Index

Action management, 29
Active mode, 176
AEGIS, 197–198
al-Qaeda, 83
American Civil Liberties Union (ACLU), 84
Analysis phase, 10–11
Analytics management, 29
Arab world, 2
AUS/CAN/NZ/UK/US EYES ONLY, 62
Australia, 34–39, 100–104
Australian Crime Commission (ACC), 129
Australian Criminal Intelligence Commission (ACIC), 100
Australian Criminal Intelligence Forum (ACIF), 100
Australian Cybercrime Online Reporting Network (ACORN), 103
Australian Geospatial-Intelligence Organization (AGO), 35
Australian Intelligence Community (AIC), 34–39
Australian Secret Intelligence Service (ASIS), 34
Australian Security Intelligence Organization (ASIO), 34
Australian Signal Directorate (ASD), 34
Auxiliarization, 137

BAE systems, 198
Big Data analytics, 184, 185
Black satellites, 169
Booz Allen Hamilton (BAH), 198–199

British Security Industry Association (BSIA), 173
CACI International Inc., 199
Canada, 39–45, 104–107
Canadian Forces Intelligence Command (CFIC), 44
Canadian Forces Joint Imagery Centre (CFJIC), 44
Canadian intelligence community (CIC), 40–43
Canadian Security Intelligence Service (CSIS), 93
Catholic Church, 2
CCTV technology, 173, 174–175
Cellular Analysis and Notification of Antigen Risks and Yields (CANARY), 180
Central Intelligence Agency (CIA), 28, 75
Chilling effect of secrecy, 21
Code of conduct, 227–230
Cold War, 4
Collation phase, 10
Collection phase, 10
Combined DNA Index System (CODIS), 178
Communications Security Establishment (CSE), 40
Community-based policing model, 135
CompStat approach, 98
Compulsive data demand, 14
Conceptual approaches, 20–22
Consequentialist approach, 210
Constructive methods, 20
Counterterrorism Center, 79
Counter Terrorism Command (CTC), 111
Creation of knowledge, 28
Criminal intelligence
  acceptance, 95
  activities, 5
  basic knowledge, 96–97
  detecting criminal activity, 97–98
  “Five Eyes” countries, 100–115
  functions, 96–100
  guiding decisions, 99–100
  international police cooperation, 115–119
  operations, 99–100
  policy, 85–86
  practice, 90–92
  predicting criminal activity, 98–99
  services, 130
  strategy, 86–89
  structure, 89–90
  structure and integration, 100–115
  targets, 92–93
Criminal Intelligence Service Canada (CISC), 106
Criminal Investigation Branch (CIB), 108
CSRA Inc., 199–200
Cuban missile crisis, 13
Cyber Action Team (CAT), 157
Cyber insecurity, 160
Cyber intelligence
  cybersecurity risk, 159–161
  defensive, 139
  intensity, 146–148
  law enforcement, 156–159
  offensive, 139
  private and public entities, 140
  strategic form, 140
  technical form, 140
Cyber threats
  actors, 140
  cyberspace, 143–146
  evolution, 140
  landscape, 140–143
  modus operandi, 143
Dark Web, 146
DCSNET, 176
Decision-making process, 20
Defense Intelligence Agency (DIA), 194
Defense Intelligence Organization (DIO), 34–35
Deontological approach, 210–211
Detecting criminal activity, 97–98
Digital divide, 13
Directorate of Defence Intelligence and Security (DDIS), 46
Director of Central Intelligence (DCI), 79
Dissemination phase, 11
“Diversion Team,” 104
Drug Enforcement Administration (DEA), 85
Dual conceptualizations of intelligence, 4–7
Echelon program, 62
Efficiency, 71
Electronic Frontier Foundation (EFF), 171
Embedded knowledge, 28
Environmental Protection Agency (EPA), 183
Espionage, 2
Ethics
  analysis, 212
  code of conduct, 227–230
  consequentialist approach, 210
  deontological approach, 210–211
  immoral intelligence collection techniques, 207
  intelligence analysis, 218–220
  intelligence collection, 212
  intelligence collection methods, 217–218
  intelligence management, 213
  just intelligence approach, 211–212
  Just War Theory, 211
realist approach, 209–210
secrecy violation, 220–227
truth approach, 209
utilitarian approach, 208
whistleblowing, 220–227
Ethics of risk, 71
European Cyber Crime Center, 158
Explicit knowledge, 27
Exploitative methods, 20
Export Administration Regulations (EAR), 161

Facebook, 151
Facial Analysis, Comparison, and Evaluation (FACE), 179
Federal Bureau of Investigation (FBI), 28, 156
Five Eyes countries
Australia, 34–39
Canada, 39–45
New Zealand, 45–49
United Kingdom, 49–54
United States, 54–61
“Five Eyes” countries
Australia, 100–104
Canada, 104–107
New Zealand, 107–109
United Kingdom, 109–112
United States, 112–112
FlexiSPY, 177
Foodborne Disease Outbreaks Surveillance System (FDOSS), 183
Foreign Intelligence Surveillance Act Court (FISA), 23

Geospatial intelligence (GEOINT), 7
Geosynchronous orbit (GEO), 168
Global Hawk, 170
Government Accountability Office (GAO), 23
Government Communications Headquarters (GCHQ), 175

Government Communications Security Bureau (GCSB), 46
Government policy, 73
Great Firewall, 146
Greece, 2
Guardian of Peace (GOP), 147
Gunwalking Scandal, 21

Hacktivists, 227
Hard surveillance technology, 167
hearing, 175–178
scent, 180–181
sight, 167–175
software surveillance technology, 184–186
taste, 182–184
touch, 178–180
Her Majesty’s Inspectorate of Constabulary (HMIC), 111

High policing activity, 5
Homeland Security Act, 79
Horizontal communication, 132
House Permanent Select Committee on Intelligence (HPSCI), 56
Human intelligence (HUMINT), 7
HUMINT, 218

Identification of knowledge, 28
ILP model, 99
Imagery intelligence (IMINT), 7
Immoral intelligence collection techniques, 207
Independent Police Complaints Commission (IPCC), 111
Industrial revolution, 3
Information gap, 13
Information overload, 14
Inspector General of the Intelligence Community (IGIC), 204
Institutional friction, 14
Integrated National Security Enforcement Teams (INSETs), 105–106
Integrated Terrorism Assessment Centre (ITAC), 45
Intelligence. See also Ethics
analysis, 218–220
collection, 212
collection disciplines, 7, 8
collection methods, 217–218
cycle, 8, 9
dual conceptualizations, 4–7
historical evolution, 2–4
intelligence collection disciplines, 7
limitations, 11–14
process, 7–11
Intelligence Community (IC), 77
Intelligence Coordination Group (ICG), 46
Intelligence knowledge management conceptual approaches, 20–22
limitations, 31–32
risk management, 25–27
state intelligence and surveillance, 22–25
and surveillance activities, 27–31
Intelligence-led policing (ILP), 95
criminal intelligence activities, 130–131
environmental contingencies, 124
criminal environment, 124–125
evolution, 121–124
hostility, 125–127
legal environment, 127–130
organizational contingencies, 130
organizational culture, 134–138
organizational structure, 131–134
structuring intelligence activities, 130
Intelligence management, 213
Intelligence outsourcing
civil liberties threat, 203
lack of accountability, 202–203
loss of stateness, 203
public analyst jobs threat, 204–205
public safety threat, 203
reputational concerns, 204
Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), 60, 79
Intelligence Services Commissioner, 53
Interception of Communications Commissioner’s Office (IOCCO), 53
International police cooperation, 115–119
International terrorist groups, 1
International Traffic Arms Regulations (ITAR), 161
Internet Crime Complaint Center, 157
Internet Mass surveillance programs national cyber surveillance programs, 149–155
transnational cyber surveillance programs, 155–156
Internet Organized Crime Threat Assessment (IOCTA), 156
Interpol, 118
Interpretation management, 29
Intrusive cyber intelligence operations, 147
Investigatory Powers Act, 54
Investigatory Powers Tribunal (IPT), 53
Islamic State (ISIS), 148
Islamic terrorism organizations, 83
Joint Cybercrime Action Taskforce (J-CAT), 158
Joint Terrorism Task Forces (JTTFs), 115
Judiciary model, 6
Just War Theory, 211
KH-11, 168
“Kill list,” 82
“Knowledge workers,” 96
Labor organizations, 3
Law enforcement, 130
agencies, 1, 172
intelligence, 24–25
Legality, 71
Levitation, 149
Linear Approach Program, 89
Linkage blindness, 13
Local law enforcement, 7
London Metropolitan Police, 95
Low earth orbit (LEO), 168
Low-intensity conflict, 1
Low policing activity, 5

Matrix organizations, 132
Measurement and signature intelligence (MASINT), 7
Merida Initiative, 88
Middle Ages, 2
Military interpretation
conceptualizing, 69–72
criminal intelligence, 85–93
national security intelligence, 72–85
operationalizing, 69–72
policy, 73
practice, 80–82
strategy, 73–76
structure, 77–80
targets, 83–85
Military industrial complex, 70
Military Intelligence Program (MIP), 56
Ministry of Science, Technology, and Innovation (MCTI), 160
Muscular program, 155

Napoleon Bonaparte, 4
National Assessments Bureau (NAB), 46
National Biosurveillance Integration Center (NBIC), 180–181
National Counterterrorism Center (NCTC), 79
National Criminal Intelligence Service (NCIS), 129
National Criminal Investigation DNA Database (NCIDD), 179
National Cyber Crime Unit (NCCU), 158
National Defense Radio Establishment (RFA), 150
National Disruption Group (NDG), 103
National Geospatial-Intelligence Agency (NGA), 78, 202
National Imagery and Mapping Agency (NIMA), 78
National Intelligence Model (NIM), 109, 129
National Intelligence Program (NIP), 56
National Reconnaissance Office (NRO), 168
National security, 72
National Security Agency (NSA), 4, 21, 71, 175
National security intelligence, 5, 22–24
Australia, 34–39
Canada, 39–45
clandestine/covert operations, 33
cooperation, 61–66
New Zealand, 45–49
United Kingdom, 49–54
United States, 54–61
New York City Police Department (NYPD), 97
New Zealand, 45–49, 107–109
New Zealand Intelligence Community (NZIC), 45–48
New Zealand Police (NZP), 107
Next Generation Identification (NGI), 179
Noise, 14
Nontraditional threats, 1
Northern Atlantic Treaty Organization (NATO), 199
Northrop Grumman, 201
NSA surveillance programs, 23
Office of Management and Budget (OMB), 23
Office of National Assessment (ONA), 34
Office of National Drug Control Policy (ONDCP), 86
Onyx program, 151
Open source intelligence (OSINT), 7
Operation Fast and Furious, 21
Organizational culture
  cultural differences, 136
definition, 134–135
government priorities, 135
intellectual resources, 138
lack of trust, 137
managerial approach, 137
multilateralization, 136
occupational differentiation, 137
roles, 134–138
statuses, 134–138
structural asymmetry, 136
Organization for Economic Cooperation and Development (OECD), 160
Organization of American States (OAS), 160
Organized and Financial Crime Agency of New Zealand (OFCANZ), 107
Organized Crime Drug Enforcement Task Forces (OCDETF), 114
Overclassification, 216

PANTHER device, 180
Passive mode, 176
Pearl Harbor, 13
Plan Mexico, 88
Police and Custom Cooperation Centre (PCCC), 118
Police organizations, 133, 134
crime, 133
criminal intelligence agencies, 134
decentralization, 130
decision-making process, 133
Policy-maker influence, 218
Predicting criminal activity, 98–99
Priorities and intelligence requirements (PIRs), 9–10
Privacy and Civil Liberties Oversight Board, 60
Private intelligence sector
  actors and services, 197
AEGIS, 197–198
BAE systems, 198
Booz Allen Hamilton (BAH), 198–199
CACI International Inc., 199
corporations, 193
CSRA Inc., 199–200
Defense Intelligence Agency (DIA), 194
general dynamics, 200–201
growth, 191–193
income incentives, 194
Northrop Grumman, 201
one-stop-shop, 193
private firms, 193
private–public interface, 195
roles, 193–195
Science Applications International Corporation (SAIC), 201–202
Private–public interface, 195
dynamics, 195
expansion, 196
extension, 195–196
privatization, 196–197
Privy Council Office (PCO), 44
Project 6, 150
Public management networks, 30
Pulsenet, 182

Racketeer Influenced and Corrupt Organizations (RICO) Act, 122
Radical secrecy, 21
Realist approach, 209–210
RealTek audio, 177
Renaissance era, 2
Responsibility, 131
Risk imaging, 13
Risk management, 25–27
Risk society, 26
Roman Inquisition, 2
Royal Canadian Mounted Police (RCMP), 44, 104, 105, 172
Science Applications International Corporation (SAIC), 201–202
Second Gulf War, 21
Secrecy
chilling effect of secrecy, 21
radical secrecy, 21
violation, 220–227
Security Intelligence Review Committee (SIRC), 40
Senate Select Committee on Intelligence (SSCI), 56
September 11, 2001, 73
Serious Organized Crime Agency (SOCA), 110
Severe Acute Respiratory Syndrome (SARS), 180
Signals intelligence (SIGINT), 7, 218
Singapore Police Force (SPF), 126
Sniffing operations, 147
Sniffing technology, 180
Social control
constructive, 20
exploitative, 20
Somali National Alliance (SNA), 78
Source management, 29
South America, 2
Soviet Union, 4
Special Operations Division (SOD), 90
Special warfare, 1
SpyToMobile, 177
State intelligence and surveillance
law enforcement intelligence, 24–25
national security intelligence, 22–24
State’s security mission, 26
StingRay machine, 175
Stockholm International Peace Research Institute, 70
Sub-Saharan African tribal chiefs, 2
Surveillance technologies
conceptual approach, 166–167
digital surveillance technology, 174
disruptive technology, 187–189
hard surveillance technology, 167
intelligence, 165–189
new collection discipline, 187–189
satellites, 167–168
Tacit knowledge, 28, 136, 138
Tactical drone, 170
Telecommunications data, 148
Titan Traffic Database, 150
Total Information Awareness (TIA), 23
TrailBlazer program, 154
UK–USA Agreement, 62
UK–USA collaborating Commonwealth countries, 62
United Kingdom, 49–54, 109–112
United Kingdom intelligence community (UKIC), 49–53
United States, 54–61, 112–112
United States intelligence community (USIC), 29, 55–59
Unmanned aircraft vehicles (UAVs), 23
US Department of Defense budget, 70
US Federal Aviation Agency (FAA), 170
US Intelligence Community, 13
Utilitarian approach, 208
Vertical compartmentalization, 131
Vulnerability Assessment–Sensor Placement Optimization (TEVA–SPOT), 183
War Measures Act, 71
“War on drugs,” 71, 85
“War on terror,” 69, 73
Waterborne Disease and Outbreak Surveillance System (WBDOSS), 183
Weapons of mass destruction (WMD), 21
Westphalian sovereignty, 4
Whistleblowing, 220–227
World War I, 3