INDEX

Above ground level (AGL), 279
Academy of Counter-Terrorist Education (ACE), 237
Actionable intelligence, 138
Adbusters, 263
Advance Law Enforcement Rapid Response Training (ALERRT), 162
Advanced persistent threats (APTs), 65
After-action reports (AARs), 21, 205
Air and Marine Operations (AMO), 95
Airspace integration, innovation in, 280
Albert sensors, 74
Alien Act of 1798, 90
Alien smugglers, 102–103
All-hazards approach, 204
Alliance to Combat Transnational Threats (ACTT), 98
American Civil Liberties Union (ACLU), 281
American Society of Civil Engineers (ASCE), 18
Anti-Terrorism Advisory Council (ATAC), 126
Artificial intelligence (AI), 79
Asset response, 76
Assistant United States Attorney's Offices (AUSA), 126
Atmospheric storms, 5
Attribution, 46
Automated Indicator Sharing (AIS), 65
Aviation and observation technologies, 276

Backdoor access, 57
Baltimore 2015, 264–265
Battle in Seattle, 262
Binding Operational Directives, 64
Blockchain, 79–80
Border Enforcement Security Taskforces (BESTs), 98
Border security, 89–90
  coordinating structures, 98
  federal law enforcement border security responsibility, 95–96
  FIOPs, 93–95
  fiscal years 2014–2018 strategic plan, 95
  homeland security nexus, 90–92
  law enforcement border security collaborative structures, 98–99
  military and border security, 99–100
  national protection goal and national preparedness system, 92
  NPF, 92–93
  subnational law enforcement's role in border security, 96–98
  US borders, 100–106
Boston Marathon Bombing, 204–209
  changes in law enforcement preparedness, 212–214
  themes and excerpts, 211–212
Botnet, 35, 60
Brennan Center, 156
Brute force attack, 59
Budapest Convention, 44
Bundibugyo virus, 252
Bureau of Alcohol, Tobacco, and Firearms, Customs and Border Protection, 115
Bureau of Justice Assistance and the Police Executive Research Forum (BJA-PERF), 69

Business email compromise schemes (BEC schemes), 30, 33–34, 61
Bystanders, 158

California, cybersecurity in, 67
California Cybersecurity Integration Center (Cal-CSIC), 67
California Cybersecurity Task Force, 67
California v. *Ciraolo*, 282
Capacity building, 25
Carpenter v. *United States* (2018), 47
Cascading failures, 18–19
Catfishing, 34
Cell phone analysis, 134
Cell site location information (CSLI), 47
Cell tower manipulation, 58
Center for Domestic Preparedness (CDP), 237
Centers for Disease Control and Prevention (CDC), 240–241
Central Intelligence Agency (CIA), 117–118
Certificate of authorization (COA), 279
Check And Report Ebola kit (CARE kit), 254
Chemical, Biological, Radiological, Nuclear and Explosives event (CBRNE event), 207, 236
Chemical, Ordnance, Biological & Radiological Training Facility (COBRATF), 237
CHEMPACK, 245
Chicago Public Private Task Force (CPPTF), 24
ChicagoFIRST, 24
Cities readiness initiative (CRI), 246
City of Baltimore, 260
Clarifying Lawful Overseas Use of Data Act (CLOUD Act), 44–45
Collaboration, 70, 194–195
Collection Act of 1789, 90
Combined intelligence, 7
Commission on Accreditation for Law Enforcement Agencies (CALEA), 185, 227
Communication, 210
Communications Decency Act (CDA), 40
Community Emergency Response Teams, 24
Community Oriented Policing Services (COPS), 285
Company insiders, 62
Comprehensive emergency management (CEM), 171, 173
Comprehensive Preparedness Guide (CPG), 181
Computer crimes, 30
Computer Fraud and Abuse Act (CFAA), 38–39
Computer models, 270
Congressional Research Service (CRS), 162
CONPLAN, 221
CONTEST, 158
Continuity Guidance Circular (CGC), 185
Continuity operations plans (COOPs), 182, 185, 248
Continuous Diagnostics and Mitigation (CDM), 64
Coordinated attack, 4
Coordinating structures, 98
Coordination, 210
Corporate competitors, 61
Countering violent extremism (CVE), 114, 158
Counterterrorism (CT), 123
  operations, 114–115
Covert incident, 249
COVID-19 pandemic, 7
Crime prevention through environmental design (CPTED), 22
Criminal intelligence, 132–133

Crises, 4–7
Critical infrastructure (CI), 17
  capacity building, 25
  cascading failures, 18–19
  cybersecurity, 25–26
  infrastructure protection strategies, 19–25
  owners, 25
  sectors and sector-specific federal agency, 20
  system failure, 17–18
Critical infrastructure and key resources (CIKR), 15–17, 224
  cascading effect of CIKR failure, 19
  protection, 27
  risk management framework, 20
  systems, 18
Critical infrastructure security (*see also* Border security)
  improving, 64
  and resilience, 63–64
Critical partnerships, 31
Crowd management, 272
Culture of preparedness, 204
  areas of improvement for law enforcement response, 208–212
  Boston Marathon Bombing, 206–209
  building, 205
Customs and Border Protection (CBP), 94–95
Cyber, 66
Cyber Assistant Legal Attaché program (ALAT program), 45
Cyber corridor, 68
Cyber incident management, 43
Cyber incident response
  asset response, 76
  federal government's role in, 76–77
  intelligence support, 77
  policies, 76
  state and local governments' role in, 77–78
  threat response, 77
Cyber Information Sharing and Collaboration Program (CISCP), 65
Cyber Intrusion Command Center, 71
Cyber investigations and prosecutions
  cybercrime environment, 29–30
  cybercrime notifications, 41–43
  cybercrime terms and trends, 33–38
  evidence gathering, 43–46
  federal criminal statutes, 38–41
  federal government investigative strategy, authorities, and framework, 30–33
  investigative challenges, 46–47
Cyber Lab, 71
Cyber Task Forces (CTFs), 32
Cyber threat environment, 55–56
Cyber Threat Intelligence Integration Center (CTIIC), 72
Cyber Threat Team model, 32
Cyber threats, 18 U.S.C. § 875 (d), 39
Cyber-enabled crimes, 33
Cyberattacks, 25–26, 31
  backdoor access, 57
  company insiders, 62
  corporate competitors, 61
  DDoS attack, 59–60
  hacktivists, 61
  malware, 57
  man-in-the-middle attack, 57–59
  methods, 56
  motivations, 60
  nation-states, 60–61
  opportunists, 62
  organized crime groups, 61–62
  password attack, 59
  phishing, 57
  SQL injection, 60
  zero-day vulnerabilities, 56–57
Cyberbullying, 34
Cybercrime
  business email compromise, 33–34
  catfishing, 34
  cyberstalking, cyberharrasment, and cyberbullying, 34

DDoS attack, 35
doxing/swatting, 35
duty to report child pornography, 42
environment, 29–30
general cybercrime reporting–current voluntary self-reporting, 41–42
jurisdiction, 43
notifications, 41
pharming, 35
phishing/spear phishing, 35–36
ransomware, 36
revenge porn, 36
sextortion, 36–37
SIM card swapping, 37
smishing, 38
social engineering, 38
spoofing/online impersonation, 38
terms and trends, 33
UCR/NIBRS, 42
victim notification, 42–43
vishing, 38
Cyberharrasment, 34
Cybersecurity, 25–26, 64, 72 (*see also* Election security example)
of federal networks and critical infrastructure, 64
Cybersecurity and Infrastructure Security Agency (CISA), 43, 64
Cyberspace Solarium Commission (CSC), 31, 56
Cyberstalking, 34
18 U.S.C. § 2261A, 39
Cynefin, 260

Data, 133
Decision-making models, 7
Deductive approach, 250
"Defend forward" approach, 66
Democratic Republic of the Congo (DRC), 236
Department of Defense (DOD), 66, 117–119
Department of Homeland Security–Cybersecurity and Infrastructure Security Agency (DHS-CISA), 60
Department of Homeland Security–Federal Emergency Management Agency (DHS-FEMA), 68
Department of Transportation (DOT), 78, 280
Destructive attacks, 30
Dictionary attack, 59
Director of National Intelligence (DNI), 56, 117
Disaster researchers, 177
Dissemination/action, 138–139
Distributed denial of service attacks (DDoS attacks), 30, 35, 59–60
District of Columbia (DC), 243
Diversion, 158
Do Not Board (DNB), 243
DOD's Cyber Crime Center (DC3), 72
Domain name server/system spoofing (DNS spoofing), 38, 58
Domestic Drones, 281
Domestic Preparedness Program (DPP), 236
"Don't Name Them" campaign, 162
Dow Chemical v. *United States*, 476 U. S. 227, 282
Doxing, 35
Drones, 263, 276
applications and cost advantages, 277–278
culture, 281
current legal landscape, 282–283
innovation in airspace integration, 280
limitations, 278–279
privacy issues, 280–282
recommendations for drone technology adoption, 283–288
regulatory environment, 279–280
Droughts, 6

Drug Enforcement Administration (DEA), 102
Drug Enforcement Agency (DEA), 115
Dual use vulnerability, 79
Duty to report child pornography, 42

Earth Liberation Front (ELF), 266
Ebola 2014–2016 case study, 252–255
Ebola virus (EBOV), 252
Ebola Virus Disease (EVD), 236
Economic Espionage, 18 U.S.C. §§ 1831–1839, 39–40
Economic Espionage Act (EEA), 39
Ecosystem, 1
8Chan, 163
EINSTEIN program, 64–65, 74
  EINSTEIN 1, 65
  EINSTEIN 2, 65
  EINSTEIN 3A, 65
El Paso MATRIX, 140–142
Election security example, 73
  federal government's role, 73–74
  local government's role, 75
  state government's role, 74–75
Electronic Crimes Task Forces (ECTFs), 33
Electronic evidence, data collection, and fourth amendment, 47
Email hijacking, 58
Email spoofing, 38
Emergency Assistance and Disaster Act, 68
Emergency management, 1, 260
  activities, 2
  cycle, 2
  positioning law enforcement within, 3
Emergency Management Assistance Compact (EMAC), 78, 230–231
Emergency medical officials, 237
Emergency medical personnel, 270
Emergency medical service (EMS), 212, 222
Emergency operations center (EOC), 178, 253
Emergency operations plans (EOPs), 182–185
Emergency planning, 177
Emergency support functions (ESFs), 223
Emergent threats, 4, 6–7, 79
  AI, 79
  blockchain, 79–80
  IoT, 79–80
Emerging threats (*see* Emergent threats)
Encryption, 46–47
Enforcement and Removal Operations (ERO), 96
Enhanced Cybersecurity Services (ECS), 65–66
Environmental Protection Agency (EPA), 282
Escalated force, 260–261
Evidence gathering, 43 (*see also* International evidence gathering)
  SCA, 43–44
  Wiretap Act, 44
Executive Order (EO), 242
  Executive Order 13636, 64
  Executive Order 13691, 64
  Executive Order 13800, 64
Exercise participation, 205
Explosive Ordinance Detection (EOD), 214
Extortion, 61
Extraordinary rendition, 118
Extreme weather, 5

Federal Aviation Administration (FAA), 278
Federal Bureau of Investigation (FBI), 30, 70, 115, 135, 156, 214, 221, 250
Federal criminal statutes, 38
  CFAA, 38–39
  cyber threats, 18 U.S.C. § 875 (d), 39

cyberstalking, 18 U.S.C. § 2261A, 39
economic espionage, 18 U.S.C. §§ 1831–1839, 39–40
online human trafficking, 40
sexual exploitation of children, 18 U.S.C. § 2251, 40
threats and harassment, 47 U.S.C. § 223, 41
wire fraud, 18 U.S.C. § 1343, 41
Federal cyber centers, 72
Federal cyber investigators, 32–33
Federal cyber strategy, 30–31
Federal Emergency Management Agency (FEMA), 92, 154, 179, 204, 220
Federal government investigative strategy, authorities, and framework, 30–33
Federal government's role, 73–74
in cyber threat management, 62
offensive cyber operations, 66
policies, 63–64
systems monitoring, threat detection, and information sharing, 64–66
Federal Interagency Operational Plans (FIOPs), 93–95, 182
Federal investigative authority, 31–32
Federal law enforcement border security responsibility, 95–96
Federal Radiological Emergency Response Plan (FRERP), 221
Federal Response Plan (FRP), 221
Federal Trade Commission (FTC), 36
Federalism, 240–241
Feedback, 139
Felt need, 195–196
high level of, 199
Ferguson Effect, 269
Filoviridae Ebolavirus, 252
Firefighters, 270
Fiscal year (FY), 105
2014–2018 strategic plan, 95
Fixed-wing aircraft, 276
Floods, 5
Florida v. *Riley*, 488 U.S. 445, 282
Force protection, 19
Formalized processes, 198
Freedom of Information Act, 16
Fusion centers, 21, 72, 124–126
liaison officer programs, 134
risk-assessment model, 136

Game theory, 22
Geographic information system (GIS), 271
Global positioning devices, 134
Global positioning system (GPS), 47, 147, 262
Globalization, 18
Governor's Guide to Homeland Security, *A*, 120, 125

Hacktivists, 61
Hazardous materials (HazMat), 207
Hazards, 3–4, 7
Health Insurance Portability and Accountability Act (HIPAA), 239
Heat waves, 6
Helicopters, 276
High threats, 6
High-reliability organization (HRO), 227–228
Homeland Security Exercise Evaluation Program (HSEEP), 188
Homeland Security Information Network (HSIN), 164
Homeland Security Investigations (HSI), 96, 115
Homeland security nexus, 90–92
Homeland Security Presidential Directive 5 (HSPD-5), 220
Household preparedness, 172
HTTPS spoofing, 58
Human behavior, 175–180
Human immune system, 27
Human responses to extreme events, 175–177

Human vulnerability, 79
Human-induced hazards, 4–6
Hurricanes, 5
Hybrid intelligence cycle, 139–140
Hydrologic systems, 5

Illegal immigration, 103–104
Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA), 97
Immigration and Customs Enforcement (ICE), 94–95, 115
Improvisation, 179
Improvised explosive devices (IEDs), 206
  awareness, 209
Incident action plan (IAP), 185
Incident Command Post (ICP), 225–227
Incident Command System (ICS), 2, 70, 178, 187, 210, 220–221, 225–227
  critique, 227–230
Incident commander (IC), 186
Incident management teams (IMTs), 186–187
Indoctrination, 155
Inductive approach, 250
Information, 132–133
Information sharing, 64–66, 71, 134
  federal cyber centers, 72
  fusion centers, 72
  InfraGard, 72
  ISAO, 72–73
  MS-ISAC, 73
  NCFTA, 73
Information Sharing and Analysis Centers (ISAC), 64
Information Sharing and Analysis Organizations (ISAOs), 64, 72–73
Information Systems Audit and Control Association (ISACA), 41
Information technology (IT), 64
InfraGard, 25, 72
InfraGard Members Alliance (IMA), 72
Infrastructure protection strategies, 19–25
Innovation Team, 179
Insurance, 25
Integrated planning, 208
Integration of federal, state, and local agencies, 122–126
Integration Pilot Program (IPP), 280
Intelligence, 114, 132–133
  analysis, 138
  center, 134
  collection, 136–137
  cycle, 135–139
  dissemination/action, 138–139
  feedback/reevaluation, 139
  fusion centers, 120
  key intelligence functions, 134–140
  liaison officer, 134
  planning and direction/requirements, 135–136
  processing, 137–138
  support, 77
Intelligence and investigation function (I/I function), 228
Intelligence community (IC), 31, 104
Intelligence Community's Security Coordination Center (IC-SCC), 72
Intelligence Reform and Terrorist Prevention Act (IRTP Act), 116
Intelligence-led policing (ILP), 133–134
Intentional biological events, 236
Interagency, 199
International Association of Chiefs of Police (IACP), 284
International City/County Management Association, 77
International evidence gathering, 44
  Budapest Convention, 44
  CLOUD Act, 44–45
  international cooperation, 45–46

MLAT, 45
International pandemic, 6
Internet, 34
Internet billboard, 61
Internet Crime Complaint Center (IC3), 30, 33, 41
Internet Crimes Against Children Task Force Program (ICAC), 33
Internet of Things (IoT), 79–80
Internet protocol spoofing (IP spoofing), 38, 58
Internet Service Provider (ISP), 36
Investigative challenges, 46–47
Irish Republican Army (IRA), 157
Isolation, 241–244

Jihadization, 155
Joint Counterterrorism Assessment Team (JCAT), 118
Joint investigations, 251
Joint Operations Center (JOC), 72
Joint Task Force (JTF), 99
Joint Terrorism Task Forces (JTTF), 115, 123–124, 159
Jurisdiction, 43

Katz v. *United States*, 282
Kent State University, 261
Key logger attack, 59
Known and Suspected Terrorists (KSTs), 104

Law enforcement, 1, 21, 90, 114
  agencies, 8–9
  best practices, 140–148
  border security collaborative structures, 98–99
  crises, 4–7
  hazards and threats, 3–4
  intelligence process, 131–132
  intelligence-led policing, 133–134
  key intelligence functions, 134–140
  levels, 22
  officers, 3
  paradigmatic shift, 7–8
  parties, 2
  positioning law enforcement within emergency management, 3
Law Enforcement Online (LEO), 164
Law Enforcement Support Center (LESC), 99
Leadership, 197
  as primary factor, 199
  trust and leadership compensate, 200
Legal Attaché program (LEGAT program), 45
Local government's role, 75
Los Angeles, cyberattacks, 70
Los Angeles Police Department (LAPD), 164
Louisiana, cybersecurity in, 68
Louisiana State University (LSU), 237

Machine learning (ML), 79
Major Cities Chiefs Association (MCCA), 163
Malware, 36, 57
Man-in-the-middle attack, 57–59
Managed inventory (MI), 245
Mandated system, 197–198
Mass violence, 153
  early research and strategies, 155–157
  evolution of multidisciplinary team approaches, 159–164
  United Kingdom's counterterrorism strategy, 157–158
  United States' countering violent extremism model, 158–159
Mathematical modeling, 260
Medical assistance, 209
Medical countermeasures (MCM), 241
Megacities, 17
Memorandums of understanding (MOU), 230
Mental Evaluation Unit, 164
Metropolitan statistical areas (MSAs), 246
Michigan, cybersecurity in, 68

Michigan Cyber Civilian Corps (MiC3), 68
Michigan Cyber Disruption Strategy, 68
Michigan Cyber Initiative, 68
Military and border security, 99–100
Misattribution, 46
Mobilization, 210
Money Mule Team (MMT), 34
Motivation, 56
Multi-Agency Tactical Response Information Exchange (MATRIX), 140
Multi-state Information Sharing and Analysis Center (MS-ISAC), 71, 73
Multidisciplinary team approaches, evolution of, 159–164
Mutual aid agreements (MAAs), 230
Mutual Legal Assistance Treaty process (MLAT process), 45

Nation-states, 60–61
National Aeronautics and Space Administration (NASA), 226
National Association of Secretaries of State (NASS), 74
National Center for Biomedical Research Training (NCBRT), 237
National Computer Forensics Institute, 33
National Conference of State Legislatures (NCSL), 75
National Counterterrorism Center (NCTC), 116, 123
National Criminal Intelligence Sharing Plan, 134
National Cyber Incident Joint Task Force (NCIJTF), 32, 43
National Cyber Incident Response Plan (NCIRP), 67
National Cyber Investigative Joint Task Force (NCIJTF), 72, 77
National cyber strategy, 31, 63
National Cyber Strategy of the United States of America, 30–31
National Cybersecurity and Communications Integration Center (NCCIC), 72
National Disaster Preparedness Training Center (NDPTC), 237
National Domestic Preparedness Consortium (NDPC), 237
National Emergency Management Association (NEMA), 230
National Emergency Response and Recovery Training Center (NERRTC), 237
National Governors Association (NGA), 67
National Guard, 99–100
National Incident Based Reporting System (NIBRS), 42
National Incident Management System (NIMS), 2, 70, 177, 187, 207, 220, 229
  critique, 224–225
  expanding capabilities of local response, 230–231
  limitation to, 225
  steps, 221–222
  structure, 222–224
National Infrastructure Protection Plan (NIPP), 63
National Institute of Standards and Technology (NIST), 78
National Joint Terrorism Task Force (NJTTF), 126
National Nuclear Security Administration (NNSA), 237
National Oceanic and Atmospheric Administration (NOAA), 4
National Operations Center (NOC), 99
National Planning System (NPS), 180
National policy, 171
National power, 31

National preparedness, 63
National Preparedness Goal (NPG), 92, 173–175, 204
National Preparedness System (NPS), 92, 173
National Protection Framework (NPF), 92–93
National Response Framework (NRF), 222
National Response Plan (NRP), 222
National Security Agency (NSA), 119
National Security Decision Directive (NSDD), 56
National security investigations, 32
National Security Special Events (NSSE), 199
  recommendations for successful events, 198–200
  supportive factors, 195–198
National Training and Education Division (NTED), 122
National-level policy, 126–127
Natural events, 236
Natural hazards, 4–5
Negotiated management, 261–262
New Jersey ROIC, 142–145
New Mexico Energetic Material Research and Testing Center (EMRTC), 237
New Orleans Police Department (NOPD), 177
New York, cybersecurity in, 69
New York Police Department (NYPD), 23–24, 121, 155
New Yorkers, 18
Noble Training Facility (NTF), 237
Non-pharmaceutical interventions, 244–245
Nongovernmental organizations (NGOs), 2, 222
NSA's Cybersecurity Threat Operations Center (NCTOC), 72
Nunn-Lugar-Domenici Act, 236

Oakland City government, 264
Occupy Movement, 260, 263–264, 272
Offensive cyber operations, 66
Office of Field Operations (OFO), 95
Office of the Director of National Intelligence (ODNI), 118
Online human trafficking, 40
Online impersonation, 38
Operational coordination, 229
Operational-level planning, 182–185
Opportunists, 62
Organizational behavior, 175–180
Organizational preparedness, 9
Organizational responses, 177–180
Organized crime groups, 61–62
Overt incident, 249

Pakistani International Airports' computer system, 26
Pandemics, 246–248
Password(s), 46–47
  attack, 59
Payroll diversion, 61
Personal identification numbers (PIN), 35
Personal identifying information (PII), 35, 60
Pharming, 35
Phishing, 35–36, 57
Physical assets, 15
Physical security, 19
Pittsburgh, 71
Planning, 171
  assumptions, 175–180
Planning, Organization, Equipment, Training, and Exercises (POETE), 181
Points of distribution (PODs), 245
Police commanders, 269
Police departments (PDs), 214, 263, 277
Police Executive Research Forum (PERF), 42, 247, 264–265
Police organization terrorism preparedness, 173

Policing civil disturbances, 259
  case studies, 263–269
  evolutions of response to demonstration and unrest, 260–263
  integrated responses for future, 270–272
Policing protest, 260
Polyvinyl chloride (PVC), 263
Portland Police Department (PPD), 263
Posse Comitatus Act, 99
Posse Comitias, 214
Post-9/11 criminal justice research, 173
Pre-radicalization, 155
Preparedness, 171–175
  improving preparedness plans, 188
  for US law enforcement agencies, 180–188
President's Task Force on 21st Century Policing, 261
Presidential Policy Directive (PPD), 16
  PPD 21, 20, 63–64
  PPD 41, 76
  PPD 8, 63, 173, 175, 204
PREVENT, 158
Prevention mission, 9
Private sector cybersecurity information sharing, 64
Project Solarium, 31
Protecting Privacy from Aerial Surveillance, 285
Protection mission, 9
Protests
  as complex–adaptive environments, 266
  zones, 262
Providing Alternatives to Hinder Extremism initiative (PATHE initiative), 164
Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (PATRIOT Act), 116
Public health, 236
  change in approach–pushing capability to lowest level, 236–237
  Ebola 2014–2016 case study, 252–255
  law enforcement and public health organizational interactions, 249–251
  limitations to interaction, 239–241
  mechanisms of interaction, 241–248
  and practice of medicine, 238–239
Public Health Emergency of International Concern (PHEIC), 236
Public mass shootings, 154
Public safety-oriented platform, 8

Quadrennial Homeland Security Review (QHSR), 90–91
Quarantine, 241–244

Radicalization, 155
Rampant wildfires, 5
Random anti-terrorism measures (RAMs), 22
Ransomware, 36
  attacks, 30
Rapid intelligence, 139
Recovery and Investigative Development team (RaID team), 34
Recovery Asset Team (RAT), 34
Red flag laws, 162
Reevaluation, 139
Regional Operations and Intelligence Center (ROIC), 140
Reinsurance, 25
Reporting system, 41–42
Research-based knowledge, 171
Response, 67
  mission, 10
Reston virus, 252
Revenge porn, 36

Revenge pornography, 30, 36
Riley v. *California* (2014), 47
Risk management, 19

Sabotage, 60
Salmonella Typhimurium, 249–250
San Diego, 71
Santa Fe Police Department Criminal Intelligence Center, 145–146
Secret Service, 115
Secure sockets layer hijacking (SSL hijacking), 58
Security and Emergency Response Training Center (SERTC), 237
"See Something, Say Something" public information campaign, 204
Self-radicalization, 155
Semi-autonomous agencies, 120
Sensemaking, 178–179
Severe acute respiratory syndromes (SARS), 242
Sextortion, 36–37
Sexual Exploitation of Children, 18 U.S.C. § 2251, 40
SHIELD, 23–24
SmartPhones, 46–47
Smishing, 38
Social capital, 196–197
Social distancing, 243
Social engineering, 38
Social identity, 272
Social media covert operations, 134
SONY attack, 46
Southern California fires, 2
Southern Poverty Law Center (SPLC), 7
Spear phishing, 35–36
Special Interests Aliens (SIAs), 104
Special weapons and tactics (SWAT), 35, 207, 264
Spoofing, 38
Spyware, 57
Stakeholder Preparedness Review (SPR), 181
State, Local, Tribal and Territorial (SLTT), 21
State Active Duty (SAD), 70
State and local governments' role
  in cyber incident response, 77–78
  in cyber threat management, 66–67
State Cyber Disruption Response Plans, 67
State government's role, 74–75
Stealing browser cookies, 58–59
Stop Enabling Sex Traffickers Act of 2017 (S. 1693) (SESTA), 40
Stored Communications Act (SCA), 43–44
Storm surges, 5
Strategic incapacitation, 262–263
Strategic intelligence, 138–139
Strategic National Stockpile (SNS), 244–246
Strategic-level planning, 181–182
Strategy, 90
Structure Query Language injection (SQL injection), 60
Structured Interview for Violence Risk Assessment (SIVAR), 164
Structures, 94–95
Subnational law enforcement's role in border security, 96–98
Subscriber identity module card swapping (SIM card swapping), 37
Sudan virus, 252
Surveillance cameras, 134
Swatting, 35
Sweeping generalizations, 155
Swift trust, 196
System failure, 17–18
Systems monitoring, 64–66

Tactical intelligence, 138
Tactical-level planning, 185–188
Tai Forest virus, 252
Target and Blue program, 24
Targeting intelligence methodology, 136
Tariff Act of 1789, 90

Task force environment, 33
Task Force Officers (TFOs), 163
Technical vulnerability, 79
Technological solutions, 134
Technology, 47
Technology adoption, 283–288
Telecommunications device, 41
Telephones, 41
Terrorism, 154
  nexus, 104–106
Terrorism Liaison Officer (TLO), 122
Terrorism prevention, 113–114
  at federal level, 114–120
  integration of federal, state, and local agencies, 122–126
  at local level, 121–122
  national-level policy, 126–127
  at state level, 120–121
Terrorism Risk Insurance Act, 25
Terrorist Screening Center (TSC), 116
Thornton's 4C's model, 7–9
Threat and Hazard Identification and Risk Assessment (THIRA), 181
Threat(s), 3–4, 7, 56
  to border security, 101
  detection, 64–66
  and harassment, 47 U.S.C. § 223, 41
  response, 77
Thunderstorms, 5
Tornadoes, 5
Trade secret, 39–40
Traditional crimes, 30
Training, 205
Transnational criminal organizations (TCOs), 102–103
Transportation Security Administration (TSA), 224
Trickery, 59
Trust, 196–197
  and leadership compensate, 200
  as primary factor, 199–200
  trust-building, 284
Tuberculosis (TB), 243

Ukrainian electrical system, 26
Unified command (UC), 186
Unified Coordination Group (UCG), 76, 78
Uniform Crime Reporting (UCR), 42
United Kingdom's counterterrorism strategy, 157–158
United Nations Department of Economic and Social Affairs (UN DESA), 17
United States Cyber Command (USCYBERCOM), 66
United States Department of Agriculture (USDA), 198
United States Department of Justice (US DOJ), 30, 60, 221, 285
United States Intelligence Community (USIC), 114, 118
United States Secret Service (USSS), 33
United States v. *Causby*, 328 U.S. 256, 283
United States v. *Jones* (2012), 47
United States v. *Microsoft* (2017), 45
United States' countering violent extremism model, 158–159
University of Delaware Disaster Research Center (DRC), 177
Unmanned aerial vehicles (UAVs), 263, 276
Unmanned aircraft, 281
Unmanned aircraft systems (UASs), 276
Urbanization, 17
US Border Patrol (USBP), 95
US borders, 100
  illegal immigration, 103–104
  security strategy, 90
  terrorism nexus, 104–106
  threats to border security, 101
  transnational criminal organizations and alien smugglers, 102–103
US Coast Guard (USCG), 95
US Department of Homeland Security (DHS), 16, 20, 36, 90, 116–117, 173, 204, 221

US law enforcement agencies, preparedness for, 180–188
USSS-NTAC, 160–161
Utah
  cybersecurity in, 69
  model, 69
Utah Department of Public Safety (DPS), 69
Utah Olympic Public Safety Command (UOPSC), 197
Utah Technology Governance Act, 69

Vehicle-borne improvised explosive attacks (VBIED attacks), 19
Vermont, cybersecurity in, 69–70
Victim notification, 42–43
Violence Project, The, 162
Virginia, cybersecurity in, 70
Viruses, 57
Vishing, 38
Visible intermodal protection and response operations (VIPR operations), 22
Voice over Internet protocol (VOIP), 41, 78
Vulnerabilities, 56–57

"WannaCry" virus, 36
WarGames, 55
  cities, 70–71
  cyber threat environment, 55–56
  cyberattack methods, 56–60
  cyberattack motivations, 60–62
  election security example, 73–75
  emerging threats, 79–80
  federal government's role in cyber incident response, 76–77
  federal government's role in cyber threat management, 62–66
  information sharing, 71–73
  state and local governments' role in cyber incident response, 77–78
  state and local governments' role in cyber threat management, 66–67
  states, 67–70
Watch operations, 146–147
Weapon and vehicle protocols, 209–210
Weapons of Mass Destruction (WMD), 94, 236
Whole-community approach, 204
Wi-Fi eavesdropping, 58–59
Winter Olympics, 194–195
Winter storms, 5
Wire fraud, 18 U.S.C. § 1343, 41
Wiretap Act, 44
Wisconsin, cybersecurity in, 70
Wisconsin Emergency Management (WEM), 70
World Health Organization (WHO), 7
World Trade Organization (WTO), 262

Zero-day
  attack, 56
  vulnerabilities, 56–57