
 - National Military Strategy for Cyberspace Operations, 3
 - and NATO, 12
 - natural evolutionary trends, 282–283
 - and NICCS, 287
 - NORTHCOM and CYBERCOM, 287
 - and NSA, 281
 - Operation Aurora, 13
 - "Operation Israel", 12–13
 - physical infrastructure, 280
 - principles, 278
 - pro-Palestinian attack tool, 12–13

Cyber warfare (*Continued*)
 Revolution in Military Affairs (RMA), 279
 and SCADA, 280
 “social networking” activities, 284
 Solar Sunrise, 11
Swordfish 2001, 2
 tactical and operational reasons, 4–6
 at 4th annual homeland security conference, 286
 Titan Rain, 11
 traditional method, 15
 United Nations (UN), 4
 the United States, 9–10
 World War II, 15–16
 Cyber warfare forces
 Australia, 94
 Brazil, 93
 Canada, 94
 China, 91–92
 corporation, 95–96
 countries, 95
 criminal, 96
 cyber warfare arena, 90, 91f
 France, 92–93
 Israel, 93
 Japan, 94
 Malaysia, 94
 North Korea, 93–94
 organizations, 90
 Russia, 92
 Singapore, 93
 South Korea, 93
 United Kingdom, 95
 the United States, 91
 Cyber warrior
 certifications, 84–85
 cyber operations, 83
 cyber warfare forces (*see* Cyber warfare forces)
 education, 85–86
 experience and skills, 86–87
 next generation, 101
 staff, cyber warfare (*see* Staff, cyber warfare)
 traditional fighting forces (*see* Traditional fighting forces)
 training, 86

D

Dangerous threats, 46–48
 DARPA. *See* Defense Advanced Research Projects Agency (DARPA)

DCID. *See* Director of Central Intelligence Directive (DCID)
 DCMA. *See* Digital Millennium Copyright Act (DCMA)
 DDoS. *See* Distributed Denial of Service (DDoS)
 Deception, 189
 Defense Advanced Research Projects Agency (DARPA), 37, 287
 Defense-in-depth
 “Annualized Loss Expectancy”, 32
 cloud computing, 37
 compliance, 32
 configuration management, 31
 cyber attacks, 203–204
 DARPA, 37
 description, 30–31
 Internet Service Provider (ISP), 36–37
 management, identity, 31–32
 risk management, 32
 SOC and CERT, 31
 the Twitter Revolution, 37
 types, metrics, 30–31
 users types, 32–33
 Defense Information Systems Agency (DISA), 91
 “Defense Reform 2020”, 68
 Defense Security Command (DSC), 67–68
 Defense Signals Directorate (DSD), 94
 Defensive skill, 86, 87
 Degradation, 190
 Demilitarized Zone (DMZ), 21
 Democratic People’s Republic of Korea (DPRK), 93–94
 Denial attack, 190
 Denial of Service (DoS), 190
 Department of Defense (DoD)
 cyberspace, 3–4, 55
 and INFOCONs (*see* Information Operations Condition (INFOCON))
 MESL events, 79–80
 and POM, 55–56
 Titan Rain, 11
 Department of Homeland Security (DHS), 10, 73–75, 287
 Destruction, 190
 Deterrence, 268–269, 271
 Development Centers and Defense Advanced Research Projects Agency (DARPA), 273

DHCP. *See* Dynamic Host Configuration Protocol (DHCP)
 DHS. *See* Department of Homeland Security (DHS)
 DIACAP. *See* DOD Information Assurance Certification and Accreditation Process (DIACAP)
 Digital forensics
 certification, 241–242
 computer devices and networks, 239–240
 computer forensics, 241
 Computer Network Defense, 239–240
 court of law, 240–241
 cryptographic hash, 241
 and CSI, 240
 physical forensics, 240
 standard template, 241
 systematic gathering and analysis, 239–240
 tools, 241
 Digital Millennium Copyright Act (DCMA), 236
 DIME. *See* Diplomatic, Information, Military and Economic (DIME)
 Diplomatic, Information, Military and Economic (DIME), 7, 281
 Director of Central Intelligence Directive (DCID), 261
 Director of the National Security Agency (DIRNSA), 91
 DIRNSA. *See* Director of the National Security Agency (DIRNSA)
 DISA. *See* Defense Information Systems Agency (DISA)
 Disaster Recovery Planning (DRP), 203
 Disruption, 189–190
 Distributed Denial of Service (DDoS)
 Australian senator, 211
 patriotic hackers, 211
 DMZ. *See* Demilitarized Zone (DMZ)
 DNS. *See* Domain Name Server (DNS)
 Doctrine, 260, 273
 DoD. *See* Department of Defense (DoD)
 DOD Information Assurance Certification and Accreditation Process (DIACAP), 261

Domain Name Server (DNS)
 defense, 112–113
 dig query, 109, 110*f*
 dnsenum, 109
 maltego, 111–112
 metadata (*see* Metadata)
 nslookup command, 108–109, 109*f*
 numerous tools, 108
 DoS. *See* Denial of Service (DoS)
 DPRK. *See* Democratic People's Republic of Korea (DPRK)
 DSD. *See* Defense Signals Directorate (DSD)
 Dynamic Host Configuration Protocol (DHCP), 126

E

Educational exercises, 80
 Electromagnetic attacks
 defense *vs.* conventional attacks, 147–148
 and EMP, 146–147
 jamming technologies, 147
 Electromagnetic pulse weapons (EMP), 146–147
 Electronic Communications Privacy Act (EPCA), 239
 Electronic discovery, 234–235
 Elicitation
 conventional collection techniques, 164
 definition, 159
 indirect approach, 164
 EMP. *See* Electromagnetic pulse weapons (EMP)
 EnCase Certified Examiner (ENCE), 84
 EPCA. *See* Electronic Communications Privacy Act (EPCA)
 Ethical hacking, 99–100
 Ethics
 collateral damage issues, 255
 cyber operations, 245
 cyber warfare (*see* Warfare, ethics)
 definition, 245
 Enron scandal, 245
 the Geneva and Hague conventions, 255
 governmental and civilian networks, 255
 hactivist attacks, 246
 intent, 255
 issue, cyber warfar, 255

 just war theory (*see* Just war theory)
 European Countries cyber doctrine, 68–70
 Exfiltration tools
 attack process, 188
 band methods, 126
 defense, 126–127
 description, 125
 encryption and steganography, 125
 physical, 125
 protocols, 126
 Extensible Markup Language Remote Procedure Call (XML-RPC), 120–121
 Extensible Messaging and Presence Protocol (XMPP), 188

F

FAA. *See* Federal Aviation Administration (FAA)
 Facility and equipment hardening process, 148–149
 FBI. *See* Federal Bureau of Investigation (FBI)
 Fear Uncertainty and Doubt (FUD), 39
 Federal Aviation Administration (FAA), 39
 Federal Bureau of Investigation (FBI), 39
 Federal exercises, 78–79
 Federal Information Security Management Act (FISMA), 237–238
 Federally Funded Research and Development Centers (FFRDCs), 212
 Fielding systems
 contract requirements, 50–51
 cyber attack weapons, 50
 IT acquisition process, 50
 security, 49–50
 File Transfer Protocol (FTP), 188, 190
 FISA. *See* Foreign Intelligence Surveillance Act (FISA)
 FISMA. *See* Federal Information Security Management Act (FISMA)
 Foreign Intelligence Surveillance Act (FISA), 237
 FTP. *See* File Transfer Protocol (FTP)
 FUD. *See* Fear Uncertainty and Doubt (FUD)

G

GCFA. *See* GIAC Certified Forensic Analyst (GCFA)
 General access attack, 157–158
 General Staff Department (GSD), 91–92
 Geospatial intelligence (GEOINT), 7
 GHDB. *See* The Google Hacking Database (GHDB)
 GIAC. *See* Global Information Assurance Certification (GIAC)
 GIAC Certified Forensic Analyst (GCFA), 241–242
 GIAC Certified Penetration Tester (GPEN), 84
 GIG. *See* Global Information Grid (GIG)
 GLB. *See* Gramm Leach Bliley Act (GLB)
 Global Information Assurance Certification (GIAC), 84
 Global Information Grid (GIG), 5
 Google hacking, 105–106
 The Google Hacking Database (GHDB), 106
 Government Off the Shelf (GOTS), 262
 GPEN. *See* GIAC Certified Penetration Tester (GPEN)
 Gramm Leach Bliley Act (GLB), 236
 GSD. *See* General Staff Department (GSD)

H

Hactivist, 29, 210–211
 Health Insurance Portability and Accountability Act (HIPAA), 239
 HIPAA. *See* Health Insurance Portability and Accountability Act (HIPAA)
 Homeland Security/Presidential Directives (HSPDs), 75–76
 HSPDs. *See* Homeland Security/Presidential Directives (HSPDs)
 HTTP. *See* Hypertext Transfer Protocol (HTTP)
 Human intelligence (HUMINT)
 behaviors, 162
 body language and personal representation, 162
 operators/interrogators, 162
 Hypertext Transfer Protocol (HTTP), 188

I

IACIS. *See* International Association for Computer Investigative Specialists (IACIS)
 ICANN. *See* The Internet Corporation for Assigned Names and Numbers (ICANN)
 ICS. *See* Industrial control system (ICS)
 Identity management (IDM), 264, 272
 IDF. *See* Israel Defense Force (IDF)
 IDS. *See* Intrusion Detection Systems (IDS)
 Imagery intelligence (IMINT), 7
 IMINT. *See* Imagery intelligence (IMINT)
 Immunity CANVAS, 123–124
 Individual actors
 attacks, 208
 blackhats, 210
 hacktivists, 210–211
 malware authors, 209
 non-state attackers, 208, 209*t*
 patriotic hackers, 211
 Personally Identifiable Information (PII), 208
 scammers, 209–210
 script kiddies, 208–209
 skill level, 208
 Industrial control system (ICS), 140
 Information Operations Condition (INFOCON), 62–63
 Information Security Management System (ISMS), 238
 Information Security Policy Council (ISPC), 94
 Information Systems Audit and Control Association (ISACA), 84, 238, 261
 Information Technology Infrastructure Library (ITIL), 238
 Infrastructure process, hardware and software, 148
 Insider threat, 29, 266, 270, 272
 Intelligence Preparation of the Operational Environment (IPOE), 70–71
 Intent, 247, 250–251
 International Association for Computer Investigative Specialists (IACIS), 241–242

International law
 disciplines, 230
 maritime law, 231–232
 and NATO, 231
 space law, 232
 the United Nations, 231
 International Trafficking in Arms Regulations (ITAR), 235
 The Internet Corporation for Assigned Names and Numbers (ICANN), 263–264
 Intrusion detection and prevention, 201–202
 Intrusion Detection Systems (IDS), 184, 265
 Intrusion Protection Systems (IPS), 265
 Intrusion Response System (IRS), 218
 IPOE. *See* Intelligence Preparation of the Operational Environment (IPOE)
 IPS. *See* Intrusion Protection Systems (IPS)
 IRS. *See* Intrusion Response System (IRS)
 ISACA. *See* Information Systems Audit and Control Association (ISACA)
 ISMS. *See* Information Security Management System (ISMS)
 ISPC. *See* Information Security Policy Council (ISPC)
 Israel Defense Force (IDF), 93
 ITAR. *See* International Trafficking in Arms Regulations (ITAR)
 ITIL. *See* Information Technology Infrastructure Library (ITIL)

J
 Jamming technologies, 147
 JMEM. *See* Joint Munitions Effectiveness Manual (JMEM)
 JOAC. *See* Joint Operational Access Concept (JOAC)
 Joint doctrine
 and CO, 57
 doctrinal library, 58
 and JOAC, 58
 Joint Pub 1 Doctrine, 57
 and multinational integration of forces, 56–57
 Joint Munitions Effectiveness Manual (JMEM), 71
 Joint Operational Access Concept (JOAC), 58

Justice after war
 extract reparations, 254–255
 hold morally culpable individuals accountable, 254
 principles, 254
 seek a lasting peace, 254
 Just war theory
 cyber warfare, 248
 Immanuel Kant, 248–249
 justice after war (*see* Justice after war)
 principles, 249
 proper conduct in war (*see* Proper conduct in war)
 the right to wage war (*see* The right to wage war)

K

KIICA. *See* Korea IT International Cooperation Agency (KIICA)
 Korea Information Security Agency (KISA), 93
 Korea IT International Cooperation Agency (KIICA), 93

L

Law enforcement agencies (LEAs)
 certifications, 241–242
 evidence, 233
 the United States act of war, 222
 Law of armed conflict
 definition, 247
 development, 248
 the Geneva Conventions, 248
 Hague Convention, 248
 just war theory, 248
 the right to wage war, 248
 Law of Armed Conflict (LOAC)
 conflict and customary international law, 227
 international armed conflicts, 221
 principles, 227
 the United Nations (UN) Charter, 227
 LEAs. *See* Law enforcement agencies (LEAs)
 Legal systems
 act of war, 227
 “armed attack”, 242
 civil law, 230–231
 common law, 230–231
 conflicts/wars categories, 221
 Congress, 226
 congressional statutes, 239

criminal law, 233–235
 cyber operations, 223
 cyberspace, 224, 226
 cyber war, 221
 “cyber weapon”, 227
 the Department of Defense
 Cyberspace Policy Report,
 224–228
 deterrence/effective retaliation,
 225
 digital forensics (*see* Digital
 forensics)
 and DoD, 226
 enact laws, 231
 and EPCA, 239
 escalation, cyberwarfare, 225
 foundational principles,
 geography, 231
 and HIPAA, 239
 “humane war”, 221
 intelligence-gathering function,
 226
 International Group of Experts,
 222–223
 international law
 (*see* International law)
 Internet and typical transaction,
 230
 Koh’s statement, 229
 Legal Adviser, 228–229
 and LOAC, 221
 NATO Cooperative Cyber
 Defence Centre of Excellence,
 222
 Nuisance Law, 229–230
 President’s freedom, the United
 States, 224
 the Principle of Neutrality, 230
 privacy rights, 239
 public and commercial networks,
 229
 religious law, 230–231
 sharia and *halakha*, 230–231
 third-party sovereignty, 227
 the United States laws (*see* The
 United States laws)
 use of force, 222, 228
 LOAC. *See* Law of Armed Conflict
 (LOAC)
 Locks. *See* Tackling locks
 Logical attack systems
 physical effects, 139–140
 physical hardware, 138–139
 Logical weapons
 assault tools (*see* Assault tools)

broad categories, tools, 104
 commercial tools, 104
 compromised system, 135
 cyber warfare, 103–104
 damage and disrupt systems, 135
 defense, 124
 deleterious effects, 103
 description, 103
 and DNS (*see* Domain Name
 Server (DNS))
 escalation tools, 135
 exfiltration tools (*see* Exfiltration
 tools)
 immunity CANVAS, 123–124
 the Metasploit Project (*see* The
 Metasploit Project)
 military weapons, 104
 nation-states, 135
 obfuscation tools (*see* Obfuscation
 tools)
 password tools, 119–120
 reconnaissance tools
 (*see* Reconnaissance tools)
 scanning tools (*see* Scanning tools)
 sustainment tools
 (*see* Sustainment tools)
 U.S. Air Force, 103

M

MAD. *See* Mutually Assured
 Destruction (MAD)
 Malaysian Administrative
 Modernisation and
 Management Planning Unit
 (MAMPU), 94
 Malaysian Communications and
 Multimedia Commission
 (MCMC), 94
 Maltego, 111–112
 Malware, 209, 216–217
 MAMPU. *See* Malaysian
 Administrative Modernisation
 and Management Planning
 Unit (MAMPU)
 MASINT. *See* Measurement and
 signature intelligence
 (MASINT)
 MCMC. *See* Malaysian
 Communications and
 Multimedia Commission
 (MCMC)
 Measurement and signature
 intelligence (MASINT), 7
 Measures of Effectiveness (MOEs),
 72

MESL. *See* Mission Event
 Synchronization List (MESL)
 Metadata
 exiftool, 110–111
 file size, 109–110
 metagoofil, 110, 111f
 strings, 111
 The Metasploit Project
 description, 120
 Express and Metasploit Pro,
 121–123
 framework, 120–121
 Military information support
 operations (MISO), 155
 Ministry of National Defense
 (MND), 67–68
 Ministry of Science, Technology and
 Innovation (MOSTI), 94
 MISO. *See* Military information
 support operations (MISO)
 Mission assurance, 260–261
 Mission Event Synchronization List
 (MESL), 80
 MND. *See* Ministry of National
 Defense (MND)
 MOEs. *See* Measures of Effectiveness
 (MOEs)
 MOSTI. *See* Ministry of Science,
 Technology and Innovation
 (MOSTI)
 Motivations, hackers, 48–49
 Mutually Assured Destruction
 (MAD), 271

N

National Information Security
 Center (NISC), 67–68, 94
 National Initiative for Cybersecurity
 Careers and Studies (NICCS),
 287
 National Initiative for Cybersecurity
 Education (NICE), 267, 287
 National Institute of Standards and
 Technology (NIST), 76–77, 236,
 237–238
 National Internet Development
 Agency of Korea (NIDAK), 93
 National Security Agency (NSA), 86,
 104, 281, 282–283
 Nation-based law, 230
 NATO. *See* North American Treaty
 Organization (NATO)
 Nessus
 classification, 115–116
 complexity, 116

Nessus (*Continued*)
 and NASL, 118
 and nmap, 115
 OpenVAS, 118
 port scan results, 116, 117f
 SCADA plugins, 115–116, 116f
 scan in progress, 116, 116f
 scanning tool, 115
 vulnerability listing, 116–118, 117f
 NICCS. *See* National Initiative for Cybersecurity Careers and Studies (NICCS)
 NICE. *See* National Initiative for Cybersecurity Education (NICE)
 NIDAK. *See* National Internet Development Agency of Korea (NIDAK)
 NISC. *See* National Information Security Center (NISC)
 NIST. *See* National Institute of Standards and Technology (NIST)
 Nmap
 add complexity, 114
 and NSE, 115
 operating systems, 113
 port scan, 114
 scan results, 114, 114f, 115f
 Zenmap, 113
 Noncombatant, 252
 Non-state actors
 activities, terrorist groups, 207
 advantages, cyber warfare, 207
 autonomous actors
 (*see* Autonomous actors)
 corporations (*see* Corporations, non-state actors)
 criminal organizations
 (*see* Criminal organizations)
 cyber terrorism (*see* Terrorism, cyber)
 individual actors (*see* Individual actors)
 individual scale and smaller groups activity, 218
 North American Treaty Organization (NATO), 7, 10, 12, 222, 231
 Northern Command (NORTHCOM), 287
 NSA. *See* National Security Agency (NSA)

O
 Obfuscation tools
 defense, 134
 description, 131
 file manipulation, 133–134
 location obscuration, 131–132
 log manipulation, 132–133
 OCS. *See* Office of Cyber Security (OCS)
 OCTAVE. *See* Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)
 Offensive Security Certified Professional (OSCP), 84
 Offensive skill, 87
 Office of Cyber Security (OCS), 95
 Open source intelligence (OSINT), 7, 171–173
 Open Vulnerability Assessment System (OpenVAS), 118
 Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE), 238
 Operational Security (OPSEC)
 techniques
 description, 165
 tactical level actions, 165–166
 Organizations, cybersecurity and AOC, 40–41
 CIO and CFO, 38–39
 CYBERCOM and services, 41
 and FAA, 39
 and FBI, 39
 federal government, 39
 hierarchical authority structure, 40
 Organized crime, 28
 OSCP. *See* Offensive Security Certified Professional (OSCP)
 OSINT. *See* Open Source Intelligence (OSINT)

P
 Passive reconnaissance, 173–174
 Patriot hacker, 211
 Penetration test, 202–203
 Personally identifiable information (PII), 98, 208, 210, 237–238
 Physical infrastructure, 37–38
 Physical weapons
 conventional explosives, 137
 description, 137
 infrastructure concerns, 140–143

logical and physical realms, 138–140
 supply chain concerns, 143–145
 tools, attack and defense, 145–153
 PIA. *See* Privacy impact assessment (PIA)
 PII. *See* Personally Identifiable Information (PII)
 Pin-tumbler locks, 152
 Post Office Protocol (POP), 185–186
 Privacy impact assessment (PIA), 237–238
 Private/Mercenary Armies, 70
 Privilege escalation, 187–188
 Proper conduct in war
 collateral damage, 253
 distinction, 251–252
 limiting attacks, 253–254
 noncombatants, 252
 principles, 251
 proportionality, 252–253
 Psychological Operations (PSY OPS)
 description, 155
 military and SE, 161–165
 MISO and OPSEC, 155
 and SE (*see* Social engineering (SE))

R
 Read Only Memory (ROM), 130
 Reconnaissance process
 and OSINT, 171–173
 passive, 173–174, 174f
 Reconnaissance skill, 86, 99
 Reconnaissance tools
 description, 104–105
 engines, 106
 Google hacking, 105–106
 information, 105
 search engines, 105
 Shodan, 106
 websites and web servers, 105
 Whois tool, 106–107, 107f, 108f
 The Regional Internet Registries (RIR), 107–108
 Resilience, 261–262
 Revolution in Military Affairs (RMA), 6
 The Right to wage war
 last resort, 251
 non-state attackers, 249–250
 principles, 249–250
 probability of success, 251
 proportionality, 251

- right authority, 250
right intention, 250–251
RIR. *See* The Regional Internet Registries (RIR)
RMA. *See* Revolution in Military Affairs (RMA)
ROM. *See* Read Only Memory (ROM)
- S**
SANS. *See* SysAdmin, Audit, Network and Security (SANS)
Sarbanes—Oxley Act (SOX), 236
SCADA. *See* Supervisory Control and Data Acquisition (SCADA)
Scammer, 209–210
Scanning tools
 defense, 118
 description, 113
 nessus (*see* Nessus)
 nmap, 113–115
Science, Technology, Engineering and Mathematics (STEM), 267
Script kiddies/noobs, 29–30, 208–209
SE. *See* Social Engineering (SE)
Secrecy, 255
Secretary General for National Defense (SGDN), 92–93
Secure Shell (SSH), 126
Security awareness, CND, 198–199
Security Operations Centers (SOC), 31
Security training, CND, 199–200
SGDN. *See* Secretary General for National Defense (SGDN)
Signals intelligence (SIGINT), 7
Singapore Infocomm Technology Security Authority (SITSA), 93
Situational awareness and visualization, 269, 272
SOC. *See* Security Operations Centers (SOC)
Social Engineering (SE)
 approaches, 159–160
 methods, 160–161
 military approaches, 161–165
 vs. military defends, 165–168
 as science, 156
 and TTPs, 157–159
SOX. *See* Sarbanes—Oxley Act (SOX)
SSH. *See* Secure Shell (SSH)
Staff, cyber warfare
 “ethical hacking”, 99–100
financial and emotional trauma, 98
issues, 100
malicious attacker, 99
military recruits, 97
Personally Identifiable Information (PII), 98
physical and logical sense, 99–100
recruitment, talented people, 97–98
rigorous and time-consuming training processes, 97
skills requirement, 99
strategic and tactical knowledge, 100
training paradigm, 98–99
the United States and China, 96–97
STEM. *See* Science, Technology, Engineering and Mathematics (STEM)
Stored Communications Act (SCA), 239
Strategic Command (STRATCOM), 91
Supervisory control and data acquisition (SCADA)
 consequences, failures, 143
 control and monitor, 141
 description, 141
 potential outright hardware damage, 131
 remote monitoring sensor, 141–142, 141f
 sagging lines, 213, 280
 security issues, 142
 use of force, 246
 utility systems, Ohio begin, 213
 vulnerabilities, 115–116, 116f
Supply chain
 compromised hardware, 144
 corrupted components, 144–145
 definition, 262
 nontechnical issues, 145
Surveillance, CNE
 and APT, 175–176
 data, 176–177
 justifications, 175
 large-scale programs, 177–178
 uses, 178
 voice, 176
Sustainment tools
 adding “authorized” access, 127
 backdoors, 127–128
defense, 128
description, 127
SysAdmin, Audit, Network and Security (SANS), 84
- T**
Tackling locks
 bypassing locks, 151
 common lock picks, 151, 151f
 defending *vs.* covert attacks, 152–153
 padlock/combination lock, 151
 pin-tumbler locks, 152
Tailgating methods, 150
Targeted access attack, 158–159
Technical intelligence (TECHINT), 7
Technical Reconnaissance Bureaus (TRB), 91–92
Terrorism, cyber
 attribution, 214
 communications methods, 214
 conventional terrorists, 212
 definition, 212
 intelligence agencies, 213
 military build-up, 213
 motivation, 213
 organizations, 214
 and SCADA, 213, 218
 the United States, borders security, 213–214
 virtual and physical world, 214
Traditional fighting forces
 age, 87–88
 attitude, 88
 credentials, 89
 physical condition, 88–89
TRB. *See* Technical Reconnaissance Bureaus (TRB)
- U**
The Uniform Code of Military Justice (UCMJ), 236
The United States
 Air Force cyber doctrine, 59–60
 Army cyber doctrine, 61–62
 cyber capabilities and plans, 225
 Navy cyber doctrine, 60–61
The United States doctrine
 Air Force, 59–60
 Army, 61–62
 CNO functions, 53–54
 forces, 55–56

The United States doctrine

(Continued)

and INFOCONs, 62–63

IO framework, 54, 54*f*

joint doctrine, 56–59

Navy, 60–61

offensive capabilities, 53–54

The United States laws

Computer Fraud and Abuse Act, 236

cyber incidents, 232–233

Cyber Security Enhancement Act, 236–237

DCMA and GLB, 236

and FISMA, 237–238

and HIPPA, 236

incentivize industry, 233

and ITAR, 235

national cybersecurity, 232–233

National Defense Authorization

Acts of 2006 and 2007, 236

National Guard and Coast Guard, 235

and NIST, 236

penal codes, 232–233

the Posse Comitatus Act, 235

the Radio Act of 1912, 236

standards to support

cybersecurity, 238

tribunal law, 232–233

and UCMJ, 236

uniformed services, 236

Use of force

and act of war, 222

ethics, cyber warfare, 246–247

hold morally culpable individuals

accountable, 254

international law, 222, 227

last resort, 251

probability of success, 251

right authority, 250

right intention, 250–251

unlawful cyber operations, 222

war and LEAs, 222

the War Powers Act, 228

The U.S. Internal Revenue Service (IRS), 105

V

Voice over IP (VoIP), 176

Voice surveillance, 176

Vulnerability assessment, 202–203

W

Waging war, cyber era

and CNO, 184

electronical, 182–183

and IDS, 184

logical, 183

physical, 182

reaction times, 184

reactive *vs.* proactive, 183

small-scale skirmishes, 184

traditional methods, 182

Warfare, ethics

attribution, 247

intent, 247

military laws, 247–248

use of force, 246–247

War-fighting domains

air, 43–44

combined arms, 44–45

cyber, 44

land, 42

sea, 42–43

space, 44

Weapons of Mass Destruction (WMD), 8

X

XML-RPC. *See* Extensible Markup

Language Remote Procedure

Call (XML-RPC)

XMPP. *See* Extensible Messaging

and Presence Protocol

(XMPP)