

## Index

- Aaviksoo, Jaak, 39  
 Abi-Saab, Georges, 21, 29  
 ‘accumulation of events’ theory *see*  
 ‘pin-prick’ attacks  
 Afghanistan, US-led invasion (2001–),  
 123, 145  
   use of private contractors, 26  
 aggression, use of, 44  
   definition, 51, 78–9  
 Ago, Roberto (Judge), 103, 104  
 Ahmadinejad, Mahmoud, 37, 129, 291  
 Aideed, Mohamed Farrah, General, 16  
 Al Qaeda, 15, 17, 19, 123, 142, 239–40,  
 287  
 Aldrich, Richard, 126  
 Ali, Mohamed (Indonesian saboteur), 153  
 Angola, threats to the peace, 110–11  
 anticipatory self-defence, 82–93  
   against computer attacks, 88–91  
   gravity of threat, 87, 90–1  
   imminent threat, as criterion for, 87–8  
   method of delivery of threat, 87–8, 90  
   terminology, 91  
 Arab oil embargo (1973–4), 47–8, 60  
 Arab Spring revolutions (2010–), 16  
 armed attack  
   as criterion for right to self-defence,  
   76–82  
   lack of definition, 77–9  
   use of force tantamount to, 79–80  
 armed conflict(s)  
   changes in methods/technology, 139  
   changes in purpose, 23, 182–4  
   industrialisation, 22  
   influence of/on societal trends, 10  
   intent-based classification, 121,  
   130, 132–3  
   lack of statutory definition, 119  
   politicisation of vocabulary, 58–9  
   presence of, legal relevance, 117–18  
   requirement of protracted attacks,  
   130–1  
   unchanging basic nature, 29–30, 32  
   *see also* internal conflicts;  
   international conflicts; law of armed  
   conflict  
 armed force, 131–3  
   defined, 49–62  
   force amounting to, 40–9  
   lack of statutory definition, 122–3  
   required for definition of armed  
   conflict, 122–3  
 armed forces (state)  
   defined, 124  
   involvement in international  
   conflicts, 123  
   non-conflict deployment, 123–4  
 Arquilla, John, ‘The Great Cyberwar of  
 2002’, 93  
 ‘Aurora’ cyber attack *see* Idaho National  
 Laboratory  
 backdoor payloads, 89–90  
 Barkham, Jason, 64  
 ‘battlefield,’ (broad) definition of, 272  
 Baxter, Richard, 155  
 belonging, as requirement for combatant  
 status, 150–1  
 biological weapons *see* chemical/biological  
 weapons  
 Black, Jeremy, 10  
 Black Hawk incident (1993), 15–16  
 Bletchley Park, code-breaking  
 operations, 65  
 Boden, Vitek, 6, 221–2, 243–4, 285  
 Boivin, Alexandra, 210  
 Bond, James, 44, 62, 69  
 booby-traps, 258–60  
   defined, 258  
   prohibited forms, 259–60

- Boothby, William H., 254  
 booty, 266–7, 270–2  
   contrasted with seizures in occupied territory, 269–70  
   narrow definition, 270  
 Bothe, Michael, 83, 188, 190, 197–8, 199–200, 264  
 botnets, 89–90, 95, 100, 268  
 Bowett, D. W., 58  
 Bradwell nuclear plant (UK), 240–1  
 Brazil, contributions to use-of-force debate, 43–4, 47  
 Bremer, Paul, 175  
 Briand, Aristide *see* Kellogg-Briand Pact  
 Brown, Davis, 28  
 Brownlie, Ian, 46, 58–9, 62, 68–9, 73, 77, 83  
 Buckshot Yankee, Operation, 291  
 Bush, George H. W., 71  
 Bush, George W., 56  
   ‘Bush Doctrine’, 91–3
- Caffrey, Aaron, 286–7  
*Caroline* incident (1837), 84–5, 87, 92, 102  
 carrying arms openly, as condition of combatant status, 145–9  
   problems of, 148–9  
 Cassese, Antonio, 31  
 Chechnya, conflicts in, 143  
 chemical/biological weapons, 58–9, 256  
 children, 175–8  
   state obligations towards, 176–7  
   (supposed) computing abilities, 175–6, 177–8
- China  
   accused of cyber attacks, 57, 71, 100  
   cyber attack capabilities, 55–6, 82  
 CIA (Central Intelligence Agency), 6  
 civil wars *see* internal conflicts  
 civilianisation (of warfare), 25–7, 139, 178  
 civilian(s)  
   accompanying armed forces, 141, 151–2, 159, 172  
   calls for inclusion among permissible targets, 181–4  
   centrality to ‘unnecessary suffering’ principle, 254–5  
   employment by military, 159–61  
   *see also* (outsourcing)  
   facilities, military reliance on, 26–7, 74  
   feigning of status, 262–3, 264  
   forfeiting of civilian status, 139–40, 143–4  
   as human shields, 216–17  
   increasing use to augment forces, 25–6  
   negative definition, 141  
   networks, as gateways to military objectives, 201  
   objects indispensable to, 227, 243–4  
   precautionary obligations regarding, 209–19  
   protection of persons/property, 9, 159, 180–1, 195–205, 222, 227, 242  
   in occupied territory, 273–4  
   right to defend property, 172  
   *see also* civilianisation; direct participation; technology  
 Clark, Wesley, General, 192  
 Clarke, Richard, 100, 286  
 Clinton, Hillary, 56  
 ‘CNN effect’, 15  
 Code Red worm, 285–6  
 Cold War, 6  
 combatant status, 139, 178  
   controversy over, 140–1  
   disqualifications from, 150, 152–9  
   and duty of allegiance, 151  
   level of computer activity entailing, 140  
   of mercenaries, 173  
   qualifications for, 140–2, 144–51  
   statutory definition, 140–1  
   *see also* distinctive signs; lawful combatants; rebel forces; unlawful combatants; volunteer groups  
 command/control systems, 22–3  
 commanders, military/humanitarian obligations, 209–19  
   best possible intelligence, 206–7, 212  
 computer network attacks, 4–8  
   anticipatory self-defence against, 88–91  
   areas for future research, 280  
   as ‘armed attack’, 75–6, 80, 131–3, 179;  
   falling short of, 107–8  
   attribution, problems of, 3, 71, 76, 99–102, 150–1, 172, 211  
 challenges to international law, 279  
 civilian targets, 196–202  
   as classified information, 31  
   comparison with conventional weaponry, 255–6  
 contemporary debates on, 33  
 counter-attacks, 211–12, 217–19  
   *see also* (countermeasures)  
 deceptive, 261–2  
   within definition of prohibited weapons, 258–60  
   designed to appropriate property, 275–6  
   as direct participation in hostilities, 167  
   and distinction principle, 145–9  
   distinguishing features, 2, 4–5, 28, 64–74, 129  
   and dual-use technology, 194–5  
   increase in possible targets, 179, 183–4  
   as indicator of intent, 134

- on installations containing dangerous forces, 239–43
- international recognition of significance, 53–4
- knock-on effects, 66, 132–3, 179–80, 205, 207–8
- lack of specific statutory provisions, 117, 127
- legal review obligations, 260–1
- legitimate objectives, 179, 184–5, 196–202
- as means/method of warfare, 250–1, 254, 277–8
- non-lethal effects, 72–3, 74, 133–4, 137, 196–202, 213–14, 255–6, 275–6
- not defined as military action, 39–40
- physical consequences, 74, 81, 279
- precautionary issues, 210–17, 218–19
- as preparation of electronic battleground, 89–90
- and proportionality principle, 206–9
- range of aims/outcomes, 129, 196, 216
- relationship with military trends, 3–4, 21–7
- relationship with societal trends, 3–4, 11–27, 32–3
- routing through multiple hosts/countries, 262–3
- and sabotage/espionage, 152, 154–5, 157–9; as lawful ruse, 154
- scale of battlefield, 272
- shortage/inaccuracy of data on, 32
- as sole method of attack, 117, 127, 129–34, 137
- system support, 167–70
- terminology, 27–32
- territorial issues, 134–7
- UN-authorized defence to, 109, 112–13
- as use of force, 40, 41, 53–7, 58–9, 64–74, 123
- vulnerability to, 220–1 *see also* conventional attacks; cultural property; denial of service attacks; indirectness; indiscriminate attacks; intangibility; law of armed conflict; ‘pin-prick’ attacks
- computer network defence, defined, 27
- computer network operations, defined, 27–8
- computers/computer systems
  - defence of, 171
  - designation as military, 145–7
  - explosion, 259
  - generic IT support, 170–2
  - government-owned, as booty, 270
  - as legitimate targets, 147–8
  - as non-defended/demilitarised zones, 247–9
  - remote appropriation, 266–8
  - seizure, 266–70
  - in occupied territory, 2008, *see also* weapons
- contextualism, 58, 61–2
  - problems of, 62
- contractors, 159–61
  - bearing of arms, 163–4
  - coming under fire, 171
  - design/execution of computer programs, 167
  - hired by private companies, 174–5
  - nationality extended to, 174
  - salaries, 175 *see also* private military companies
- conventional attacks
  - computer network attacks as precursor to, 88–9, 104, 117, 131–2
  - computer network attacks used in conjunction with, 7–8, 75–6, 82–3, 117, 127–9
  - insufficient to count as armed attack without computer back-up, 117, 127, 134
- copying (of data), 266–7, 268–70
  - see also* unauthorised copying
- copyright *see* unauthorised copying
- Corten, Oliver, 62
- countermeasures, 3, 105–8
  - factors affecting permissibility, 101–2
  - test for justification, 107–8
- counter-terrorism, 125
- Cuba, US embargo on, 60
- cultural property, 220, 227–39, 270
  - ‘born-digital’, 228, 231–2
  - and cultural heritage, 239
  - damage/destruction, liability limited to, 234–5
  - definitions, 228–9, 230–1
  - ‘grave breaches’, 234–5
  - legal framework, 228–33
  - protective obligations, 1750; on attackers, 229, 232–3; on defenders, 232–3
  - refuges, 232
  - registration, 232
  - reproductions, 231
  - theft, pillage or misappropriation, 235–9
  - vulnerability to computer attack, 231–2, 233–9 *see also* digital heritage; digitisation; unauthorised copying
- Cultural Property Convention
  - 230–3, 260
- cyber commands, establishment of, 53–4

- cyberspace  
 applicable law, 8–10  
 as fundamentally distinct from physical space, 28, 71–2
- 'Dambusters' raid (1943), 1
- dams  
 (potential) attacks on, 240  
 special protection, 241
- databases (medical), 244–7  
 compilation, 245  
 obligation to distance from military objectives, 246–7  
 statutory protection, 245–6
- Davis-Besse nuclear plant (Ohio), 240–1
- DCS (distributed control systems), 5
- Deadhat virus, 288
- deception  
 development in line with attack advancements, 261–2  
 permissibility, 261–3
- defenders, obligations towards civilians, 217–19 *see also* cultural property
- demilitarised zones, 247–9  
 agreements as to, 249
- Democratic Republic of the Congo,  
 conflicts with neighbours, 97
- denial of service attacks, 2, 5, 15, 38–9,  
 66–7, 81, 82–3, 88–90, 98, 100–1,  
 124–5, 190, 204, 289, 290
- definition/method, 38
- legality, 149
- problems of attribution, 71
- structure of organising group, 150
- as use of force, 54–5
- Denning, Dorothy, 12
- digital heritage, 239
- digital works/records  
 undetected changes to, 233–4  
 vulnerability to computer attack, 233–5  
*see also* digital heritage; digitisation;  
 unauthorised copying
- digitisation, 12  
 of cultural property, 228, 231, 236
- Dinstein, Yoram, 10, 60, 62, 73, 84, 88,  
 103, 141–2, 144, 155, 157, 158, 175,  
 187, 188–9, 191, 194, 203, 213–14,  
 242, 247, 254–5, 272
- direct participation, civilian, 159–75, 178
- academic analysis, 161–4
- actions amounting to, 159–66
- belligerent nexus, 166
- case-by-case determination, 161
- defensive/protective, 163–4, 170–2
- definitions, 159, 162–4, 165–6, 168
- direct application to violence, criterion of, 162–3
- direct causation, criterion of, 165–6, 168
- electronic interference as, 167
- and geographic proximity, 164
- Red Cross guidelines, 143–4, 151, 161,  
 165–6, 167, 170–1
- risks to non-participant civilians, 163
- statutory provisions, 161
- surrender of civilian status, 139–40
- threshold of harm, 165, 167, 170–1
- discrimination, principle of, 256
- distinction, principle of, 137, 139–40,  
 145–9, 228, 280
- controversy over, 181–4
- statutory provisions, 180–1
- distinguishing marks, wearing of,  
 145–9, 157
- problems of, 148–9 *see also* naval warfare
- DNS root servers, 204, 287, 288–9
- Dogger Bank Incident* (1904), 120, 133
- Doomjuice virus, 288
- Dörmann, Knut, 197–8, 206
- Doswald-Beck, Louise, 125, 133
- Downey, William, 267
- dual-use technology, 26–7, 193–5,  
 204, 216–17
- and proportionality principle,  
 208–9
- Dunlap, Charles, 181–2, 189
- East Timor, 110  
 location of government website servers,  
 72, 276, 284
- Eastern African Submarine Cable  
 System, 186
- Echelon (listening post system), 158
- economic coercion *see under* use of force
- effects-based operations, 24–5, 183
- Egypt  
 military threats to neighbours, 20
- role in 1967 war, 85–6
- shutdown of communications, 111,  
 112, 186
- El Salvador, civil war in, 137
- Electronic Disturbance Theatre, 108,  
 111, 283–4
- Eligible Receiver, 281–2
- emails, designed to wreck target  
 computer, 264
- EMP (electromagnetic pulse) technology,  
 4, 261
- ENMOD Convention, 224–5
- environment, 221–2  
 case law, 226
- general rules applying to, 226–7
- specific protective measures, 222–5
- restricted ambit, 223–4
- war crimes, 226–7 *see also* ENMOD

- Convention: environmental modification techniques
- environmental modification techniques defined, 224–5
- hostile manipulation, 225
- espionage, 151–2, 156–9
  - activities short of attack, 156
  - capture of operatives, 157
  - definition, 156
  - legality, 157
  - location, 152, 157–8
  - operatives' liability, 158–9
  - penetration of enemy networks, 158
- Estonia, denial of service attacks (2007), 2, 5, 15, 38–9, 54, 66–7, 71, 81, 88, 124–5, 289
  - difficulty of attribution, 100
  - international response, 54, 57
  - level of impact, 190
  - youth group involvement, 176
- Ethiopia/Eritrea Claims Commission, 120, 276–7
- European Union, 19
- Falun Gong movement, 100
- 'Farewell Dossier' incident, 6, 38, 57, 72, 250–1, 281
- Farquharson, John, 269
- feasibility, criterion of, 217–18
  - and child soldiers, 176–7
  - and precautionary measures, 211, 214–15, 218
- fibre-optic cables, 186, 267
- Flesche, Alfred, 159
- Flick, Friedrich, 238, 275
- 'Floodnet' attacks, 108
- force *see* armed force; use of force
- foreign exchange markets, 18
- Franck, Thomas, 86, 97–8
- Frowein, Jochen, 110
- Georgia, denial of service attacks (2008), 2, 8, 54–5, 66–7, 71, 81, 82–3, 110, 111, 124–5, 150–1, 172, 176, 290
  - co-ordination with conventional attacks, 89, 98, 101
- globalisation, 17–20
  - early eras of, 17–18
  - economic, 18
  - impact on causes of conflict, 17–18
- Goering, Hermann, 238
- Goloskokov, Konstantin, 176
- Gordon, Edward, 45
- GPS (Global Positioning Systems), 194–5, 218
  - spoofing, 194–5
- Gray, Christine, 62, 83, 86, 91, 97
- Greenburg, Lawrence T., 133
- Greenwood, Christopher, 84–5, 87–8, 90–1, 92, 118, 120, 207, 214, 216, 218, 252, 253, 254–5, 257–8
- guerrilla fighters, 148–9, 150, 155
- guided missiles, 84
- Gulf War (1990–1), 26, 194, 207–8, 214, 216
  - environmental impact, 221, 222
  - use of earthmovers, 254
- 'hack back' measures, 105
- hacker collectives, 15
- Haiti, threats to peace/rights violations, 110
- Hanseman, Robert G., 126–7
- Happold, Matthew, 177–8
- Hargrove, John, 106
- Harris, David, 43
- Haslam, Emily, 126
- health, protective measures, 223
- Held, David, 18–19
- Higgins, Judge (later Baroness), 30, 87, 99
- hospitals, 244
  - hospital ships, 247
- Houston Port Authority, cyber-attack on (2001), 286–7
- Hulse, Christopher, Ambassador, 211
- humanitarian law, principles/applicability, 128, 132, 133–4, 179, 252–8
- ICBL (International Campaign to Ban Landmines), 19
- ICC (International Criminal Court), 226–7
- ICJ (International Court of Justice), 48–53, 252 *see also* Table of Cases
- ICTY (International Criminal Tribunal for the former Yugoslavia), 122, 130, 151, 209, 237 *see also* Table of Cases
- Idaho National Laboratory, 6, 289
- IMF (International Monetary Fund), 19
- indirectness (of computer network attacks), 65–7
  - as constituting use of force, 66
  - use of unwilling agents, 66–7
- indiscriminate attacks, 202–5, 211
  - defined, 204
  - limits of definition, 256–7
  - prohibition, 202–5
  - weaponry, 256–7
- individual combatants
  - distinguished from civilian population, 148
  - prohibition on independent activity, 145
- Indonesia, 284
- industrial control systems, targeting of, 37–8

- inflammable bullets, 253
- information  
 economies based on, 189–90  
 increased access to, 15–16  
 permissible means of obtaining, 156  
 property rights over, 268  
 quantity, 13–14  
 range of definitions, 4–5  
 society, 220–1  
 ubiquity, 12–13
- information revolution, 10–17  
 and globalisation, 17–20  
 and organisational change, 16–17, 24–5  
 and societal change, 14–16, 29
- information warfare, 27, 59, 73, 126, 133
- insignia *see* distinctive signs
- installations containing dangerous  
 forces, 239–43  
 military objectives in the vicinity of,  
 241–3  
 special protection, 241 *see also* nuclear  
 facilities
- intangibility, 67–70  
 of damage, 67  
 of targets, 67–8
- intangible assets  
 applicability of property law, 265–6  
 damage to, 73  
 increasing importance, 280  
 monetary value, 21
- intellectual property, 20–1, 68, 270
- intent  
 role in definition of armed attack,  
 120–1, 132–3, 134, 279  
 role in military advantage, 193
- internal conflicts, 118–19, 121–2, 134–5  
 applicability of humanitarian law, 253  
 applicability of perfidy, 263  
 and combatant status, 142  
 problems of definition, 124–6
- international conflicts, 118–21  
 regulatory ambiguities, 9–10  
 requirement of state armed forces’  
 involvement, 123–6
- internet  
 access, as fundamental human right, 11  
 shutdown, as response to civil unrest,  
 186–7 *see also* DNS servers; IP  
 addresses
- Intocchia, Gregory F., 168
- IP addresses, 146–7  
 designation as military networks,  
 145–7, 246–7  
 problems of, 146–7
- Ipsen, Knut, 168
- Iran  
 attacks on US embassy, 52  
 damage to nuclear facilities, 2, 37–8, 57,  
 81–2, 129–31, 241, 291–2  
 nuclear programme, threats posed by,  
 112–13  
 US claims against, 103
- Iran Ajr*, attack on, 121
- Iraq  
 disabling of power systems (1991), 194,  
 208, 242  
 Israeli attacks on (1981), 87–8  
 no-fly zone, 84  
 projected attacks on banking  
 system, 205  
 Tiger Song air defence network, 208  
*see also* Gulf War; Iraq War; Kuwait
- Iraq War (2003– ), 82, 218–19  
 and civilian hackers, 145, 178  
 use of private contractors, 26, 160,  
 163–4, 171, 175
- isolated incidents, (non-)definable as  
 armed conflict, 131
- Israel, 182  
 (alleged) complicity in Stuxnet, 37–8  
 attacks on Iraq (1981), 87–8  
 attacks on Lebanon (2006), 99  
 bombing of Syria (2007), 7, 13, 73, 76,  
 82, 88, 132, 261–2, 289–90  
 claims of self-defence, 94  
*Wall* case, 96–7
- Israeli–Arab War (1967), 85–6
- Jacobson, Mark, 69
- Jennings, Judge, 78
- Jensen, Eric, 105
- JSTARS system, 169
- jus ad bellum* (right to wage war), 2–3,  
 279–80
- jus in bello* (laws of war), 3, 280
- Kalshoven, Frits, 213, 215
- Kellogg-Briand Pact, 45–6, 77
- Kelsen, Hans, 83
- KGB, theft of Western technology, 6
- Khomeini, Ruhollah, Ayatollah, 52
- knowledge economy, 20–1
- Kosovo, NATO campaign in, 23, 183, 191,  
 192, 196, 285  
 data storage, 262
- Ku, Raymond, 8–9
- Kuwait, Iraq invasion (1990), 103
- LaRae-Perez, Cassandra, 59–60
- law of armed conflict, 3  
 anomalies, 202  
 applicability to computer network  
 attacks, 8–27, 28–31, 119–20, 126–34,  
 137–8, 252, 279

- balancing of military/humanitarian needs, 10–11, 30–1, 260
- difficulty of application, 26–7
- general principles, 29–31, 33, 222, 252–8
- geographical scope, 135
- incidents on borderline of, 120–1, 131
- limitations on weaponry, 251–2
- policy-oriented approach, 31
- requirement of armed force, 122–3, 131–3
- scope of application, 117–18
- theoretical debates, 9, 126–7, 128–9
- threshold for application, 118–22
  - see also* combatant status
- lawful combatants
  - determination of status, 141–3
  - privileges, 142
- League of Nations, Covenant, 45, 77
- Lebanon, conflicts in, 99, 104–5
  - environmental damage, 221
- letter bombs, 259–60
- Liberia, threats to peace/rights violations, 110
- Liberty*, USS, attack on (1967), 120, 133
- Libicki, Martin, 27
- Libya, shutdown of communications, 111
- locus (of computer attacks), 70–2, 134–7
- logic bombs, 258
- long-range missiles, 256
- Lynn, William, III, 56, 93, 291
  
- Maguire, Martin, 284
- malware, 5, 89–90 *see also* rootkit
  - malware; viruses; worms
- Martens Clause, 28, 127–8, 202, 257–8
  - applicability to computer attacks, 257–8
- McChrystal, Stanley, General, 17
- McConnell, Michael, Admiral, 271
- McDougal, Myers, 61
- McGrew, Anthony, 18–19
- McLuhan, Marshall, 14
- means of warfare *see* methods/means of warfare
- medical units, 244–7
  - aircraft, 246
  - obligation to distance from military objectives, 246
  - specific protections, 245
  - see also* databases
- Melzer, Nils, 121, 166
- mercenaries, 172–5
  - criminal status, 175
  - definition, 173–4
  - as lawful combatants, 173
  - withdrawal of combatant status, 173
    - see also* private military companies
- methods/means of warfare, 277–8
  - legal review, 260–1
  - prohibition of those causing unnecessary suffering, 253–6
- Michelangelo (Buonarrotti), 231
- military advantage
  - balanced against suffering, 254–5
  - as criterion of military objectives, 190–3
  - defined, 191–3, 201
- military objectives
  - contribution to military action, 188–90
  - definition, 184–94, 197–8
  - breadth of, 188–90
  - gateways to, 201
  - legitimate, 179, 180–1
  - location, 185–7
  - nature, 185
  - purpose/use, 187
  - verification of targets as, 211–12
  - in the vicinity of dangerous installations, 241–3
- military operations
  - breadth of definition, 199–201, 209–10
  - distinguished from attacks, 198–202
- militia(s) *see* volunteer groups
- Milosevic, Slobodan, 23, 183, 191, 196
- minesweepers, 171
- mistaken identity, 120, 133, 134
- Moir, Lindsay, 84, 97
- money transfers, electronic, 21
- Moonlight Maze incident, 284–5
- Moore, Joe Wesley, 168
- Mountain View surveillance program, 240, 286
- Mubarak, Hosni, President, 20, 186
- multi-national corporations, role in global economy, 18
- murder, law of, 70
- Myanmar, shutdown of communications, 111, 186
- Mydoom virus, 288
  
- Nashi (Russian youth movement), 176
- Nasser, Gamal Abdel, President, 85–6
- Natanz nuclear facility *see* Iran, damage to nuclear facilities
- national liberation, wars of, 136, 142–3, 149
- NATO (North Atlantic Treaty Organization)
  - cyber security policy, 57
  - operations in former Yugoslavia, 49–50, 183, 191, 192, 196, 207–8, 212
  - response to Estonian cyber attacks, 39, 54
  - Treaty provisions, 46–7, 77
- naval warfare, flying of flags, 146, 262

## 328 INDEX

- necessity, principle of, 102–3, 265, 273–4  
 and damage to cultural property, 234  
 environmental application, 226
- Nepal, shutdown of communications, 186
- network-centric warfare, 24
- neutralisation, 197–8, 216
- New Haven school, 61–2
- New Zealand, 149  
 contributions to use-of-force debate, 44  
 financial law, 21  
 intellectual property law, 68  
 internet connections, 186
- NGOs (non-governmental organisations), 18–19
- Nicaragua  
 claims of US coercion, 47, 48, 50–3  
 incursions into neighbouring territory, 94, 105–6
- non-defended localities, prohibition of attacks on, 247–8
- non-intervention, policy of, 50
- non-state actors  
 combatant status, 142–3  
 increasing power/influence, 14–15, 16–17, 18–19  
 international recognition, 125–6  
 self-defence against, 95–9 *see also* rebel forces; volunteer groups
- nuclear facilities  
 (potential) attacks on, 7, 240–1  
 special protection, 241
- nuclear weapons, use of, 128–9
- Nuremberg Military Tribunal (1945), 237–8, 265–6, 267
- OAS (Organization of American States), 46–7
- Obama, Barack, 92–3
- occupied territory, 142–3, 149  
 guerrilla operations, 148–9  
 protection of property, 233  
 seizure of property, 269–70, 272–4
- Oeter, Stefan, 182, 189, 191, 209
- oil well fires, 221
- Oppenheim, Lassa, 23
- organisation, required for combatant status, 150
- Orwell, George, 233  
 1984, 233
- Ottawa Convention 19, 270
- outsourcing (of military operations), 25–6, 139, 159–61, 168–70, 276  
 reasons for, 160
- Papua New Guinea, internal unrest, 174
- Parks, W. Hays, 162–3, 168–9
- perfidy, 261, 263–4, 278  
 defined, 263  
 limits of prohibition, 264  
 purpose of prohibition, 263
- Pictet, Jean, 119, 122, 123, 130
- pillage, 236, 237, 274–6, 278  
 defined, 274  
 of digital property, 274–6  
 statutory prohibition, 265
- ‘pin-prick’ attacks, 75, 93–5  
 case law, 94–5  
 self-defence against, 93–5
- plunder, 274–6, 278  
 distinguished from pillage, 275–6
- positivism, 30, 58–61, 62
- precautionary measures, 209–17
- Predator drones, 123
- prisoners of war  
 disqualifications from status of, 144–5, 151–3, 157, 173  
 entitlement to status of, 141–2, 144–51  
 taking of, relevance to legal status of conflict, 121
- private military companies, 163–4, 174–5
- property, 265–77, 278  
 enemy-owned, in belligerent territory, 276  
 permissible categories for seizure, 271–2  
 private: in belligerent territory, 276–7  
 duty to respect, 265  
 prohibition on destruction, 273–4  
 state/private, distinction between, 270–1 *see also* booty; civilians; seizure
- proportionality principle, 98–9, 102–4, 170, 205–9  
 environmental application, 226  
 statutory provisions, 205–6  
 and unnecessary suffering, 254–5
- public services, computer regulation, 12–13
- Queensland (Australia), attack on water supply, 6, 221–2, 285
- Radio Television Serbia (RTS), attack on (1999), 192
- Randelzhofer, Albrecht, 43
- Reagan, Ronald, 121
- rebels, combatant status, 143
- Red Cross, International Committee of, 119, 143–4, 165–6  
 misuse of symbols, 264–5 *see also* direct participation
- Reisman, Michael, 61–2
- ‘resource wars’, 182
- responsible command, as condition of combatant status, 145
- Roach, J. Ashley, 247



- Robertson, Horace B., 82  
 Rogers, A. P. V., 162, 192–3, 209  
 Roosevelt Dam, Arizona, 1–2, 6, 240, 282–3  
 rootkit malware, 259–60  
 Russia  
   accusations/denials of involvement in cyber-attacks, 39, 54–5, 98, 100, 110, 150–1, 284–5, 289, 290  
   draft resolution on communications technology, 258  
   military conflict with Georgia, 89, 98, 101  
   (planned) response to cyber-attacks, 57  
 Rwanda, threats to peace/rights violations, 110  
 sabotage, 151–5, 264  
   and acts of deception, 155  
   computer network attacks amounting to, 154–5  
   by non-uniformed operatives, 152–4  
   physical presence in territory, 152–3, 154–5  
 Sandline International (private military company), 174  
 satellites, 272  
   navigation systems, 13  
 SCADA (Supervisory Control and Data Acquisition) systems, 5, 220, 221–2  
 Schmitt, Michael, 23, 25, 33, 42, 47, 60–1, 62–4, 68, 79, 80, 124, 127, 132, 134, 142, 144, 162–4, 166, 169–70, 171, 198–200, 202, 206, 208, 209, 212, 213, 244, 262  
 Schwebel, Judge, 78  
 Scott, Roger D., 127  
 seizure, 266–70  
   by copying, 268–70  
   definitions, 267–8  
   ‘firm possession’ criterion, 267–8  
   property subject to, 271–2, 276–7  
 self-defence, right of, 3, 75–108, 279–80  
   appropriate time for exercising, 83–5  
   case law, 76–80, 85, 96–7  
   doctrinal divide, 113  
   against non-state actors, 95–9  
   proposed limitations, 113  
   scope, 75–6  
   state practice, 85–8, 97–8  
   statutory provisions, 76  
   ‘without undue delay’ principle, 103  
   *see also* anticipatory self-defence  
 September 11 attacks (2001), 103, 147  
 Sharp, Walter, 81  
 Shulman, Mark, 126  
 Sierra Leone, 110, 177, 275  
 Simma, Bruno, Judge, 79, 106–7  
 Singapore, bank sabotage, 153  
 Singer, Peter, 164  
 skirmishes *see* isolated incidents  
 Slammer/Sapphire worm, 250  
 Smith, Sir Rupert, General, 23  
 ‘Solar Sunrise’ attacks, 71, 282  
 Solf, Waldemar, 137  
 Solferino cycle, 246  
 Somalia, threats to peace/rights violations, 110  
 Somalia, US operations in, 15–16  
 South Ossetia, conflict over *see* Georgia; Russia  
 Southern Arab Federation, 94  
 space, conflicts based in, 273  
 special protection, 220–1  
 spy satellites, 69  
 Sri Lanka, 182  
 St Petersburg Declaration (1868), 24–5, 29, 202, 251–2, 260  
 Stark, USS, attack on (1987), 120, 133  
 state(s)  
   as basis of international law, 25  
   citizens’ relationships with, 15–16  
   complicity in non-state initiatives, 96  
   difficulty of establishing, 100–1  
   interdependence, 19–20  
   obligation to review weaponry/means of war, 260–1  
   obligations to citizens, 140  
   reduction in powers, 18, 143  
   vulnerability to cyber-attack, 1–2, 6–7  
 stock exchanges, hacking of, 41  
 Storm worm, 251, 256  
 Stuxnet worm, 2, 5, 13, 37–8, 53–4, 57, 70, 81–2, 112–13, 129–31, 133, 201, 203–4, 241, 256–7, 291–2  
   components, 251  
   international response, 57  
   origins, 130  
 Suez Crisis (1956), 190  
 superfluous injury *see* unnecessary suffering  
 support staff, as direct participants, 167–70  
 ‘Suter’ technology, 7, 261–2, 287–8  
 Swiney, Gabriel, 182  
 symbols, internationally recognised, misuse of, 259, 264–5  
 Syria  
   Israeli attacks on (2007), 7, 13, 73, 76, 82, 88, 132, 289–90  
   shooting down of US aircraft (1983), 121

- Taiwan, information-based economy, 189–90  
 Taliban, 17  
 target area bombing, 204, 216–17  
 targets, choice of, 216–17 *see also* military objectives; target area bombing  
 technology  
   developments in, 21–2, 139, 178, 257–8  
   integration of civil and military, 208–9, 218–19  
 telecommunications networks  
   seizure in occupied territory, 272–3  
   targeting in computer attacks, 186–7, 192  
 territory, 134–7  
   control over, 136–7  
   effects-based definition, 135  
   and espionage, 152, 157–8  
   irrelevance to cultural property protection, 234  
   and sabotage, 152–3, 154–5  
 terrorism, applicability of law of armed conflict to, 125 *see also* counter-terrorism  
 Thames Barrier (London), 225  
 threats to the peace, 44  
   computer attacks amounting to, 110  
 Timor Leste *see* East Timor  
 ‘Titan Rain’ attacks, 71, 156, 236, 288  
 Toffler, Alvin/Heidi, 10, 20, 22  
 Trans-Siberian Pipeline *see* ‘Farewell Dossier’ incident  
 transnational armed groups, emergence of, 25  
 treaty interpretation, principles of, 41  
 Trojans, 168, 250  
 truck drivers, combatant status, 162, 163  
 Turing, Alan, 65  
 Uganda, conflicts with neighbours, 97  
 UN Charter, provisions on use of force, 40–6, 58–60, 76  
   historical background, 45–6  
   and self-defence, 83–4, 95–7  
 unauthorised copying (of digital works), 236–9  
   criminal classification, 237–8  
   (potential) scale of operations, 236  
 uniforms *see* distinctive signs  
 United Kingdom  
   intellectual property law, 68  
   mine-sweeping operations, 49  
   MoD satellite hack, 285  
   national security strategy, 2  
   oil supply, 222  
   stance on feasibility, 214–15  
 United Nations  
   collective security regime, 3, 109–13  
   Declaration on Friendly Relations, 47–9, 50–1  
   Declaration on the Non-Use of Force, 48–9  
   responses to states’ claims of self-defence, 94 *see also* UN Charter; use of force  
 United States, 32  
   Air Force maintenance, 169  
   Civil War weaponry, discovery/ownership, 267  
   complaints of economic coercion, 60  
   concerns over Kosovo operations, 196  
   criticisms of post-9/11 conduct, 103  
   cyber attack plans, 205  
   definition of military objectives, 181–2, 188–90  
   Department of Transport, DoS attack on, 100  
   isolated military incidents, 120–1  
   Joint Publication on Information Operations, 27–8  
   medical information system, 245  
   military networks, as legitimate targets, 170  
   military use of civilian networks, 187, 218, 271  
   national security strategy, 2, 91–3  
   network invasion capabilities, 7  
   (planned) response to cyber attacks, 56, 57, 108, 111  
   plans for telecommunications shutdown, 186–7  
   relations with neighbours *see* Cuba; Nicaragua  
   self-defence strategy/measures, 91–3, 101–2, 103  
   Tehran embassy *see* Iran; US Department of Defense  
   unlawful combatants, 141–2  
   saboteurs/spies as, 151–2  
 unnecessary suffering, 252–6, 280  
   balancing requirements, 254–5  
   defined, 253  
   weapons relevant to, 253–4  
 US Department of Defense, 71, 214  
   classification policy, 31  
   targeting by hackers, 147, 283–4, 291  
   terminology, 27–8, 168  
 use of force  
   attempts at clarification, 46–9  
   balancing of rights/obligations, 9  
   border violations, 70–1, 93–4  
   broad interpretation, 49–53  
   case law, 40, 48–53  
   categories of permissibility, 61–2

- collective, UNSC authorisation, 42, 75, 76, 109–13
- defining factors, 63–4
- economic/political coercion *see as*, 41, 43–4, 47–9, 52, 59–60
- ‘encouragement’ of, 51–2
- as evolving concept, 52–3
- fatality/property damage, as defining factor, 73, 75
- grave vs. less-grave forms, 50–1, 79, 105–7
- indirect assistance as, 65–6
- problems of definition, 39–49, 65
- prohibition, 2–3, 40
- result-oriented approach, 59–61, 62–3, 68–9, 72–4, 80, 279
- state practice, 53–7
- theoretical approaches, 58–62  
*see also* UN Charter
- Vienna Convention on Diplomatic Immunity, 52
- Vietnam War (1955–75), 222
- viruses, 154, 168, 203–4, 288
  - cost, 154
  - specific targets, 203
- volunteer groups, combatant status, 142–4
- war(fare) *see* armed conflict
- water supplies
  - poisoning, 256
  - vulnerability to attack, 242, 243–4  
*see also* Queensland
- Watts, Sean, 140–1, 145, 160–1
- weapons
  - anti-personnel vs. anti-materiel, 253–4
  - choice of, 212–15
  - civilian maintenance, 160
  - comparison between systems, 255–6
  - computer systems as, 168, 253–4
  - computerised, nature of, 70
  - defined, 69
  - held in reserve, 214–15
  - indiscriminate, 256–7
  - intangible, 67, 68–70
  - law of, 251–61, 277–8
  - legal reviews, 260–1
  - specific prohibitions, 258–60
- Webster, Daniel, 84, 102
- Wedgwood, Ruth, 206
- Westphalia, Treaty of (1648), 25
- World Bank, 19, 20
- World Trade Center attacks  
*see* September 11
- World War II
  - bombing campaigns, 197
  - intelligence methods, 211  
*see also* ‘Dambusters’ raid
- worms, 203–4, 285–6
  - mass-mailing, 288
  - as means/method of attack, 250–1
- worship, places of, 229
- WTO (World Trade Organization), 19
- Xinhua (news agency), 56
- Yugoslavia (former) *see* ICTY; Kosovo; NATO