
Index

- 9/11 attacks 45, 198–9, 224–5
 - conflict characterization impacts 257–8
 - counter-actions, self-defense justification 231
- 60-day clock 263–5
- absolute necessity 159, 243–4
- accountability
 - AWS, of 357–65
 - accidents 361–2
 - accuracy parameters 363, 435–6
 - command responsibility 360–61, 369, 413–15, 432–6, 440–41
 - criminal responsibility 387, 392–4
 - default settings 437–8
 - human operator role 358–63, 365, 369, 459–60
 - international law, implications 385–6
 - knowledge 359–60
 - meaningful human control 391, 401–4, 431–40
 - output reviews 435–6
 - predictability 388–9, 392–3, 459
 - programmer or manufacturer error 363–4, 392
 - programming limitations 351–2, 364–5
 - recklessness, and 362–3, 386
 - state responsibility, and 386–8
 - target identification capability, and 357–8
 - updates 435–6
 - war crimes, for 357–8, 365
 - wilful intention 359–60
 - command responsibility 360–61, 369, 414–15, 432–6, 440–41
 - command and control arrangements 365
 - international law applicability 393
- dynamic diligence standard 441–2
 - criteria 406–7
 - dynamic assessments 434–6
 - dynamic parameters 436–40
 - flexibility requirement 407
 - human-machine interfaces 432–4
 - IHL compliance assessments, and 406–7, 431–40
 - military command structure, and 406
- limitations 167
- obligations
 - armed conflict, during 163–4, 167
 - human rights law, under 160–67, 178
 - IHL, under 160, 162–8
 - investigations 164–5, 167, 178
 - remote warfare, in 160, 168, 184
 - transparency, and 163
- Afghanistan
 - armed conflict
 - US interpretation 115–17
 - use of force, justification 198–9
 - drone warfare 68–9
- aggression
 - definition 199–200
 - pre-stationed forces, by 200
- Akerson, David 344–5
- Alston, Philip 115, 167
- armed attack
 - civilian distinction requirement 203
 - cyber attacks, whether 280–84, 287–8
 - definition 195–8

- dual-use infrastructure 203
- information operations, as 196–7
- interpretation 196–7, 451–2
- non-state actors, by 198–9, 256
- self-defense, as 198–9, 280
- use of force, difference from 195–8
- armed conflict, generally
 - see also* international armed conflict; non-international armed conflict
 - accountability obligations 163–4, 166–8
 - conduct of hostilities rules 173–5, 184, 253
 - cyber attacks
 - activities below threshold 287–94
 - law applicability to 121, 324–5, 330–31
 - role in 75–6, 274, 278, 324–5
 - unwitting involvement 75–6
 - definition 92–3, 110–13, 252–4
 - ambiguity 201–2
 - evolution of 110, 111–13, 119, 131–2
 - internal disturbances 201, 254–6
 - self-defense, and 115–16, 172–3
 - transnational armed conflict 257–8
 - US approach 115–17
 - use of force 81
 - distinction, principle of 52–6, 408–9
 - drone warfare, and
 - consent requirement 98–9, 313–14, 318–19
 - counter-terrorism justification 226–30
 - determination criteria 23, 97–107
 - human rights law, applicability 104–7, 315–16
 - international armed conflict, whether 97–100
 - interstate requirement 99–100
 - law, applicability to 120, 314–15, 330–31
 - legal challenges 318–21, 331
 - non-international armed conflict, whether 100–104
 - targeted killings 114–20, 225–44
 - geographical scope
 - challenges 107–9
 - criterion for 90–91
 - definition 86–90, 92
 - expansion 80–81, 89–90
 - judicial interpretation 91–5, 118–19
 - nexus approach 93–5
 - origin of attack, and 96
 - remote warfare, applicability 79–81, 89–90, 319–20
 - synonyms 87–90
 - territorial interpretation 93–5
 - human rights law, and
 - applicability 104–7, 315–16
 - law enforcement role 172–5, 179, 184–5
 - international humanitarian law, and
 - accountability, role of 124–5, 160, 162–8
 - applicability 50–51, 81, 84–5, 110–13
 - challenges 107–8
 - chivalric warfare principles 42–4
 - definition, importance 86–8
 - human rights law applicability 104–7
 - protracted armed violence 81, 100–101, 108, 201–2
 - temporal scope 119, 179
 - thresholds
 - armed forces utilization, and 201
 - exploitation 201
 - gaps 198
 - information operations 202–3
 - internal disturbances 201, 254–6
 - interpretation 201–3, 202, 253–4
 - lowering, implications of 120, 125, 130, 446–56, 478
 - violence beneath 201, 253–4
 - transnational armed conflict 257–8
 - transparency obligations 163–4, 166–8

- armed force
 - see also* use of force
 - definition 195
- artificial intelligence
 - bayesian networks 417–19
 - dehumanizing effect of 374
 - development of 140–41
 - machine learning 415–20
 - pattern recognition 422–6
 - proportionality, understanding 352–3
 - remoteness, and 138–9
- asymmetrical risk
 - historical development 18–21
 - new technology implications for 460–64
- reduction
 - AWS 17, 33–5, 399–400
 - chivalric warfare, conflicts with 42–8
 - costs reduction, and 41–2
 - cyber attacks 16–17, 27–33, 312
 - defense incentive or disincentive, whether 37–42, 48–9
 - drones 22–7, 66–7, 248–9, 260–61
 - generally 35–6, 48–9
 - implications 36–7, 48–9
 - international law conflicts, and 40–41
 - jus ad bellum violations, and 36–42
 - negative impacts 44
 - number of attacks, influences on 37–8, 48–9
 - purpose 48–9
 - reputation, and 37–8
 - trends 16–17
- autonomous weapons systems
 - accountability
 - accidents 361–2
 - accuracy parameters 363, 435–6
 - command responsibility 360–61, 369, 414–15, 440–41
 - criminal responsibility 387, 392–4
 - default settings 437–8
 - human operator role 358–63, 365, 369, 459–60
 - international law, implications 385–6
 - knowledge 359–60
 - meaningful human control 391, 401–4, 431–40
 - output reviews 435–6
 - predictability 388–9, 392–3, 459
 - programmer or manufacturer error 363–4, 392
 - programming limitations 351–2, 364–5
 - recklessness, and 362–3, 386
 - state responsibility, and 386–8
 - target identification capability, and 357–8
 - updates 435–6
 - war crimes, for 357–8, 365
 - willful intention 359–60
- attitudes to 405–6, 443–4, 454
- benefits 372–4, 405–6
- characterization 1–2, 130–31
 - autonomous vs. automated 136–7, 140–41, 376
 - exclusions 136
 - human counterpart, comparison with 342–3
 - human role, and 136–8, 375–6
 - offensive vs. defensive 344–5
 - semi-autonomous 135–6, 140
 - types 135–8
- Chinese policy 144
- criticisms 373–4, 406
- definition 123, 135–7, 339, 375–7
- dehumanization implications 374
- development 336–7, 368, 371
 - concerns 336–7, 372
 - implications 122–3
 - scope of 371–2
 - trends 372
- disadvantages 373–4
- distinction, principle of 67–71, 336, 342, 395–6
- dynamic diligence standard 441–2
 - criteria 406–7
 - dynamic assessments 434–6
 - dynamic parameters 436–40

- flexibility requirement 407
- human-machine interfaces 432–4
- IHL compliance assessments, and 406–7, 431–40
- military command structure, and 406
- ethical concerns 366–8, 373–4
 - debate, focus of 372
- human rights law, and
 - dignity, principle of 152, 169–70, 184, 400–401
 - enforcement role 134
 - extraterritorial jurisdiction, and 155–6, 172
 - human responsibility, and 170
 - legality under 178–83
 - peacetime use of 171–5
 - right to life 149, 152–3
- human supervision, and 135–7, 432–4
- IHL, applicability 122–5, 369, 469–70
 - ability to comply, and 394–9
 - accountability, and 124–5, 160–68
 - challenges for 125, 383–90
- in-the-loop weapons 136, 353–4, 377
- international law, implications for
 - ability to comply 394–9
 - accountability 124–5, 160–68, 385–6
 - generally 383–4
 - state responsibility 386–90
- lethal autonomous weapons
 - armed conflict threshold impacts 120, 130, 446–56
 - asymmetric warfare impacts 460–64
 - compliance-based approach 468–70
 - concerns 445–7
 - cost vs. risk 41–2, 367, 455–6, 465
 - definition 444
 - national policy development, need for 471–3
 - proliferation implications 464–6
 - UN expert consultations 144–5, 445–7, 467–8
 - unintended engagements 456–60
 - US policy on 142–3, 368–9, 371–2, 434, 467–78
 - use of force, attitudes to 120, 130, 447–56
- objections to 344
- on-the-loop weapons 136, 353–4, 377
- operating procedures
 - artificial intelligence 138–41
 - cognitive flaws 421–2
 - decision making 420–22
 - decision trees 428–30
 - errors 415–16, 419, 421–2
 - human bias, and 421–2
 - human-machine interface 432–4
 - interpretability, and 428–30
 - limitations 430–31
 - machine learning 415–20
 - movement actions 426–7
 - pattern recognition 422–6
 - probability calculations 416–20
 - validation 416
- outside-the-loop weapons 354, 377–8
- precautionary principle
 - attacks on other AWS 131, 345–6
 - cancellation protocols 354–5, 388
 - challenges 67–71, 327, 341–2
 - choice of options, and 355–6
 - collateral damage, and 340–41, 350–54
 - decisions, compared with human role 33–4, 123–5, 341–3, 345–6
 - feasibility of 328–9, 349, 398
 - human vs. computer, comparison 33–4, 123–5, 341–3, 345–6
 - limitations, programming 351–2, 364–5
 - remoteness, and 349–50
 - target identification 67–71, 336, 344–8
- proportionality, and 344–5, 350–54, 396–7
- purpose 15, 17, 33–4, 379

- remoteness concept, and 138–9
- risk
 - asymmetrical risk 17
 - civilians, to 35
 - reciprocal risk, influences on 17
 - reduction impacts 33–4, 399–400
- robotic infantry devices 34–5
- Russian policy 144
- state responsibility
 - accountability 386–8
 - attribution 386
 - cancellation protocols 388
 - criminal responsibility 388, 392–4
 - due diligence 388–9
 - liability, and 389–91
 - predictability, and 388–9, 392–3
 - recklessness and negligence, and 386–9
 - strict liability 389–91
- surrender, recognition of 348–9
- Swiss policy proposals 468–70
- targeting, autonomous 33–4
 - accountability, and 124–5
 - benefits 34
 - criticism 344
 - law, applicability to 123–4
- targeting, generally
 - accuracy 344–5
 - challenges 67–71, 327, 341–2
 - distinction, principle of, and 67–71, 336, 342, 395–6
 - human vs. computer, by 33–4, 123–5, 341–3, 345–6
 - nature-location-use-purpose test 59–60
 - objects 345–6
 - obligations 341–9
 - other AWS 131, 345–6
 - persons, direct participation 346–8
 - proportionality, and 344–5, 350–54, 396–7
- types 135–6
- UK policy on 143, 471
- unintended engagements 456–60
- US policy on 142–3, 368–9, 371–2, 434, 467–78
- use trends
 - fully-autonomous systems 140–41
 - generally 139–40, 465
 - law enforcement and security, in 145–8
 - semi-autonomous systems 140
- autonomy
 - definition 377–8
 - development implications 376, 385
 - interpretation challenges 378
 - meaningful human control 391, 401–4, 431–40
 - three-step test 377–8
- Backstrom, Alan 345–6
- Bates, E.S. 222
- battlefield areas 87–9
 - combat activities in vicinity of 102–4
- bayesian networks 417–19
- Biontino, Michael 446–7
- Blank, Laurie 66
- Boelaert-Suominen, Sonja 112
- Boothby, William 121–2, 130, 346
- Bothe, Michael 62
- botnets 75–6
- Breedlove, Philip 196
- Brennan, John 115–16
- Brenner, Joel 279
- Cameron, David 226–30, 238–40
- Campaign to Ban Killer Robots 150, 373, 445, 467
- Canning, John S. 345
- cannons 19–20
- China
 - AWS policy development 144
- chivalric warfare 42–8, 318
- civilians
 - identification
 - combatants, distinction from 74–5, 207–9
 - direct participation, interpretation 61, 70–71, 75, 208–9, 327, 346–8
 - weapons, possession of 70–71

- protection
 - AWS risks 35
 - choice of attack options 355–6
 - collateral damage 24–7, 29, 44, 324, 355–6
 - cyber actions 29, 324
 - drone strikes 24–5, 317
 - exclusions 61, 70–71, 75, 208–9
 - immunity codification 53–4
 - obligations 25–7, 44, 51–2, 203, 207–8
 - precautionary principle 339–56
 - risk, absence of 16
 - technological advantages for 16
 - transference of risk 25, 317
- risks to
 - cyber warfare, from 29, 32, 74–5
 - drone strikes, from 24–5, 317
- targeting
 - military functions, carrying out 61
 - misidentification 67–71, 342–3
- Clinton, Bill 266
- collateral damage
 - AWS, calculation by 350–54
 - civilian protection obligations 340–41
 - cyber actions 29, 324
 - drone strikes 24–5
 - obligation to reduce 24–7, 29, 44, 340–41
 - precautionary principle 340–41, 350–54
 - proportionality 350–54
 - risk, absence of 16
 - transference of risk 25
- collateral damage, and
 - choice of attack options, and 355–6
- combat
 - preparation for, interpretation 62
 - purpose 48–9
- combat zones 87–90
 - combat activities in vicinity of 102–4
- combatants
 - fair dealing requirements 203–4
 - identification 52, 75, 224, 327
 - direct participation 61, 70–71, 75, 208–9, 327, 346–8
 - misidentification 67–71, 342–3
 - moral equality 43–4
 - non-combatants, distinction from 207–9
 - targeting rules 60–1
 - terrorists, as 224
- command responsibility
 - AWS, and 360–61, 369, 414–15, 432–6, 440–41
 - international law applicability 393
 - principles 413–14
- computer network attacks (CNA) 71
- computer network exploitation (CNE) 71
- conduct of hostilities rules 173–5, 184, 253
- Convention on Conventional Weapons 2016 123–4
- Convention on the Law of Treaties 1980 126–7
- cowardice, remote killing as 44–5
- Crootof, Rebecca 403
- crossbow 20
- cruise missiles 21
- customary international law
 - civilian protection obligations 203
 - interpretation 126–7
 - Lotus* principle 202–3
 - Martens Clause 43, 202–3
 - non-intervention principle, and 191–4
 - self-defense of state, against an individual 233–8
 - use of force prohibition 195–6
- cyber attacks
 - acknowledgment 273, 290
 - anonymity
 - attribution, and 310, 312
 - challenges of 27, 122, 288–9, 310, 312
 - plausible deniability, and 310
 - armed conflict
 - activities below threshold 287–94

- law applicability to 121, 324–5, 330–31
- role in 75–6, 274, 278, 324–5
- unwitting involvement 75–6
- asymmetrical risk 16–17, 27–33, 310, 312
- characterization 71, 130, 274, 306, 309–11, 321–2
- civilian impacts 29, 32, 74–5
- collateral damage 29, 324
- cost asymmetries 310
- counter-measures
 - active defenses 285–6, 291–2
 - anticipatory 283, 288–9
 - cascading effects, consideration 328–9
 - effectiveness 285–6
 - feasible precautions 328–9
 - limitations 279, 285–6
 - necessity, and 283–4
 - non-forceful 284–6
 - non-intervention principle, and 284–5
 - non-state actor attacks, to 285–6
 - regulatory development 291–2
 - reprisals, and 32–3, 310
 - self-defense justification 278–84, 286–7, 297
 - state responsibility 284–5
 - terrorism 281–2
- cyber exploitation 290–91
- definition 71–3, 121–2, 275–6, 321
- distinction, principle of, and applicability 208–9, 323–7
 - benefits for 72–4, 77
 - challenges for 74–6, 325–7
 - remoteness, and 76–8
- implications 274, 278
- information operations 187–8
- international law applicability 30–32, 275–7, 289–91, 294–7, 321–3, 330–31
- international humanitarian law 121–2, 209, 290–91
- non-intervention principle, and 192–3, 284–5
- proportionality 30–31, 326
- targets, interpretation 29–32, 327
- use of force 276, 278–81
- interpretation
 - armed attack, whether 280–84, 287–8
 - challenges 122, 129–30
 - distinction principle, applicability to 208–9, 323–7
 - drone strikes, differences from 27–9
 - information operations 187–8
 - intervention, as 192–3
 - limitations 72, 311–12
 - military uses
 - advantages 309–11
 - disadvantages 311–12
 - intelligence and surveillance 307–8, 311
 - non-intervention principle, and 192–3, 284–5
 - non-state actor role 274, 285–6, 306–7
 - precision 73–4
 - purpose 1, 15, 28–9, 72, 275–6, 330
 - intelligence and surveillance 307–8
 - military role 307–9
 - non-destructive impacts 311
- regulation
 - activities below armed conflict threshold 287–94
 - ad hoc approach 287–8
 - basis for 129–30
 - challenges 275–7, 279, 287–8, 296–7, 322–3, 331
 - development 291, 322–3
 - international law applicability 30–32, 121–2, 209, 275–7, 289–91, 321–3
 - Talinn Manual* 1, 72–3, 121, 275–6, 321–2, 327–8
 - US strategy 280, 289–94
 - reprisals, fear of 32–3, 310
 - source or location, ability to identify 27–8
- sources
 - identification challenges 27–8, 276, 279, 288–9, 310, 312

- responsibility, and 28, 277–8
- state responsibility
 - attribution challenges 289
 - countermeasures 284–5
- targets 29, 274
 - data, as military object 327–8
 - dual-use infrastructure 29–30, 74–5, 203, 311–12, 326
 - military vs. civilian, identification 74–5, 327
 - non-lethal 311
 - revenue-enhancing operations 31–2
- terrorism, and 275–6, 278–9, 281–4
- time and location benefits 309–10
- traditional weapons, differences from 330
- trends 273–5, 308–9
- use of force, and 196–7, 276, 278–61, 278–81, 287
- vulnerability risks 16, 274
- cyber-exploitation 290–91

- de Vattel, Emmerich 213–14
- dignity, principle of 152, 168–70, 184, 400–401
- Dinnis, Harrison 197
- Dinstein, Yoram 197
- direct participation
 - IHL applicability 208–9
 - targeting, interpretation 61, 70–71, 75, 208–9, 327, 346–8
- disarmament treaties 380
- discrimination, principle of 46
- distinction, principle of
 - achievement mechanisms 51–3
 - AWS 67–71, 336, 342, 395–6
 - challenges 52–3
 - codification 55–6
 - combatants vs. non-combatants 207–8
- cyber attacks
 - applicability to 208–9, 323–7
 - benefits of 72–4, 77
 - challenges of 74–6, 325–6
 - remoteness, and 76–8
- definition 54–5

- drones/ drone warfare
 - benefits of 65–7, 77
 - challenges of 67–71, 336
 - safeguards 66–7
 - generally 51–2, 78, 325, 408–9
 - historical development 53–6
 - importance 51
 - obligations under 51–2, 58, 207–8
 - practical application
 - challenges 62–3
 - generally 57–8
 - obligations, negative and positive 58
 - rules of engagement 57–8
 - targeting rules 58–62
 - precautionary principle, and 336, 397
 - proportionality, and 52, 326
 - purpose 53
 - remote warfare, and
 - benefits 63, 65–7
 - challenges 52–3, 62–3, 67–71, 336
 - drones/ drone warfare 65–71
 - remoteness, relevance of 76–8
 - targeting rules
 - AWS identification challenges 67–71, 336, 342, 395–6
 - objects 58–60, 345–6
 - persons 60–62, 346
- ‘Dogo,’ the 146
- domaine réservé* concept 190, 192
- Dörr, Oliver 196
- drone warfare
 - accuracy 67–71, 77, 248, 304–5
 - armed conflict, in
 - applicability of law of 120, 314–15, 330–31
 - consent requirement 98–9, 313–14, 318–19
 - determination criteria 23, 97–107
 - human rights law, applicability 104–7, 315–16
 - international armed conflict, whether 97–100
 - interstate requirement 99–100
 - legal challenges 318–21

- non-international armed conflict, and 100–104, 259–60
- transnational armed conflict, role in 259–60
- attitudes to 249–50
- benefits 15–16, 22, 29, 83, 247–50, 259–60, 270–72
- breach of sovereignty, as 22–4, 452–4
- challenges
 - civilian/ military target misidentification 67–71
 - latency 67–8
 - video quality 68–9
- collateral damage 24–7
- constitutional war powers, and 265–6, 268–70, 272
- cyber attacks, differences from 27–9
- distinction, principle of
 - benefits for 65–7, 77
 - challenges for 67–71, 336
 - remoteness, and 76–8
- extraterritorial jurisdiction 222–4, 240–41, 320
- human rights law, and
 - applicability to 81, 106–7, 315–16
 - due diligence obligations 222–3
 - law enforcement, and 171, 179, 184–5
 - War on Terror, in 171
 - whether violation of 24–5
- international humanitarian law, and
 - applicability to 24–5, 80–81, 120, 314
 - obligatory use potential 270
- law on, generally
 - basis for 129, 313–14
 - conflicts 246–7
- legality of 316–18
- non-international armed conflict
 - classification as 100–104, 259–60
- political pressures, and 260–61
- remoteness, relevance of 76–8, 317–18
- risk transference 25, 303
- safeguards 66–7
- self-defense justification 22–3, 172–3
 - against individuals 230–44, 320
- targeted killings 81
 - armed conflict law, applicability 114–20
 - non-international armed conflict, and 108
 - Reyaad Khan, of 226–44
 - self-defense, and 225–44
- transparency and accountability 160–61
- unwilling or unable test 23, 238, 249, 270–71, 318–19
- use of force
 - breach of sovereignty, as 23–4, 452–4
 - self-defense justification 23–4, 225–44
- use trends 62–3, 80, 139–40, 465
- drones
 - accuracy 67–71, 77, 248, 304–5
 - asymmetrical risk reduction 22–7, 66–7, 248–9, 260–61
 - benefits 15–16, 22, 29, 83, 247–50, 259–60, 270–72, 303–6
 - characteristics 64–5, 301
 - other weapons, similarities and differences 247–50, 270–71, 302, 316–18, 330, 461–2
 - consent requirement 98–9, 313–14, 318–19
 - definition 62, 301
 - development 301–3
 - disadvantages 83
 - equipment 64–5
 - limitations 22–3, 302–3
 - purpose 15, 29, 62–5, 301–3, 316–17
 - counter-terrorism 305–6
 - intelligence and surveillance 301, 303–5
 - range and duration of flight 64–5, 304
 - regulation
 - conflicts and challenges 220, 247, 331

- international law applicability
 - 220–21, 330–31
- limitations 224–5
- necessity 221
- risk transference 62, 303
- security concerns 221–2
- self-defense implications 221
- sovereignty, and 22–4, 452–4
- targeting
 - accuracy 16, 67–71, 77, 304
 - immediacy of response 304–5
- use of
 - non-state actors, by 82–3, 142, 466
 - trends 62–3, 82–3, 139–40, 301
- dual-use infrastructure
 - targeting 29–30, 74–5, 203, 344–5
 - cyber attacks 29–30, 74–5, 203, 311–12, 326
- due diligence obligations 222–3, 388–9
- dynamic diligence standard *see*
 - accountability
- effective control test 206–7
- effective remedy, right to 149, 162–3
- Egan, Brian 449–50
- espionage 290–91
- Estonia
 - cyber attacks 76, 290
- Fallon, Michael 117
- force, interpretation 195, 197
 - see also* use of force
- forced migration, as use of force 196
- France
 - drone use policy 454
 - terrorism counter-measures 219
- Friendly Relations Declaration 190
- Geiß, Robin 74
- General Robotics Ltd 146
- Geneva Conventions 1949
 - Additional Protocols 127–8
 - Martens Clause 43, 202–3, 381–2
 - precautionary principle 339–56, 397–8
- technology, keeping up with 381–2
- definitions 55, 89
- armed conflict, generally 111–12, 119, 252–3
- combatants *vs.* non-combatants 207–8
- geographical scope 90–92
- international armed conflict 98–100, 252
- limitations 122, 126
- non-international armed conflict 101–4, 252
- IHL applicability under 110–13, 131, 252–3
- customary law interpretation 126–7
- remote warfare, and 128–9
- purpose 55, 128–9, 131, 203
- travaux préparatoire* 128
- geographical scope
 - armed conflict
 - challenges 107–9
 - criterion for 90–91
 - global scope 116–19
 - judicial interpretation 91–5, 118–19
 - nexus approach 93–5
 - origin of attack, and 96
 - remote warfare, applicability 79–81, 89–90, 319–20
 - US approach 115–17
 - War on Terror 115–17
 - definition
 - importance of 86–7
 - synonyms 87–90
 - interpretation challenges 87–8
 - non-international armed conflict 91
- Georgia
 - cyber attacks 76, 290
- Germany
 - drone use policy 454
- Gilli, Andrea 466
- Gilli, Mauro 466
- globalization 10, 116–18
- Gray, Christine 119
- Gross, Oren 270
- Grotius, Hugo 217

- Hamas 142
 Harman, Harriet 240
 Henderson, Ian 345–6
 Heyns, Christof 119–20, 145–6, 152, 169, 378
 Hezbollah 142
 High Contracting Party, territory of 91, 290–91
 Hobbes, T. 217–18
 Hollis, Duncan B. 187, 196–7, 202–3
 Horowitz, Michael C. 403–4
 human rights law
 accountability 160–67, 178
 remote warfare, in 160, 168, 184
 armed conflict, and
 applicability to 104–7
 law enforcement role 133–4, 172–5, 184–5
 AWS
 dignity, principle of 152, 169–70, 184, 400–401
 extraterritorial jurisdiction 155–6, 172
 human responsibility, and 170
 ICRC position on 150–51, 156
 international discussions on 148–53
 peacetime use of 171–5
 common principles 159
 derogable rights 154
 dignity, principle of 168–70
 remote warfare, applicability to 152, 169–70, 184, 400–401
 drone warfare
 applicability to 81, 106–7, 315–16
 counter-terrorism justification 226–30
 targeted killings 81
 whether violation of 24–5
 due diligence obligations 222
 extraterritorial jurisdiction 154–5, 172, 204–5
 avoidance 156
 drone strikes 222–4, 240–41
 remote warfare, applicability 155–6, 172
 targeting 155–6
 triggers 104–5
 freedom of assembly 149, 152
 freedom of expression 149
 IHL, and
 as complement to 133, 153–70
 harmonization 166–7
 influences of 149–50
 role instead of 133–4
 investigation obligations 164–5, 167, 178
 jurisdiction
 effective control, and 105–6
 international obligations, and 105–6
 state agent authority exception 106–7
 law enforcement, and 152–3, 179
 use of force justification 172–5, 179
lex specialis, as 157–8
 necessity, principle of 104, 159, 175–6, 243–4, 250–51
 peacetime, in 154, 171–5, 204–5
 proportionality, principle of 104, 159–60, 176
 use of force 176, 179, 181–3
 public emergency, and 154
 remote warfare, applicability to 157, 184
 dignity 152, 169–70, 184
 extraterritorial jurisdiction 155–6, 172
 legality 177–83
 peacetime, in 171–5
 psychological remoteness 138–9, 183
 self-defense 172–3, 178–9
 transparency and accountability 160, 168, 184
 right to effective remedy 149, 162–3
 right to fair trial 149
 right to life 149, 152–4
 right to privacy 149
 right to security 224–5
 targeting
 drone strikes 81

- extraterritorial jurisdiction 155–6, 172
- IHL, relationship with 158–60
- targeted killings 81, 108
- use of force, and 180–81
- torture, prohibition of 169–70
- transparency 160–68
- use of force, and
 - accountability 178
 - law enforcement 172–5, 179
 - legality 177–8, 251
 - necessity 175–6, 179, 181–3, 243–4, 250–51
 - precautionary principle 176–7, 179–83
 - proportionality 176, 179, 181–3
- Human Rights Watch 150–51, 377–8
- human security
 - definition 216
 - self-defense justification 213–17
- humanitarian interventions
 - international law violations, as 40–41
- humanity, principle of 43, 170, 203, 382
- in-the-loop weapons 136, 353–4, 377
- information operations
 - see also* cyber attacks
 - armed conflict thresholds, and 202–3
 - definition 187–8
 - dual-use infrastructure, and 29–30, 74–5, 203
 - IHL, applicability to 203–4, 204–5
 - use of force, as 196–7
- intelligence and surveillance
 - cyber attacks, and 307–8, 311
 - drones, and 301, 303–5
- Intercontinental Ballistic Missiles (ICBMs) 21
- internal disturbances, interpretation 201, 254–6
- international armed conflict
 - definition 98–100, 252–3
- International Committee for Robot Arms Control 373
- International Committee of the Red Cross
 - AWS, position on 150–51, 156, 447
 - cyber attacks, position on 121
 - drone warfare, position on 118
 - human rights, extraterritorial jurisdiction 156, 172
- International Court of Justice
 - customary international law, interpretation 127
 - effective control test 206–7
- International Criminal Court
 - geographical scope of armed conflict, definition 92–3
- international criminal law
 - command responsibility 360–61, 369, 393, 413–15, 432–6, 440–41
- International Criminal Tribunals
 - armed conflict
 - definition, evolution of 111–12
 - geographical scope, interpretation 92–5, 118–19
- International Human Rights Clinic 151
- international humanitarian law
 - applicability, generally
 - customary international law interpretation 126–7
 - cyber attacks 30–32, 121–2, 209, 275–7, 290–91
 - drone strikes 24–5, 80–81
 - information operations 203–5
 - peacetime, in 154
 - public emergency, and 154
 - armed conflict, and
 - accountability 124–5, 160–68
 - applicability 50–51, 81, 84–5, 110–13
 - challenges 107–8
 - chivalric warfare principles 42–4
 - conduct of hostilities rules 173–5, 184, 253
 - definition 86–8, 110–13

- human rights law, applicability to 104–7
- internal conflicts, applicability to 254–6
- AWS
 - ability to comply, and 394–9
 - accountability, and 124–5, 160–68
 - applicability to 122–5, 369, 469–70
 - challenges for 125, 383–90
- common principles 159
- cyber attacks
 - applicability to 30–32, 121–2, 209, 275–7, 290–91
- drone strikes
 - applicability to 24–5, 80–81, 120, 314
 - obligatory requirement potential 270
- geographical scope
 - challenges 107–9
 - definition 86–8
 - nexus approach 93–5
 - origin of attack, and 96
 - remote warfare, applicability 79–81, 89–90, 319–20
- human rights law, and
 - as complement to 133, 153–70
 - harmonization 166–7
 - influences of 149–50
 - law enforcement justification 172–5
 - role instead of 133–4
- humanity, principle of 170
- lex specialis*, as 157–8
- necessity, principle of 104, 159, 175
- non-international armed conflict, and
 - applicability 81, 84–5
 - cross-border spillovers 100–104
 - geographical scope 81, 86–8, 91
 - non-state fighters, cross-border retreat 102–4
 - protracted armed violence requirement 81, 100–101, 108
 - territory of High Contracting parties 102–3
- perfidy, prohibition of 203–4
- proportionality, and 30–31, 104, 159–60
- purpose 128–9
- technology, keeping up with 381–2
- use of force 251
- war crimes, investigation obligations 164–5
- international law, generally
 - basis for 313–14
 - disarmament treaties 380
 - military operations, of 313
 - new weapons/ technology
 - ability to comply with 394–9
 - AWS, implications 383–401
 - humanity principle test 382
 - keeping up with 378–83
 - prohibited weapons 380–81
 - review obligations 151, 382–3, 411–12, 470–71
 - purpose 41–2
 - sovereignty, and 313
 - strict liability 390–91
- intervention
 - armed attack, compared 191–2
 - coercion, as 191–2
 - countermeasure, as 194
 - cyber operations, as 192–3
 - definition 191–2
 - humanitarian, as international law violation 40–41
 - non-intervention principle 189–92
 - prohibited acts 191–2
 - propaganda, as 193–4
 - right to self-determination, and 194
 - thresholds 191–2
- Iran
 - Stuxnet cyber attack 1, 16, 73, 200, 273, 290
- Iraq
 - drone warfare 57–8, 69
- Iron Man 141
- ISIS 142
- Janjua, Tehmina 460–61

- jus ad bellum
 - conflicts 40
 - self-defense, right of 216, 231–8, 450–52
 - just war theory 291
- Kendall, Frank 141
- Khan, Reyaad 226–44
- Kiai, Maina 152
- killer robots *see* robotic infantry devices
- Koh, Harold 267
- Lahmann, Henning 74
- latency, problem of 67–8
- Lauterpacht, Hersch 126
- law enforcement and security
 - human rights law, and
 - armed conflict, and 133–4, 172–5, 179, 184–5
 - IHL, and 172–5
 - remote warfare 152–3, 171, 179, 184–5
 - use of force justification 172–5, 179
 - remote warfare, and
 - drones 171, 179, 184–5
 - human rights implications 152–3, 179, 184–5
 - psychological remoteness, and 138–9, 183
 - use of 133–4, 145–8, 152–3, 172–5, 179
- Law of War Manual* (US) 294
- legality, principle of 177–80
- legally saturated violence 215
- lethal autonomous weapons *see* autonomous weapons systems
- Libya
 - air strikes 267
- Lieber Code 43, 53–4
- Locke, John 217
- Lotus* principle 202–3
- Lubell, Noam 129–30
- machine learning 415–16
- Martens Clause 43, 202–3, 381–2
 - meaningful human control 391, 401–4, 431–40
- Mégret, Frederic 462
- migrants 188, 196
- military objectives
 - definition 58–9
 - identification challenges, cyber attacks 327
 - location, influences of 59–60
 - nature-location-use-purpose test 58–60
 - purpose 59
- military objects
 - data as 327–8
 - disguised 59–60
 - interpretation 30–32, 327–8
 - targeting rules 58–60, 327–8, 345–6
- military personnel
 - misidentification 67–71, 342–3
 - targeting rules 60–1, 346
- monitored autonomy 377–8
- morality
 - chivalric warfare 42–8, 318
 - death by algorithm 400–401
 - killing at a distance 46–8
 - risk to life, and 46–7
 - risk vs. cost 41–2, 310, 367, 455–6, 465
- nature-location-use-purpose test 58–60
- necessity, principle of 43–4, 151–2
 - absolute necessity 159, 243–4
 - cyber attack, self-defense 283–4
 - human rights law, and 175–6, 179, 181–3, 250–51
 - IHL, compared with 104, 159
 - self-defense, against an individual 234–5, 243–4
 - status-based vs. threat-based 159
- non-international armed conflict
 - acknowledgment 254–6, 271
 - armed conflict
 - applicability 110–13, 173
 - classification as 202
 - conduct of hostilities rules 173–5, 253
 - cross-border spillovers 100–104

- non-state fighters, cross-border retreat 102–4
- protracted armed violence requirement 81, 100–101, 108
- unwilling or unable test 23, 238, 249, 270–71, 318–19
- definition 252–3
- distinction, principle of, and 56, 408–9
- drone warfare
 - protracted armed violence requirement 81
 - self-defense justification 22–3, 172–3
 - unwilling or unable test 23, 238, 249, 270–71, 318–19
 - whether 100–104
- geographical scope
 - challenges 107–9
 - IHL applicability 81, 86–8, 91, 107–9
 - judicial interpretation 92–4
 - origin of attack, and 96
 - territory of High Contracting Party 91
- identification as 202, 258–9
 - acknowledgment, and 254–6, 271
 - consequences of 258–9
 - drones, role in 259–60
 - incentives 259–60
- IHL applicability 84–5, 254–6
 - cross-border spillovers 100–104
 - geographical scope 81, 86–8, 91
 - non-state fighters, cross-border retreat 102–4
 - protracted armed violence requirement 81, 100–101, 108
 - territory of High Contracting parties 102–3
- non-state threats, and 102–4, 257–8
- targeted killings 108
- trans-border actions
 - concept development 257–8
 - drones role in 259–60
 - hot pursuit 102–4
 - interpretation implications 258–9
 - non-state fighters, retreat over 102–4
 - self-defense justification 22–3
 - spillovers 100–104
- non-intervention principle 189–92
 - applicability 190
 - customary international law, as 191–4
 - cyber-attacks, violation of 192–3, 284–5
 - domaine réservé* concept 190, 192
 - Friendly Relations Declaration 190
 - international obligations 191–4
 - origins 189–90
 - propaganda, and 193–4
 - right to self-determination, and 194
- non-state actors
 - armed attack by 198–9, 256
 - AWS and drones use by 82–3, 142, 466
 - cyber attacks by 274, 285–6, 306–7
 - self-defense against, justification 198–9, 256
 - warfare, role in 84–5, 188, 202
 - applicable law 85–6
 - transnational conflict 102–4, 257–9
- Noone, Gregory 66
- Obama, Barack 117, 265, 267
- O’Connell, Mary Ellen 191–2
- on-the-loop weapons 136, 353–4, 377
- Oppenheim, Lassa 54
- origin of attack 96
- Outer Space law 390–91
- outside-the-loop weapons 354, 377–8
- overall control test 206–7
- peacekeeping 188, 242
- peacetime
 - default international framework 250
 - human rights law applicability 171–5
 - IHL applicability 154
 - remote weapons use in 171–5
 - perfidy, prohibition of 203–4

- pin-prick theory 284
- precautionary principle
 - AWS
 - attacks on other AWS 131, 345–6
 - cancellation protocols 354–5, 388
 - challenges 67–71, 327, 341–2
 - choice of options, and 355–6
 - collateral damage, and 340–41, 350–54
 - decisions, compared with human role 33–4, 123–5, 341–3, 345–6
 - feasibility of 328–9, 349, 398
 - human *vs.* computer, comparison 33–4, 123–5, 341–3, 345–6
 - limitations, programming 351–2, 364–5
 - remoteness, and 349–50
 - target identification 67–71, 336, 344–8
 - cyber attacks 328–9
 - feasibility standard 328–9, 349, 409
 - necessity, and 336
 - proportionality 344–5, 350–54
 - remoteness, and 349–50
 - suspension of attacks 354–5
 - targeting
 - accuracy 344–5
 - challenges 67–71, 327, 341–2
 - distinction, principle of, and 67–71, 336, 342
 - human *vs.* computer, by 33–4, 123–5, 341–3, 345–6
 - international obligations 341–9, 409
 - nature-location-use-purpose test 59–60
 - objects 345–6
 - persons, direct participation 346–8
 - treaty obligations 339–56, 397–8
 - use of force, and 176–7, 179–83
- propaganda 193–4
- proportionality, principle of
 - AWS, and 344–5, 350–54, 396–7
 - collateral damage 350–54
 - cyber attacks, and 30–31, 326
 - distinction, principle of, and 52
 - human operator, role of 124, 151–2
 - human rights law, and
 - IHL, applicability 30–31, 104, 159–60
 - use of force 176, 179, 181–3
 - precautionary principle, and 344–5, 350–54, 397
 - purpose of 159–60
 - self-defense, against an individual 235–6
- protracted armed violence 81, 100–101, 108, 201–2
- psychological operations 187–8
- public emergency, international law applicability 154
- Randelzhofer, Albrecht 196
- reciprocal risk
 - see also* asymmetrical risk
 - AWS, of 17
 - chivalric warfare, and 42–8
 - cyber attacks, of 16–17
 - professional conduct of soldiers 46–7
- remote-controlled devices 141–2, 149, 152–3
- remote warfare, generally
 - see also* AWS; cyber attacks; drone warfare
 - accountability, and 357–65
 - armed conflict, increases in 120, 125, 130, 399–400, 446–56, 478
 - attitudes to 143–5, 336–7, 367
 - characterization 128–9, 298, 317
 - traditional weapons, similarities and differences 247–50, 270–71, 299–300, 302, 316–18, 330, 336, 461–2
 - common features 135
 - definition 338
 - development 134–5, 141–2, 335–6
 - ethical concerns 366–8
 - human rights law, and
 - applicability to 157, 184

- dignity 152, 169–70, 184, 400–401
- enforcement role 133–4
- extraterritorial jurisdiction 155–6, 172, 222–4, 240–41
- legality 177–83
- lex specialis*, as 157–8
- peacetime use 171–5
- psychological remoteness 138–9, 183
- self-defense 172–3, 178–9
- targeting 158–60
- transparency and accountability 160, 168, 184
- impunity concerns 137–8
- law enforcement and security role 145–8
 - human rights implications 152–3, 179, 184–5
 - use of force justification 172–5
- precautionary principle obligations 340–56
- remoteness
 - definition 138–9, 338
 - psychological 138–9, 183
 - temporal 179, 184
- right to life, and 149, 152–3
- risk
 - influences on 336, 399–400
 - vs. cost 310, 367, 455–6, 465
- UN CCW meeting of experts 143–5, 445–7, 467–8
- remote weapons systems, generally
 - see also* AWS; cyber attacks; drones
 - definition 123, 135–7
 - force protection benefits 15–17
 - human rights law, and
 - ICRC position on 150–51, 156
 - international discussions 148–53
 - legality under 178–83
 - law enforcement and security role 145–8
 - human rights implications 152–3, 179, 184–5
 - use of force justification 172–5
 - new weapons/ technology
 - review obligations 151, 382–3, 411–12, 470–71
 - psychological remoteness 138–9, 183
 - types 135–8
 - use of 139–48
 - development trends 141–2
 - functions 139
 - law enforcement, in 133–4, 145–8, 152–3, 172–5, 179
 - lethal force, and 147
 - peacetime, in 171–5
 - self-defense justification 172–3, 178–9
 - trends 62–3, 80, 82–3, 139–40
- remotely piloted vehicles *see* drones
- remoteness
 - artificial intelligence, and 138–9
 - definition 138–9, 338
 - human control, and 138
 - imminence of threat, and 179, 221, 231–8
 - precautionary principle, and 349–50
 - psychological remoteness 138–9, 183
 - robotic infantry devices 34–5
 - temporal remoteness 138, 179, 184, 221, 231–8
- Riotbot 146
- risk
 - see also* reciprocal risk
 - autonomous targeting, and 33–4
 - collateral damage in absence of 16, 25
 - remote warfare implications 336, 399–400
 - reprisals, cyber attacks 32–3
 - transference of risk 25
 - vs. cost 41–2, 310, 367, 455–6, 465
- robotic infantry devices
 - ban, calls for 150–52, 373, 445, 467
 - human rights law challenges for 151–2
 - proportionality, and 124, 151–2
 - remote-controlled humanoids 141
 - remoteness, and 34–5
 - right to dignity, and 152, 169–70

- Rothenberg, Daniel 77–8
- Rousseau, Jean Jacques 54, 218
- rules of engagement 57–8
- Russia
- AWS policy development 144, 454
 - Crimea, military force in 39–40, 188, 200
 - cyber attacks 273, 290
- Rwanda
- international intervention 41
- Sassòli, Marco 60–1, 340, 342–3, 355, 367–8
- Scharre, Paul 403–4
- Schmitt, Michael 130, 193, 287, 363–4
- self-defense
- anticipatory acts 236–8, 283, 288–9
 - armed conflict, whether 115–16, 172–3
 - attack, proof of 218–19
 - collective self-defense 243
 - cyber attacks, against 278–84, 286–7, 297
 - drone warfare, legal conflicts 221–2
 - imminence of threat, and 213, 221, 223–4, 226, 229, 231–8, 283, 319–20
 - individual, against 230–38, 320
 - criminal law, under 232, 241–2
 - extraterritorial jurisdiction 232–3, 320
 - human rights law, under 232–3
 - international law, right under 233–4
 - legal principles, generally 231–2
 - necessity 234–5, 243–4
 - pre-emptive actions 236–8, 283
 - proportionality 235–6
 - UK targeted killing of Reyaad Khan 226–38
 - unwilling or unable test 238, 270–71, 318–19
 - individual right of 213–15, 219
 - justification
 - drone strikes 22–3, 23–4, 172–3, 223–4, 226–30
 - human rights law, legality under 178–9
 - human security 213–17
 - individuals, against 230–44, 320
 - non-state actors, against 198–9, 256
 - peacekeeping 242
 - provocation 233–4
 - punishment 229–30
 - sovereign right and duty 213–18, 452–4
 - terrorism, and 218–19, 226–30
 - use of force, for 22–3, 115–17, 172–3, 178–9, 198–9, 223–4, 226–30, 450–52
 - limitations 452
 - terrorism, and
 - counter-measures as 218–19
 - due diligence obligations, and 222–3
 - justifications for 218–19, 230–44
 - UK drone strikes 226–30
 - time delay implications 229–30
- self-determination, right to 194
- Serbia
- international intervention 41, 266
- Shamoon virus 273–4
- Sharkey, Noel 398
- ‘shift cold’ 305
- Simon-Michel, Jean-Hughes 446
- Singer, Peter 66–7
- snipers 46–7
- Snowden, Edward 274
- Solis, Gary 121–2
- Somalia
- international intervention 41
- Sontag, Susan 45–6
- sovereignty
- drone strikes as breach of 22–4, 452–4
 - international law, and 313
 - self-defense, right and duty 213–18, 452–4

- Space Liability Convention 390–91
- St Petersburg Declaration 1868 54
- state responsibility
 - AWS
 - accountability 386–8
 - attribution 386
 - cancellation protocols 388
 - criminal responsibility 387, 392–4
 - due diligence 388–9
 - liability, and 389–91
 - predictability, and 388–9, 392–3
 - recklessness and negligence 386–7
 - strict liability 389–91
 - cyber attacks
 - attribution challenges 289
 - countermeasures 284–5
 - due diligence, and 222–3, 388–9
 - effective control test 206–7
 - human security, and 213–17, 221–2
 - international law obligations 250–52
 - overall control test 206–7
 - scope of 205–6
 - self-defense, legal principle 231–2
 - transboundary harm, prevention
 - obligations 388–90
- strategic stability 447–8
- Stuxnet cyber attack 1, 16, 73, 200, 273, 290, 326
- surrender
 - AWS, recognition by 348–9
- surveillance *see* intelligence and surveillance
- Switzerland
 - AWS policy proposals 468–70
- Syria
 - cyber attacks 308
- Talim Manual on International Law Applicable to Cyber Warfare* 1, 72–3, 121, 275–6, 321–2, 327–8
- Taranis 141
- targeted killings
 - armed conflict law, applicability 114–20, 317–18
 - drone warfare/ strikes 81
 - non-international armed conflict, and 108
 - self-defense of state, in
 - counter-terrorism justification 225–44
 - counter-terrorism strategy, as 226–30
 - Reyaad Khan, of 226–30
- targeting
 - accuracy 10, 47–8, 181
 - drone warfare 16, 67–71, 77, 304
 - autonomous targeting 33–4
 - accountability, and 124–5
 - benefits 34, 342
 - criticism 342, 344
 - law, applicability to 123–4
 - AWS, by
 - accountability, and 124–5
 - accuracy 344–5
 - autonomous 33–4, 123–5, 344
 - benefits 34
 - challenges 67–71, 327, 341–2
 - criticism 344
 - distinction, principle of, and 67–71, 336, 342, 395–6
 - human vs. computer, by 33–4, 123–5, 341–3, 345–6
 - law, applicability to 123–4
 - nature-location-use-purpose test 59–60
 - objects 345–6
 - obligations 341–9
 - other AWS 131, 345–6
 - against other AWS 131, 345–6
 - persons, direct participation 346–8
 - proportionality, and 344–5, 350–54, 396–7
- civilians
 - direct participation 61, 70–71, 75, 208–9, 327, 346–8
 - military functions, carrying out 61

- misidentification 67–71, 342–3
- cyber attacks 29, 274
 - data, as military object 327–8
 - dual-use infrastructure 29–30, 74–5, 203, 311–12, 326
 - military vs. civilian, identification 74–5, 327–8
 - non-lethal 311
 - revenue-enhancing operations 31–2
- distinction, principle of 67–71, 336, 408–9
- drone strikes
 - accuracy 67–71, 77, 304–30516
 - challenges 66–7
 - criteria for 65–6
 - legality 317–18
 - self-defense justification 223–4, 230–44
- economic activity, objects involved in 31–2
- human rights law, and
 - implications 158–60
 - use of force legality 180–81
- IHL, and
 - applicability 158–60, 171–2
 - human rights law, and 158–60
- individuals 230–38, 320, 409–410
 - criminal law, under 232, 241–2
 - extraterritorial jurisdiction 232–3, 320
 - human rights law, under 232–3
 - international law, right under 233–4
 - legal principles, generally 231–2
 - necessity 234–5, 243–4
 - pre-emptive actions 236–8, 283
 - proportionality 235–6
 - UK targeted killing of Reyaad Khan 226–38
 - unwilling or unable test 238, 270–71, 318–19
- location, influences on 59
- military objectives
 - definition 58–9
 - identification challenges, cyber attacks 327
 - use and purpose 59
- military objects 334–46
 - data as 327–8
 - disguised 59–60
 - interpretation 30–32, 327–8
 - rules 58–60, 327–8
- military personnel
 - misidentification 67–71, 342–3
 - rules 60–1, 346
- persons, rules regarding 346
 - direct participation, interpretation 61, 70–71, 75, 346–8
 - military functions, carrying out 61
 - military personnel 60–61
 - preparation for combat, and 62
 - self-defense conflicts 221, 223–4
 - situational/signature targeting 410–11
- stages 409–410
- target identification 409
 - categorical targeting 409
 - challenges 67–71, 327, 341–2, 408–9
 - distinction, principle of, and 67–71, 336
 - human vs. computer, by 33–4, 123–5, 341–2, 345–6
 - international obligations 341–9
 - nature-location-use-purpose test 59–60
 - proportionality, and 344–5
- technology, generally
 - dehumanization effect 374
 - development influences 220–21, 244–5
 - law keeping up with 378–83
 - strict liability, and 390–91
- Technorobot 146
- terrorism
 - 9/11 attacks 45, 198–9, 224–5, 231, 257–8
- counter-terrorism 305–6
 - geographical scope 93–4
 - justification 226–31

- drone strikes
 - counter-terrorism role 226–30, 305–6
 - justification 226–30
- lone wolf terrorists 172–3
- protracted armed violence, as 101
- self-defense, and
 - counter-measures as 226–31
 - due diligence obligations, and 222–3
 - right and duty 218–19
 - use of force as 22–3, 172–3
- targeted killings
 - Kahn, Reyaad 226–30
- technology impacts on 215
- terrorists as combatants 224
- warfare methods, impacts on 84, 257–8
- Thomas, A. J. 194
- Thomas, Ann van Wynen 194
- threat of force 197
- transboundary harm, prevention
 - obligations 388–90
- transnational armed conflict 84–5, 257–8
- transparency
 - accountability, and 163
 - armed conflict, obligations during 163–4, 166–8
 - definition 161
 - effective remedy, right to 162–3
 - human rights law obligations 160–68
 - IHL obligations 160, 162–8
 - importance of 161–2
 - limitations 162–3
 - remote warfare, in 160–68
- UAVs *see* drones
- UN Certain Conventional Weapons
 - informal meetings of experts 143–5, 445–7, 467–8
- unintended engagements 456–60
- United Kingdom
 - AWS, policy on 143
 - counter-terrorism drone strikes
 - justification 226–30, 238–44
 - legality 230–44
 - targeted killings, Reyaad Khan 226–44
- United States
 - armed conflict, interpretation 115–18
 - War on Terror 117–18
 - defense policy development
 - 60-day clock 263–5
 - applicability 267
 - AWS 142–3, 368–9, 371–2, 434, 467–78
 - concerns and conflicts 268–70
 - congressional opposition 264–8
 - constitutional war powers (WPR) 263–72
 - Conventional Arms Transfer Policy 475–7
 - cyber attacks 280, 289–94
 - de minimis risk approach 267–70
 - drone warfare 265–6, 268–70, 272
 - generally 261–2
 - historical development 262–4
 - Law of War Manual* 294
 - post-enactment practices 264–5
 - principles of use requirements 476–7
 - purpose 264–5
- unmanned aerial vehicles *see* drones
- unmanned robotic weapons *see* autonomous weapons systems
- unwilling or unable test 23, 238, 249, 270–71, 318–19
- use of force
 - aggression, compared 199–200
 - alternative weapons 177–8
 - armed attack
 - compared 195–8
 - interpretation as 280–84, 287–8, 451–2
 - consent of territorial state, and 449–50
 - cyber attacks 196–7, 276, 278–81, 287
 - defensive obligations 177–8
 - definition 195

- drone strikes
 - breach of sovereignty, as 23–4, 452–4
 - self-defense justification 23–4, 223–4, 230–44
 - targeted killings 81
- escalation of force procedure 180–81
- forced migration, as 196
- human rights law, and
 - accountability 178
 - law enforcement 172–5, 179
 - legality 177–80, 251
 - necessity 175–6, 179, 181–3, 243–4, 250–51
 - precautionary principle 176–7, 179–83
 - proportionality 176, 179, 181–3
- IHL, applicability under 251
- imminence of threat, and 213, 221, 223–4, 226, 229, 231–8, 283
- interpretation approaches 196–7
- intervention, and 189–95
- justification
 - law enforcement 172–5, 179
 - self-defense 22–3, 115–17, 172–3, 178–9, 198–9, 223–4, 230–44, 450–52
- legally saturated violence 215
- lone wolf terrorists, and 172–3
- non-military nature, of 196
- pre-stationed forces, and 188, 200
- prohibition 195–6, 313–14
 - challenges 196–7
 - exceptions 449–50
 - information operations 196–7
- thresholds
 - gaps 198
 - lowering, implications of 120, 125, 130, 446–56, 478
 - self-defense against non-state actors 198–9, 256
- time delays, implications of 229–30
- Vanguard Defense Industries 146
- war crimes
 - AWS role in 357–8, 365
 - excuses for 44
 - investigation obligations 164–5
- war, generally
 - see also* armed conflict
 - characterization
 - conflict type, changes in 83–4, 298–9
 - migrant movements, and 188, 196
 - modern features 186–7, 298–9
 - non-state actors role 85–6, 188, 202
 - peace keeping forces role in 188
 - pre-stationed forces, and 188, 200
 - chivalric warfare principles 42–4, 318
 - constitutional powers 261–2
 - historical development 262–3
 - protection of nationals abroad 262
 - definition 111–13, 251–3
 - dehumanization 374
 - globalization 119
 - illegal wars, discouragement 41–2
 - information operations 186, 202
 - just war theory 291
 - Lotus* principle, and 202
 - norms of 43–5
 - personal risk, morality of 45–6, 399–400
 - psychological operations 186–7
 - reciprocal risk, and 44–5
 - strategic stability 447–8
 - subversive activities 186–7
 - terrorism impacts 84
- War on Terror
 - armed conflict
 - geographical scope 115–17
 - IHL, applicability of 115–16
 - self-defense justification 115–17, 198–9
 - UK policy 117–18
 - US policy 115–17
 - human rights law, applicability to 115–16, 171
- Watts, Sean 283
- Waxman, Matt 288, 292

- weaponry
 - see also* autonomous weapons systems; cyber attacks; drones; remote warfare
 - ban campaigns 150–52, 373, 445, 467
 - biological 412
 - chemical 340, 380
 - historical development
 - air and naval power 20–21, 298–9
 - artillery 19–20
 - ballistic missiles 21, 299
 - bow and arrows 18–19
 - firearms 19–21, 46–7
 - generally 18–21, 50, 79, 82, 84–5, 298–9
 - new weapons/ technology
 - asymmetric warfare impacts 460–64
 - cost vs. risk 41–2, 310, 367, 455–6, 465
 - humanity principle test 382
 - IHL applicability 381–2
 - informal consultations 143–5, 445–7, 467–8
 - international law, keeping up with 378–83
 - lowering armed conflict
 - thresholds, whether 120, 125, 130, 446–56, 478
 - predictability 388–9, 392–3, 459
 - prohibited weapons 340, 380–81
 - proliferation implications 464–6
 - review obligations 151, 382–3, 411–12, 470–71
 - traditional weapons, similarities and differences 247–50, 270–71, 302, 316–18, 330, 461–2
 - unintended engagements 456–60
 - prohibited weapons 340, 380–81
- Wilmshurst, Elizabeth 131

