

## INDEX

- Abella* Case (IACHR) 388  
 absolute rights 202–203  
 access  
   to data  
     and privacy rights 190–191  
     by states 69–71  
 to Internet/cyberspace  
   restrictions on 23, 545  
   rights to 195, 199–200  
 to neutral territory 509–510  
 rights of, of land-locked States 255  
 accessory to commission of war crimes  
   395–396  
 ACHR (American Charter of Human Rights), derogation  
   provision in 208  
 active cyber defences 453, 563  
 Additional Protocols to Geneva Conventions  
   on application of 377  
   on attacks 414–415  
   on civilian status 413  
   commentaries *see* ICRC  
   on distinction principle 420–421  
   on espionage 410  
   grave breaches of 392  
   on identification of medical units  
     and transports 517  
   on mercenaries 412–413  
   on military objectives 436, 441,  
     450  
   on non-international armed conflicts  
     391  
   on perfidy 491  
   on precautions in attack 476, 478,  
     480–485  
   on reprisals 463–464
- ADIZs (Air Defence Identification Zones) 266, 268  
 aerial blockades 504  
 agents  
   diplomatic 209, 220  
   immunities of 230–231  
   permitted activities of 229–230  
   of international organizations 158,  
     159–160  
 aggregation of cyber incidents  
   amounting to armed attacks 342  
   in assessment of harm 38–39  
 aggression 265, 339  
 aiding or assisting/abetting  
   in another state's cyber operations  
     42, 101–103  
   in commission of war crimes, and  
     criminal responsibility  
     395–396  
   responsibility for wrongful acts based  
     on 162–165  
*Air Service* Arbitral Award 117  
 aircraft  
   cyber operations by 261–265, 269  
   cyber weapons/operations used  
     against 24–25, 268–269  
   international law applicable to  
     259–261  
   nationality of 63  
 airspace  
   international, cyber operations in  
     24–25, 265–268  
   national  
     cyber operations in 261–265  
     state sovereignty over 18–19  
     and outer space 271  
*Al-Skeini* Case (ECtHR) 184

- Alvarez, Judge 41
- anonymity, right to 194–195
- anticipated military advantage 473–475
- anticipatory reprisals 462
- anticipatory self-defence 118, 139, 350–354
- Archer Daniels* Arbitral Award 116, 133
- archipelagic States, rights and duties of 251–254
- archipelagic waters
  - cyber operations in, law of the sea applicable to 251–252
  - transit rights of aircraft over 266
- archives, diplomatic, protection/immunity of 219–225
- armed attacks
  - cyber operations qualifying as 107, 139, 339–348, 354–355
  - foreign military aircraft in national airspace as 265
  - imminence of 508
  - objects of 346, 423
  - and use of force 332–333, 337, 341
- armed conflicts 375–376
  - diplomatic immunity in 212
  - participation in *see* direct participation in hostilities
  - and peaceful settlement of disputes obligation 309–310
  - thresholds for existence of 370–371, 383–384
  - use of aircraft in, and cyber operations 261 *see also* international armed conflicts; law of armed conflict; non-international armed conflicts
- armed forces
  - conscription/enlisting of children prohibited in 525
  - involvement of, and existence of armed conflict 384
  - irregular 403
  - jurisdiction over 63
  - law enforcement agencies/paramilitary groups incorporated into 406–407
  - targeting and combatant immunity of members of 401–408, 426
- armed groups *see* organised armed groups; virtual armed groups
- Articles on the Responsibility of International Organizations (ILC) 153–154, 167
- Articles on State Responsibility (ILC) 79
  - on countermeasures 119, 123–124, 127, 131, 134
  - on necessity, plea of 135
  - and non-State actors 95, 99
  - on State organs 87–88
- assessments
  - of harm 38–39
  - of imminence 138–139, 352
  - of losses 151, 530
  - of military advantage 442–443, 473–475, 482–483
  - of military objective status 444–445, 448–451
  - of proportionality 128, 130
  - of unnecessary suffering 454–455
  - of use of force 333–337
- assistance
  - duties of, in distress situations 279
  - international, in law enforcement 77–78
  - requirement to request 50
- assurances of non-repetition 143–144
- attacks 415, 442
  - indiscriminate 435, 467–469
  - precautions in 476, 487–491
    - cancellations/suspensions of attacks 483–484
    - choice of targets duty 481–483
    - constant care duty 476–478
    - means and methods of warfare choice 479–481
    - passive precautions duty 487–491
    - and proportionality 481
    - verification of targets duty 478–479
  - warnings duty 484–487 *see also* armed attacks
- attempting to commit war crimes 395

- attribution of wrongful acts
  - to international organisations 156–157, 159–160
  - to States
    - cyber operations 83, 115–116
    - by non-State actors 94–100
    - by other states 100–104
    - by State organs 87–94
    - governmental authority 89–90
    - retroactive 100
- authority, governmental, and organs of State 89–91
- Autronic AG v. Switzerland Case* (ECtHR) 183
- aviation, civil, prohibition of cyber operations against 268–269
- bandwidth 563
  - throttling 566
- Barcelona Traction Case (Belgium v. Spain, ICJ)* 152
- belligerent nexus criterion for direct participation in hostilities 430–431
- belligerent reprisals 112, 124, 460–463
- belligerent rights, exercise of 554–555
  - on neutral territory
    - and obligations of neutral States 557–560
    - prohibition of 556–558
    - remedies against failure to stop 560–561
- bleed-over effects
  - of armed attacks 344
  - of countermeasures 137
- blockades 504–507
  - cyber 505–507, 510
  - enforcement/maintenance of 508–510
  - effectiveness 506
- booby traps, cyber 457–459
- botnets 563
  - assessment of harm caused by 38–39
  - examples of use of 22–23, 49–50, 55, 83, 91, 129, 429, 453
  - targeting of 429
- breaches of international law *see* violations
- broadcasting, unauthorised, on high seas 236–237
- Cable Convention 253, 257
- cables, submarine
  - law of the sea applicable to 14, 252–258
  - neutrality/occupation law applicable to 510, 551–552
- camouflage, permissibility of 496
- cancellations of attacks 483–484
- capture, perfidious acts leading to 492
- care
  - duty of
    - constant care duty 476–478
    - for dams, dykes, and nuclear electrical generating stations 529–531
    - standards of 279
- Caroline* incident 350–351
- censorship in armed conflict, legitimacy of 527–528
- cessation
  - of wrongful acts 117, 142, 149 *see also* termination
- Charter of Fundamental Rights (EU) 191
- Chicago Convention on Civil Aviation 260–261
  - on due regard for safety of civil aviation 268
  - on international airspace 265–266
  - on ‘Rules of the Air’ 267
  - on territory of a state 261–262
  - on transit rights 263–264
- children in armed conflict, protection of 524–526
- China, commitment with United States
  - on cyber espionage 169
- circumvention 163
- civilian morale, targeting of 443–444
- civilian objects
  - avoidance of proximity to military objectives 490
  - feigning status of 494

- civilian objects (cont.)
  - and military objectives distinction 435–445
  - military use of 438–439
    - assessment of 439–440, 449–450
    - termination of 450–451 *see also* dual-use objects
  - natural environment as 537–539
  - precautions in attack principles applied to 481–483
  - proportionality principle in attacks on 481
  - targeting rules applicable to 434–435
- civilians in armed conflict
  - occupation 544–546
  - protection of objects indispensable to survival of 531–533
  - proximity to military objectives avoidance 490
  - starvation prohibition 459–460
  - terror spreading prohibition 434
- close access operations 563
- cloud computing 563
- cloud infrastructure, cyber operations
  - against, and state immunity 24–25
- co-perpetration of war crimes 393–394
- coastal States
  - enforcement jurisdiction of 246–248
  - rights and duties of 240–245, 249
    - over submarine cables 14, 253–256
- coercion
  - economic and political 331
  - and non-intervention principle 317, 317–320
  - responsibility for wrongful acts based on 103, 163
- collateral damage 471
  - by cyber attacks 418–419, 471–473
  - excessive 473
  - obligation to minimise 480, 529–530
  - uncertainty about 475–476 *see also* military advantage
- collection, of communications 190
- collective punishments prohibition 539–540
- collective security
  - peace operations 361–368
    - protection of personnel involved in 368–371
  - UN Security Council's role in 327, 357–360, 362
    - enforcement by regional organisations 360–361
- collective self-defence 354–355
- collectives, informal groups acting as 390–391
- combatant immunity 401
  - for cyber operation participants 402–408
  - for *levée en masse* participants 408–409
  - for organised armed group members 403–405
  - for spies 409–412 *see also* targeting rules of law of armed conflict; unprivileged belligerency
- commanders, criminal responsibility of 394, 396–400
- communications
  - confidentiality of 189–191
  - diplomatic/consular, freedom of 225–227
  - UN Security Council powers of disruption of 358 *see also* cables; telecommunication
- companies *see* corporations
- compensation 150–151
- compliance
  - with international law
    - by belligerent reprisals 461
    - coercion used for 317
    - countermeasures used for 112, 117
    - due diligence principle 43–50 *see also* non-compliance with international law obligations
  - with UN Security Council resolutions, obligations to 110, 562
- Computer Emergency Response Teams (CERTs) 563

- computers, computer systems,
  - computer networks 564
- camouflage of 496
- medical, protection in armed conflict of 515
- of UN, protection in armed conflict of 368–371 *see also* cyber infrastructure
- concurrent jurisdiction, over cyber operations 52
- conduct, obligations of 288–289
- confidence, creation of, and perfidy 493–494
- confidentiality, of communications 189–191
- confiscation of property, during occupation 549–552
- conscription of children into armed forces, prohibition of 525
- consensus, on Tallinn Manual rules 4
- consent
  - invalidity of 104–107
  - to conduct cyber operations on a State's territory 27
  - to enforcement jurisdiction of another state 68–69
  - to humanitarian assistance operations 541
  - to peacekeeping operations 363–364
  - wrongfulness precluded by 104–107, 166, 323
- consequences
  - of cyber operations/activities 416
  - in territorial seas 246–247
- foreseeable, of attacks/cyber attacks 59, 343–344, 416
- immediacy of 334, 336
- measurability of 335–337
- of violence 415–416
- constant care duty 476–478
- constructive knowledge 40–42, 559
- consular immunity 211
  - countermeasures not permitted against 125
  - of honorary consular officers 225
- consular law *see* diplomatic and consular law
- consular posts 209–210
  - freedom of communication of 225–226
  - immunities of officers of 230–231
  - inviolability of archives and documents of 105, 220
  - inviolability of cyber infrastructure in 213
  - use of premises 228–229
  - wireless communication equipment in 230
- contiguous zones, cyber operations in, law of the sea applicable to 248–249
- continental shelves, rights over submarine cables in 254–255
- continuous combat function 426
- contribution, to peril/harm, by injured state 140–141, 147
- control
  - of enemy weapons 451–452
  - responsibility for wrongful acts based on 103, 162–163
  - in telecommunication law 290
  - of territory, and precautions against cyber attacks 489 *see also* effective control test; overall control test
- Convention on Special Missions 210–211
- Corfu Channel Case (United Kingdom v. Albania, ICJ)* 16, 40–41, 151
- corporations
  - and countermeasures 130–131
  - as State organs 88–89, 97
- correspondence
  - of detained persons in armed conflict, protection of 522–523
  - diplomatic, immunity of 219–225, 294
  - of protected persons during occupation, rights 545
- countermeasures 111–116
  - cyber operations as 107–108
  - effects on third parties 133–134

- countermeasures (cont.)
  - by international organisations 166–167
  - limitations on 122–126
  - and necessity 114, 135–142
  - permissibility of 39–40, 50, 82–83, 307
    - and diplomatic law 125, 211–212
  - proportionality of 127–130
  - purposes of 116–122
  - urgent 120
- counterterrorism measures
  - in cyber context 199
  - and human rights 203, 205
  - treaties 76
- Court of Justice of the European Union
  - Google v. Spain* Case 195–196
  - on right to be forgotten 195–196
- crimes *see* cyber crime; war crimes
- criminal activities, in territorial seas,
  - jurisdiction over 246–248
- criminal responsibility
  - of commanders and superiors 394, 396–400
  - of individuals 391–396
- criteria
  - for armed attacks 341–342, 344
  - for combatant status 403–405
  - common 563
  - for direct participation in hostilities 429–430
  - for international armed conflict
    - existence 379–385
  - for mercenaries 412–413
  - for military objectives 438–441, 448
  - for non-international conflict
    - existence 379–380, 385, 388–391
  - for use of force assessments 333–337
- critical infrastructure 25–26, 564
  - interfering with/targeting of 37–38, 136–141, 205, 328, 343, 345
  - maintenance of 547
- cross-border activities
  - in non-international armed conflict 386–387
  - in self-defence 347–348
- cultural property, targeting of 485, 534–536
  - reprisals 463
- cultural rights, in cyber context 194
- cyber attacks *see* attacks
- cyber attacks, as terror attacks 433–434
- cyber blockades 505–507, 510
- cyber booby traps, prohibition on use of 457–459
- cyber capabilities 339
- cyber communications
  - harmful interference with 294–298
  - suspension or stoppage of 291–294
- cyber countermeasures 107–108
- cyber crime 26–27, 75
  - and fair trial rights 193
  - universal jurisdiction over 65–66
- cyber defences
  - active 563
  - hack back 565
  - passive 566
- cyber espionage 323
  - in armed conflict
    - and combatant immunity 409–412
    - and perfidy 494
  - diplomatic premises used for 229
  - and human rights law 192–193
  - in peacetime 25, 168–174
  - and State sovereignty 19–20, 25, 173
  - as use of force 335
- cyber infrastructure 564
  - camouflage of 496
  - civilian, used for cyber attacks 495
  - control by States/Parties to a conflict over, occupation law on 549–552
  - in diplomatic missions, inviolability of 212–217
- governmental
  - hostile use of 41
  - immunity of 28–29
  - and State responsibility 91–92
- jurisdiction of States over 51–54
  - flag States/States of registration 68, 232–233
- as military objective 444
- neutral 553–554
- protection of 555–556

- as object indispensable to survival of
  - civilian population 533
- obligations of occupying powers to
  - restore and maintain 547
- as State property 73, 550
- and State sovereignty 12–13, 18, 71–74
- and telecommunication law 289–290
- use of
  - for cyber attacks 495
  - neutrality law on 556–558
- cyber measures, to ensure security
  - of occupying powers 548–549
- cyber property, during occupation,
  - requisition/confiscation of 549–552
- cyber reconnaissance 564 *see also* cyber espionage
- cyber security, international
  - cooperation in 131–133
- cyber weapons 406
  - obligation of review of 465
  - testing of 242
  - transmission across neutral territory
    - of 557–559
  - use of, against aircraft 268–269
- damage 127
  - causation of
    - by cyber operations/attacks 20–25, 144–145, 418–419
    - economic 25–26
    - espionage 412
    - functionality of an object 417–418
    - gravity of 136–137
    - by space objects 282
    - to submarine cables 256–258
  - collateral 471
    - by cyber attacks 418–419, 471–473
    - excessive 473
    - and military advantage 475–476
    - obligation to minimise 480, 529–530
    - uncertainty about 475–476 *see also* harm
- dams, cyber attacks on, and duty of care 529–531
- data 564
  - access to 69–71
  - attacks on 416
    - as military objective 437
  - collection/storing of 190
    - by tapping of cables 257
  - medical
    - identification of 517
    - protection in armed conflict of 515
    - loss of 517–519
  - personal, protection of 191–192, 521
  - as property 550
  - state sovereignty/jurisdiction over
    - 15–16, 63
  - transit of 33–34, 55–56
- data centres 564
- undersea 234–235
- data embassies *see* digital embassies
- databases 564
- DDoS (Distributed Denial of Services)
  - operations 118–119, 505, 565
  - against Estonia xxiii, 376, 382, 387, 505
  - examples of use of 21, 26–27, 49–50, 150, 247, 315, 318, 518–519
- death, proximate cause of 492–493
- Declaration on Friendly Relations 271, 316
  - on armed attacks and use of force 332
  - on coercion 317
- Declaration on the Use of Outer Space 271
- definitions
  - aircraft 260
  - archipelagic States/waters 251–252
  - armed conflicts 375–376
  - booby traps 457–458
  - botnets 563
  - civilian objects 435
  - civilians 413, 423
  - cloud computing 563
  - coercion 317
  - computers, computer networks, and computer systems 564
  - consular posts 209–210

- definitions (cont.)
  - countermeasures 111
  - cultural property 534
  - cyber attacks 376, 415–420
  - cyber espionage 168, 410
  - cyber infrastructure 564
  - cyber operations 564
  - cyberspace 564
  - data 564
  - data centres 564
  - DDoS operations 565
  - diplomatic missions 209
  - disputes/international disputes 304
  - documents 220
  - domain 565
  - domain names 565
  - DoS operations 564
  - electronic archives 220
  - electronic warfare 565
  - essential interests 135–136
  - exclusive economic zones 239
  - force, use/threat of 330–339
  - hacktivists 565
  - harmful interference 296
  - high seas 233
  - honeypots/honeynets 565
  - humanitarian assistance 541–542
  - injured states 80
  - injury 144
  - international airspace 265–266
  - international organisations 154
  - international peace and security 305–306
  - international straits 249
  - Internet 565
  - intervention 313
  - inviolability 219
  - journalists 527
  - launching States 271–272
  - malware/malicious logic/logic bombs 566
  - means and methods of warfare 452–453
  - mercenaries 412–413
  - metadata 566
  - military objectives 436
  - natural environment 537
  - objects 437
  - occupation 543
  - peaceful purposes 233–234
  - peremptory norms of international law 124
  - perfidy 491
  - phishing 566
  - radio stations 295
  - responsible States 80
  - software 567
  - sovereignty 11
  - space activities 272, 280–281
  - space objects 271
  - spoofing 567
  - starvation 459–460
  - State organs 87–88
  - steganography 567
  - submarine communication cables 253
  - telecommunications 284–285
  - territorial sea 241
  - territories of state 261–262
  - UN operations 369
  - UN personnel 369
  - unauthorised broadcasting 236–237
  - weapons 452
- delayed effects, and direct participation in hostilities 431
- derogation from human rights 207–208
- destruction
  - of property, and perfidy 494
  - wanton 538
- detained persons in armed conflict, protection of 519–524
- digital cultural property, protection of 535–536
- digital embassies 23, 216
- diplomatic and consular law 209–212
  - duty to protect cyber infrastructure 217–219
- free cyber communications 225–227
- inviolability of cyber infrastructure in diplomatic missions 212–217
- inviolability of electronic archives, documents, and correspondence 219–225
- use of premises and activities of officials 227–230



- diplomatic immunity 211
  - countermeasures not permitted against 125, 211–212
- diplomatic missions 209
  - agents of 220
  - immunities of 230–231
  - permitted activities 229–230
- cyber infrastructure in, inviolability of 212–217
- use of premises 228–229
- wireless communication equipment in 230
- direct participation in hostilities 401
  - by armed forces members 401–408
  - by children 525–526
  - and civilian status presumption 425
  - by civilians 413–414, 425, 428–432
  - cyber attacks as 430–432
  - and delayed effects 431
  - by journalists 528–529
  - by spies 409–412
- direction, responsibility for wrongful
  - acts based on 103, 162–163
- discrimination prohibition, and human rights limitations 206–207
- dispute settlement
  - and countermeasures permissibility 121–122
  - peaceful, obligations to attempt 303–311
- distinction principle, in cyber attacks 420–422
- distinctive signs/emblems
  - improper use prohibition 496–499
  - requirements
    - for combatant status 405–406
    - for cultural property 536
    - for medical transports and units 515–517
- distress
  - as circumstance precluding wrongfulness 109–110
  - duty of assistance in circumstances of 279
- domain names 565
  - cyber operations against 335
- domaine réservé* see internal affairs of States
- domestic law
  - on cable laying activities 254
  - criminal cyber operations in 76–77
  - and foreign nationals 59–60
  - obligations of occupying powers for maintaining of 243
  - and prevention of harmful cyber operations obligation 48–49
- DoS (Denial of Services) operations 564
  - examples of use of 315
- double criminality principle 76–77
- doubt, about civilian status 424, 448–451
- drafting of Tallinn Manual 5–6
- ‘Hague Process’ xxvi, 2, 6–7
- dual-use objects
  - radio installations 299
  - satellites 277
  - segregation of military and civilian use 489
  - targetability of 445–447, 491
- due diligence principle
  - compliance with 43–50
  - and cyber operations 30–43, 130
  - violations of, and proportionality 50
- duration, of direct participation in hostilities 431
- dykes, cyber attacks on, and duty of care 529–531
- ECtHR (European Convention of Human Rights),
  - derogation provision in 208
- economic coercion 331
- economic damage, caused by cyber operations 25–26
- economic rights, in cyber context 194
- economic sanctions, and non-intervention principle 324
- ECtHR (European Court of Human Rights)
  - Cases
    - Al-Skeini* 184
    - Autronic AG v. Switzerland* 183
    - Leander v. Sweden* 190
    - Zakharov v. Russia* 207

- ECtHR (European Court of Human Rights) (cont.)
- on extraterritorial application of human rights law 184
  - on human rights law applicability to commercial entities 183
  - on human rights limitations, and non-discrimination principle 207
  - on privacy rights 190
- effective contribution to military action 440–441, 448
- effective control
- in human rights law 184–186
  - in the law of State responsibility 96–97
- effective remedy *see* remedy
- effects
- of countermeasures, on third parties 133–134
  - of cyber operations/attacks
    - and armed attack notion 340–344
    - delayed 431
    - indirect 472–473
    - and means and methods of warfare 457
    - spill over in neutral territory 555
  - doctrine for establishing jurisdiction 57–59, 64
- Egypt, suspension of cyber communications by 293
- electromagnetic frequencies, state sovereignty over 14
- electronic archives 220
- electronic evidence 193
- electronic surveillance, of diplomatic correspondence 222–223
- electronic warfare 565
- emblems/signs, distinctive
- improper use prohibitions 496–499
  - requirements
    - for combatant status 405–406
    - for cultural property 536
    - for medical transports and units 515–517
- encryption technologies, and state sovereignty 14
- enforcement
- actions, by regional organisations 360–361
  - of blockades 508–510
  - of law
    - by coastal States 246–248
    - consent given by another State for 68–69
    - international cooperation in 75–78
    - over piracy 67, 236
    - UN Security Council granting of powers for 69
  - of peace 364
    - mandates/authorisations for 362
- Environmental Modification Convention (1977) 537
- erga omnes* obligations, breaches of 152–153
- escalation risks, for countermeasures 117–118
- espionage
- cyber 323
    - in armed conflict, and combatant immunity 409–412
  - diplomatic premises used for 229
  - and human rights law 192–193
  - in peacetime 25, 168–174
  - and State sovereignty 19–20, 25, 173
  - as use of force 335
  - and perfidy 494 *see also* spies
- essential interests
- of international community 136
  - and plea of necessity based on 135–142, 166
- Estonia
- cyber operations against (2007) xxiii, 376, 382, 387, 505
  - digital embassies of 23, 216
- European Union, Charter of Fundamental Rights of 191
- evidence
- for attribution of wrongful acts 83
  - electronic 193
- excessiveness, of collateral damage 473

- exclusive economic zones
  - cyber operations in, law of the sea
    - applicable to 239–241
  - submarine cables in, rights over 254
- exclusive flag State jurisdiction 232–233
- expression, freedom of
  - during occupation 547–548
  - in cyber context 187–189
- external affairs of States 317
- ‘extradite or prosecute’ provisions 77
- extraterritorial application
  - of due diligence principle 32–33
  - of human rights law 184–186, 198
- extraterritorial jurisdiction
  - enforcement 52–53, 66–71
  - over cyber operations 52
  - prescriptive 60–66
- fair trial rights 193
- firmware 565
- FIRs (Flight Information Regions) 267
- flag States *see* registration, States of
- flags, warships carrying neutral or enemy 502
- force *see* use of force
- force majeure* 108–109, 141–142
- foreign nationals
  - and domestic legislation 59–60
  - and passive personality jurisdiction 64–65
- foreseeable consequences of attacks/
  - cyber attacks 59, 343–344, 416
- forgotten, right to be 195–196
- France, Additional Protocol
  - Ratification Statements of 464
- freedom of communication,
  - diplomatic/consular 225–227
- freedom of expression
  - in cyber context 187–189
  - during occupation 547–548
- freedoms of high seas 234, 239, 255, 265–266
- fulfil, obligation to, in human rights law 201
- functionality loss caused by cyber operations
  - in armed conflict 417–418
  - in peacetime 20–23
- Gabčíkovo-Nagymoros Case* (Hungary v. Slovakia, ICJ) 118, 138
- Galić Case* (ICTY) 475
- Geneva Conventions (1949)
  - application of 377
  - on belligerent reprisals 461
  - on combatant immunity 402
  - on command responsibility 397
  - commentaries *see* ICRC
  - on criteria for existence of
    - international/
      - non-international armed conflict 379–380
  - grave breaches of 392
    - on occupation law 544–545, 547
    - on terror spreading prohibition 434
- Genocide Case* (*Bosnia and Herzegovina v. Serbia and Montenegro*, ICJ) 88, 381
- geographical limitations
  - of blockades 505–506
  - of cyber warfare 378–379, 411
  - of non-international armed conflicts 386–387
- Georgia, cyber operations directed
  - against (2008 conflict with Russia) 376
- good faith
  - acts of 105–106
  - judgments in 530
  - in negotiations 120–121
  - obligation 77
    - in dispute resolution 308–309
- Google v. Spain Case* (CJEU) 195–196
- Gould Marketing Inc. v. Ministry of Defence of Iran Case* (US-Iran Claims Tribunal) 108
- government employees, civilian,
  - targetability of 427–428, 438
- governmental authority
  - exercise of 92
  - and organs of State 89–91

- governmental control, and due diligence principle 33
- governmental cyber infrastructure
  - hostile use of 41
  - immunity of 28–29
  - and State responsibility 91–92
- governmental functions, cyber attacks
  - causing loss of 21–24
- GPS navigation system 299
- cyber attacks on 471–473
- Granier and Others (Radio Caracas Televisión) v. Venezuela* Case (IACHR) 183
- grave breaches, of Geneva Conventions 392
- guarantees, of non-repetition of internationally wrongful cyber operations 143–144
- hack back operations 565
- hacktivists 565
- Hague Air Warfare Rules (1923) 436
- Hague Conventions on the Laws and Customs of War on Land (1907)
  - Convention IV 377–378
    - Regulations 438, 510, 544, 547, 550–551
  - Convention V 558
  - Convention XIII 245–246, 509
- Hague Cultural Property Convention (1954) 534
- ‘Hague Process’ xxvi, 2, 6–7
- hardware 565–567
- harm
  - caused by cyber operations, and due diligence principle 34, 36–40
  - contribution of injured States to 140–141, 147
  - imminent 138–139
  - thresholds of 36–40, 416 *see also* damage
- harmful interference with cyber communications/services
  - space law on 278
  - telecommunications law on 279, 294–298
- health, right to 194
- ‘herding’ 172
- high seas
  - freedoms of 234, 239, 255, 265–266
  - jurisdiction over vessels on 232–233
- honeypots/honeynets 565
  - use in cyber espionage 173–174
- honorary consular officers 225
- hors de combat* status 426
- hostilities
  - armed conflict in absence of 384–385
  - intensity threshold of, for non-international armed conflicts 387–389
  - outbreak of, and peaceful settlement of disputes obligation 309–310
  - participation in *see* direct participation in hostilities
  - requirement for existence of armed conflict 383–384
- human rights
  - absolute 202–203
  - fundamental 123–124
  - non-derogable 202–203, 208
- human rights law
  - applicable to cyber operations 179–187
    - derogation of rights 207–208
    - individual rights 187–196
    - limitations on rights 198, 201–207
    - respect and protect obligations 181, 196–202
  - applicable to occupation 547–548
  - applicable to peace operations 365–366
  - violations of 181–182
    - and remedy obligations 200–201
- humanitarian assistance operations, prohibition of cyber interference with 540–542
- humanitarian interventions, cyber operations in support of 324
- IACHR (Inter-American Commission on Human Rights)
  - Abella* Case 388

- on non-international armed conflicts 388
- on right of access to Internet 199
- IACtHR (Inter-American Court of Human Rights), on applicability of human rights law to commercial entities 183
- ICANN (Internet Corporation for Assigned Names and Numbers) 175
- ICAO (International Civil Aviation Organization) 267
- ICC (International Criminal Court)
  - on protection of children 525
  - Statute 369, 392
  - on criminal responsibility of commanders and superiors 399–400
  - on criminal responsibility of individuals 392, 394–395
- ICCPR (International Covenant on Civil and Political Rights)
  - derogation provision in 207–208
  - extraterritorial application of 186
  - on privacy rights 189
- ICJ (International Court of Justice)
  - on armed attacks 340–342, 344–345
- Cases
  - Barcelona Traction (Belgium v. Spain)* 152
  - Corfu Channel (United Kingdom v. Albania)* 16, 40–41, 151
  - Gabčíkovo-Nagymoros (Hungary v. Slovakia)* 118, 138
  - Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* 88, 381
  - Kosovo* (Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo) 18
  - Nicaragua* (Military and Paramilitary Activities in and against Nicaragua)
    - on armed attacks notion 330–331, 341–342, 344
    - on compelling another State into compliance with international legal obligations 317
    - and effective control notion 96–97
    - on prohibited interventions/non-intervention principle 315, 317, 319–320, 322
    - on self-defence rights 356
    - on use of force 331–332
    - Nuclear Weapons (Legality of the Threat or Use of Nuclear Weapons)* 338, 340, 420, 451
    - Oil Platforms (Iran v. United States)* 126
    - Prosecute or Extradite Obligation (Belgium v. Senegal)* 152
    - Tehran Hostages (United States v. Iran)* 99–100, 125, 382
    - Wall (Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory)* 152
    - Whaling in the Antarctic (Australia v. Japan, New Zealand intervening)* 81–82
- on compensation 151
- on countermeasures 118–119, 126
- on diplomatic/consular immunity 125
- on due diligence principle 31–38
- on effective control test 96–97
- on *erga omnes* obligations 152
- on imminent harm 138
- on intervention prohibition 314–315, 317, 319–320, 322
- on means and methods of warfare 451, 454
- on non-State actors, responsibility of 381
- on protection of civilians in armed conflict 420
- on reasonableness standards 81–82

- ICJ (International Court of Justice) (cont.)
- on self-defence rights 356
  - on State organs 88, 99
  - on threats of force 338
  - on use of force threshold 331–332
- ICRC (International Committee of the Red Cross)
- on civilian status presumption 449
  - on collective punishments prohibition 539
  - on direct participation in hostilities 428–430
  - on humanitarian assistance operations 541
  - on improper use of enemy/neutral indicators 501–503
  - on *levées en masse* 408–409
  - on military advantage 442, 473–474
  - on non-international armed conflict rules 533
  - on organised armed group membership 426–427
  - on perfidy prohibition 493
  - on protection
    - of children 524
    - of medical data 515
    - of medical units 518
    - of natural environment 538–539
  - on reprisals 462, 464
  - on starvation of civilian population prohibition 460
  - on terror spreading prohibition 433–434
  - on weapons definition 452
- ICTY (International Criminal Tribunal for the Former Yugoslavia)
- Cases
- Galić* 475
  - Limaj* 389–390
  - Tadić* 380–381, 388, 393
- on individual criminal responsibility 393
  - on joint criminal enterprise 393
  - on non-international armed conflicts
    - criteria for existence of 388–389
    - distinction principle in 421
  - on organised armed groups 389–390
  - overall control test of 380–382
  - on proportionality in attack 475
  - on reprisals 464
- ILC (International Law Commission)
- on space law 272 *see also* Articles on the Responsibility of International Organisations; Articles on State Responsibility
- immediacy
- of consequences 334, 336
  - requirement for exercise of self-defence right 350–354
- imminency of attacks
- and penetration of zones 508
  - and self-defence right 350–354
- imminent peril to essential state interests 135–142, 166
- immovable State property, obligations of occupying powers to safeguard capital value of 550
- immunity
- combatant 401
    - for cyber operations participants 402–408
    - for *levée en masse* participants 408–409
    - for spies 409–412
  - diplomatic/consular 211, 294
    - countermeasures not permitted against 125
    - of diplomatic agents and consular officers 230–231
  - of international organisations 210
  - sovereign, and inviolability over cyber infrastructure/operations 27–29, 71–74, 244
  - of vessels and aircraft 241–242, 244, 250–251
  - of States, from foreign jurisdiction 71–74
- indirect effects of cyber attacks 472–473, 480–481
- indiscriminate attacks prohibition 435, 455–457, 467–469

- individuals
  - criminal responsibility of 391–396
  - lawful targetability of 425–428, 436
  - overall control test not applicable to 382
- informal groups, collective activities of 390–391
- infrastructure
  - critical 25–26, 564
  - interfering with/targeting of 37–38, 136–141, 205, 328, 343, 345
  - maintenance of 547
- injured States 80
  - contribution to peril/harm by 140–141, 147
  - right to compensation 145–152
  - right to countermeasures 82–83, 111–116, 130–133
- injury 127, 144
  - caused by cyber operations 145–146
  - prohibition to cause superfluous 453–455 *see also* collateral damage, excessive
  - proximate cause of 492–493
- innocent passage 233, 241–245, 252, 262–263
- instigation, to commit war crimes 395
- intensity criterion for non-international armed conflicts 387–389
- intent/intentions
  - of armed attacks 24
  - and self-defence right 343–344
  - and prohibited interventions 321–322
  - to attack objects indispensable to survival of civilian population 532
  - to commit war crimes 392
  - to spread terror 434
- interference 313
  - with functionality, as damage caused by cyber attacks/operations 20–23, 417–418
  - harmful, with cyber
    - communications/services space law on 278
    - telecommunications law on 279, 294–298
  - with humanitarian assistance operations, prohibition of 540–542
- internal affairs of States, and non-intervention principle 314–317, 326
- international airspace, cyber operations in 24–25, 265–268
- international armed conflicts
  - categorisation as 379–385
  - law of neutrality in 42–43
  - and peaceful settlement of disputes obligation 309–310
  - and sovereign immunity 28–29 *see also* law of armed conflict; non-international armed conflicts
- International Code of Conduct for Information Security 26
- international community
  - essential interests of 136
  - obligations towards, breaches of 152–153
- international cooperation
  - in cyber security 131–133
  - in law enforcement 75–78
- international disputes 304–305
  - obligations of States to attempt peaceful settlement of 303–311
- international environmental law, due diligence principle in 37
- international human rights law *see* human rights law
- international humanitarian law *see* law of armed conflict
- international law
  - applicable to cyber operations 3
  - in peacetime xxiii–xxvi, 1
  - during armed conflict *see* law of armed conflict
- international organisations
  - countermeasures by 166–167
  - immunities of 210
  - responsibility of 153–167
  - and sovereignty 13, 155–156

- international peace and security
  - 305–306
  - cyber operations threatening 326
  - UN Security Council maintenance/
    - restoration of 327,
    - 357–360
- International Space Station Agreement 278
- international straits
  - cyber operations in, law of the sea
    - applicable to 249–251
  - transit rights of aircraft over 266
- international telecommunication
  - services 285
- internationally wrongful acts
  - countermeasures permissible for
    - injured States 82–83,
    - 111–116, 130–133
  - cyber operations qualifying as 84–87
    - and due diligence principle 34–35
  - obligations of states responsible for
    - 142–153
  - responsibility for
    - of international organisations
      - 156–157, 159–160
    - of States
      - circumstances precluding
        - wrongfulness 104–111,
        - 166, 323
      - cyber operations 81–83, 115–116
        - by non-State actors 94–100
        - by other States 100–104
        - by State organs 87–94
      - and governmental authority 92
      - retroactive 100
- Internet 565
  - access to
    - restrictions on 23, 545
    - rights to 195, 199–200
  - military use of 446–447, 556–557
  - as object indispensable to survival of
    - civilian population 533
  - terrorist use of 199
- intervention, prohibition of 156–163,
  - 314–317, 326
  - for States 312–325
  - for UN 312, 325–327
- inviolability 219
  - in diplomatic and consular law 105,
  - 212–217, 219–225
  - of neutral territory 555
- IP/IP address (Internet Protocol) 566
- Iran, cyber operations directed against
  - nuclear capabilities of
    - (Stuxnet, 2010) 342, 384,
    - 567
- Iran–United States Claims Tribunal
  - on *force majeure* situations (*Gould Marketing Inc. v. Ministry of Defence of Iran*) 108
  - Iran v. United States* 324
- irregular armed forces 403
- Island of Palmas* Arbitral Award
  - (*Netherlands v. United States*) 11
- ITU (International Telecommunication Union) 284–286
  - legal regime of 286–288, 294–298
    - see also*
    - telecommunication law
- jamming 297–298, 418, 505, 565
- joint criminal enterprise 393–394
- journalists in armed conflict, protection
  - of 526–528
- jurisdiction
  - over cyber infrastructure/operations
    - 51–54, 68
    - aircraft and vessels 27–28, 63,
    - 232–233, 246–248, 263
    - space objects 277–278
    - and state immunity 71–74 *see also*
      - extraterritorial
      - jurisdiction; territorial
      - jurisdiction
  - jus ad bellum*
    - applicable to cyber operations
      - 328–329, 348–350, 377,
      - 508
    - jus in bello* distinction 3–5
      - and law of armed conflict 377
  - jus cogens* *see* peremptory norms of
    - international law



- knowledge
  - constructive 40–42, 559
  - of cyber operations
    - of commanders/superiors 399–400
    - in intervention context 320–321
    - by neutral States 559
- Kosovo (Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo)* Advisory Opinion 18
- land-locked States, rights of 255
- last window of opportunity standard 351–353
- launching States 271–272, 281
- law of armed conflict
  - applicable to cyber operations/attacks 1, 375–378
  - collective punishments 539–540
  - criminal responsibility
    - of commanders and superiors 396–400
    - of individuals 391–396
  - distinction principle 420–422
  - geographical limitations 378–379
  - improper use of protective/enemy/neutral emblems/indicators prohibition 496–504
  - indiscriminate attacks/warfare prohibition 435, 455–457, 467–469
  - interference with humanitarian assistance prohibition 540–542
  - international armed conflicts 379–385
  - jamming 298
  - non-international armed conflicts 385–391
  - participation in hostilities *see* direct participation in hostilities
  - perfidy prohibition 491–495
  - precautions in attack *see* cyber attacks, precautions in
  - presumption of civilian status 424–425, 448–451
  - ruses 495–496 *see also* cyber attacks; means and methods of cyber warfare; protections in armed conflict; targeting rules of law of armed conflict
  - applicable to peace operations 366–367, 370–371
  - and human rights law 181
  - naval warfare, law of 233, 235, 240–241, 245–246
  - and space activities 277
- law enforcement *see* enforcement, of law
- law of neutrality *see* neutrality, law of
- law of the sea 232–233
  - applicable to cyber operations 233–235
  - in archipelagic waters 251–252
  - in contiguous zones 248–249
  - in exclusive economic zones 239–241
  - in international straits 249–251
  - in territorial sea 241–248
  - and right of visit 235–239
  - applicable to submarine cables 252–258
  - Convention 233–234, 252
  - on overflight of high seas 265–266 *see also* naval warfare, law of
- Leander v. Sweden* Case (ECtHR) 190
- levée en masse* participants
  - combatant immunity for 408–409
  - targetability of 425, 428
- lex specialis* principle 80–81, 181, 282
- liability *see* responsibility
- Liability Convention 281–283
- Limaj* Case (ICTY) 389–390
- limitations
  - on countermeasures 122–126
  - geographical
    - of blockades 505–506

- limitations (cont.)
  - of cyber operations in armed conflict 378–379, 411
  - of non-international armed conflicts 386–387
  - on human rights 198, 201–207
  - on State jurisdiction 60
  - temporal, on anticipatory self-defence 351–353
- losses
  - assessments of 151, 530
  - functional, caused by cyber attacks 20–23, 417–418
  - of protection in armed conflict 517–519 *see also* direct participation in hostilities
- ‘Love Bug’ malware 77
- machine inspection, of communications 190
- malware 566
  - ‘Love Bug’ 77
  - rootkit 566
  - use of
    - as cyber booby trap 459
    - as cyber espionage 173
  - worms 568
- Martens Clause 377–378
- mass surveillance 170–171
- material breaches, of treaty obligations 115
- material contribution, and responsibility for wrongfulness 109
- material damage 144–145
- means and methods of cyber warfare 451–453
  - booby traps prohibition 457–459
  - enforcement/maintenance of blockades 508–510
  - indiscriminate warfare/attacks prohibition 435, 455–457, 467–469
  - precautions in choice of 479–481
  - reprisals 460–464
  - starvation prohibition 459–460
  - unnecessary suffering prohibition 453–455
  - weapons reviews obligation 464–467
- medical personnel, units and transport, computers, computer networks and data
- identification of 515–517
- protection in armed conflict of 513–515
- loss of 517–519
- membership
  - in armed forces 426
  - in organised armed groups 426–427
- mercenaries, unprivileged belligerent status of 412–413
- mere passage regime 233, 245
- metadata 566
  - protection of 192
- methods of warfare *see* means and methods of cyber warfare
- military activities
  - cyber, on high seas 234–235
  - in outer space, law applicable to 273, 275–276
  - prohibition of compulsory participation in 523–524, 546
- military advantage 442
  - in military objective determination 440–443, 448
  - and precautions in attack 482–483
  - and proportionality principle 473–475 *see also* collateral damage
- military aircraft 260
  - cyber operations by 267
  - transit rights of 264–265, 267
- military commanders/superiors, criminal responsibility of 394, 396–400
- military objectives
  - assessment of status of 444–445, 448–451
  - attacks on/targetability of 423–424, 435–445, 469–470
  - avoidance to proximity of civilians and civilian objects to 490

- dual-use objects 445–447
  - segregation of military and civilian use 489
- military radio installations, exemption of 298–300
- Mines Protocol 457–459, 485
- moral damage 145
- motives *see* intentions
- nationality
  - and exercise of extraterritorial jurisdiction 61–62
  - of ships, aircraft and satellites 63, 237–238
- nationals
  - foreign
    - and domestic legislation 59–60
    - and passive personality jurisdiction 64–65
  - protection of, and non-intervention principle 323
- NATO (North Atlantic Treaty Organization) 355, 360–361
- Cooperative Cyber Defence Centre Of Excellence (Tallinn, Estonia) xxiii, 1, 6–7, 91–92
- Rapid Reaction Team 27
- natural environment, protection
  - in armed conflict of 537–539
- nature criterion, for military objectives 438, 440–441
- Naulilaa* Arbitral Award (*Portugal v. Germany*) 123, 127
- naval blockades *see* blockades
- naval warfare, law of 233
  - applicable to cyber operations 233, 235, 240–241, 245–246
- ne bis idem* principle 76–77
- necessity
  - human rights limitations based on 203–204
  - plea of 135
    - and countermeasures 114, 135–142
    - and gravity of peril 136–137
    - precluding wrongfulness 108, 166
  - principle, in exercise of self-defence rights 348–350
- negligence
  - contribution to harm by 147
  - in space activities 281–282
- negotiations requirement, for countermeasures 120–121
- network nodes 564–566
- network sniffer software 566–567
- network throttling 566
- neutral indicators, improper use
  - prohibition 503–504
- neutral States
  - knowledge of 559
  - obligations of 557–560
  - rights of 509–510, 555–558
- neutrality
  - and blockades 509–510
  - law of 553–555
    - and cyber operations in neutral territory 42–43, 556–558
  - inviolability of neutral territory in 555
  - mere passage regime 233, 245
  - obligations of neutral States in 557–560
  - protection of neutral cyber infrastructure 553–554
  - responses to violations of 560–561
  - and UN Security Council obligations 562
- neutralisation, of military objectives 443
- Nicaragua* Case (*Military and Paramilitary Activities in and against Nicaragua, ICJ*)
  - on armed attacks notion 330–331, 341–342, 344
  - on compelling another State into compliance with international legal obligations 317
  - and effective control notion 96–97

*Nicaragua Case (Military and Paramilitary Activities in and against Nicaragua, ICJ)* (cont.)

on prohibited interventions/non-intervention principle 315, 317, 319–320, 322

on self-defence right 356

on use of force 331–332

non-compliance with international law obligations

and plea of necessity 135 *see also* wrongful acts

non-derogable human rights 202–203, 208

non-discrimination requirement, for human rights limitations 206–207

non-forceful measures 348–349, 358

non-international armed conflicts 385–391

criteria for existence of 379–380, 385, 388–391

geographical limitations of 386–387

law of armed conflict applicable to 377

attacks on objects indispensable to survival of civilian population 532–533

blockades 507

civilians/civilian status

presumption 414, 425

combatant immunity notion 407–408

distinction principle 421

improper use of neutral indicators prohibition 503

non-intervention principle 156–163, 314–317, 326

for States 312–325

for UN 312, 325–327

non-kinetic armed attacks 340

non-State actors

armed attacks by, and self-defence right 340, 344–346

cyber operations by 174–176

and attribution to States 94–100

and countermeasures 113–114, 131, 137–138

and due diligence principle 35–36

on high seas 235

and State sovereignty 17–18

dispute settlement obligations of 305

responsibility of 381

State responsibility for 95, 99

and use of force prohibition 330–332

North Korea, harmful cyber operations by 91, 130–131

notification requirements

for countermeasures 118, 120

for invocation of responsibility 148

nuclear electrical generating stations, cyber attacks on, and duty of care 529–531

*Nuclear Weapons Advisory Opinion (Legality of the Threat of Use of Nuclear Weapons)* (ICJ) 338, 340, 420, 451

objective territorial jurisdiction 56–57

objects of attack 346, 423

obligations

breaches of *see* violations

of diplomatic law

receiving States 217–219, 226–227

third parties 221–222

of international law

*erga omnes* obligations 152–153

peremptory norms 110–111, 123–124

of neutral States 557–560

of occupying powers

to respect protected persons 544–546

to restore and ensure public order and safety 546–548

to safeguard capital value of immovable State property 550

of parties to armed conflicts

to care for dams, dykes and

nuclear electrical

generating stations

529–531

to respect and protect

civilian population 476–478

cultural property 534–536

- medical and religious personnel,
  - medical units and transports 513–515
- to take precautions in attack *see* precautions in attack
- of States 16
  - to attempt peaceful settlement of disputes 303–311
  - to comply with and implement UN Security Council resolutions 110, 358, 562
  - of due diligence 30–43
  - to establish, maintain, and safeguard international telecommunication infrastructure 288–291
  - to respect and protect human rights 181, 196–202
  - to respect and protect UN personnel 368–371
  - to respect the sovereignty of other States 17–27
  - to respect space activities 277–279
  - responsible for internationally wrongful acts 142–153
    - to review weapons 464–467
  - of treaties 367–368
    - and countermeasures 114–115
- occupation, law of 543–544
  - collective punishment prohibition in 539–540
  - confiscation/requisition of property rules in 549–552
  - and enforcement jurisdiction 68
  - protection of civilians in 544–546
  - public order and safety restoration measures 546–548
  - and security of occupying powers 548–549
- Oil Platforms Case (Iran v. United States, ICJ)* 126
- omission, and compliance with due diligence 43
- online presence, of diplomatic missions 216–217, 224, 227
- operational zones 507–508
  - cyber operations in support of 510–511
  - penetration of 508
- opinion, freedom of *see* freedom of expression
- organised armed groups
  - combatant status of members of 403–405
    - and targetability 426–428
  - and international armed conflicts 380–383
  - and non-international armed conflicts 389–391
  - prohibition to conscript/enlist children in 525
  - virtual 390
- organs of international organisations 158–160
- organs of State 87–88, 99
  - and attribution 87–94
  - corporations as 88–89, 97
  - and governmental authority 89–91
- originators of cyber attacks 344–346
  - concealing of 494
  - identification of 420
- outer space, law applicable to
  - cyber operations in 261, 270–283
- Outer Space Treaty
  - on military activities in outer space 273, 275–276
  - on peaceful purposes of space activities 276
  - on respect for space activities 278
  - on responsibility and liability 281
- overall control test 380–382
- paramilitary groups, incorporated into armed forces 406–407
- participation
  - in commission of war crimes, and criminal responsibility 395–396
  - in military activities, compulsion prohibitions 523–524, 546
    - see also* direct participation in hostilities

- passage rights
  - of aircraft 262–264, 266
  - military 264–265, 267
  - of humanitarian assistance operations 541
  - of vessels 233, 241–245, 250–252
- passive cyber defences 453, 566
- passive personality principle 64–65
- passive precautions duty 487–491
- PCIJ (Permanent Court of International Justice)
  - Phosphates in Morocco Case (Italy v. France)* 84
  - on reparations 144
- peace, threats to, and UN Security Council measures 327, 357–360
- peace operations 159, 163–164, 361–368
  - protection of persons involved in 368–371
- peaceful purposes 233–234
  - of cyber operations in outer space 273–277
- peaceful settlement of disputes, obligations to attempt 303–311
- penetration of zones, and imminence of armed attacks 508
- peremptory norms of international law 123–124
  - violations of 110–111, 124
- perfidy prohibition 491–495
- Permanent Court of Arbitration, *Island of Palmas* Arbitral Award (*Netherlands v. United states*) 11
- Permanent Court of International Justice *see* PCIJ
- personnel
  - medical, protection of 513–515, 517–519
  - religious, protection of 513–514
  - of UN, protection of 368–371
- phishing 566–568
- Phosphates in Morocco Case (Italy v. France, PCIJ)* 84
- piracy, enforcement jurisdiction over 67, 236
- platforms, jurisdiction over 27–29, 244
- plea of necessity 135
  - based on essential interests 135–142, 166
  - and countermeasures 114, 135–142
  - and gravity of peril 136–137
  - precluding wrongfulness 108, 166
- political coercion 331
- precautions in attack 476
  - cancellations/suspensions of attacks 483–484
  - choice of targets duty 481–483
  - constant care duty 476–478
  - means and methods of warfare choice 479–481
  - and proportionality 481
  - verification of targets duty 478–479
  - warning duty 484–487
- presumptions
  - of civilian status 424–425, 448–451
  - against direct participation in hostilities 432–433
  - of legality, and use of force regime 336–337
  - of public ownership, for confiscation and requisition of property during occupation 550–551
- prevention
  - of exercise of belligerent rights 560–561
  - of harmful cyber operations/attacks, and due diligence principle 44–47
  - of human rights abuses 198–199
  - state obligations of 31–32
- prisoner of war status, entitlements to 407, 411
- privacy rights, in cyber context 189–193, 287
- private contractors, targetability of 427
- private property rules on confiscation/requisitioning, in occupation 550–551

- propaganda, spread of
  - as direct participation in hostilities 528
  - and innocent passage regime 242
  - and prohibition of intervention 237
  - and state sovereignty 26
  - and transit passage regime 250
- property
  - confiscation/requisition of, in occupation 549–552
  - cultural
    - protection of 534–536
    - targeting rules applicable to 463, 485, 534–536
  - destruction of, and perfidy 494
  - of States
    - cyber infrastructure, and immunity 73
    - and obligations of occupying powers 550 *see also* civilian objects; dual-use objects; military objectives
- proportionality principle
  - in countermeasures 127–130
  - in cyber attacks 470–476
  - and precautions requirements 481
  - in exercise of self-defence right 348–350
  - in human rights limitations 204–205
- Prosecute or Extradite Obligation Case (Belgium v. Senegal, ICJ)* 152
- prosecution *see* criminal responsibility
- protect, obligation to
  - in diplomatic law 217–219, 226–227
  - in human rights law 181, 196–202
  - and non-intervention principle 323
  - of parties to armed conflicts 476–478, 513–515, 534–536
- protections in armed conflict 512–513
  - of children 524–526
  - of civilians/civilian objects 413–414
  - distinction principle 420–422
  - and occupation 544–546 *see also* direct participation in hostilities; precautions in attack
- of cultural property 463, 485, 534–536
- of detained persons 519–524
- of journalists 526–528
- of medical personnel, units, and transport, computers, systems, and networks 513–515
- loss of 517–519
- of natural environment 537–539
- of neutral cyber infrastructure 555–556
- of objects indispensable to survival of civilian population 531–533
- of religious personnel 513–514
- of UN personnel and equipment 368–371
- protective emblems, improper use prohibitions 496–498
- protective principle 63–64
- protracted violence requirement for non-international armed conflicts 388
- proximity operations 282–283
- punishments, collective, prohibition of 539–540
- purposes
  - of countermeasures 116–122
  - criterion for military objectives 439–440
  - legitimate, for limitations on human rights 203
  - peaceful 233–234
    - of cyber operations in outer space 273–277
  - of reparations 144
- radio frequencies, harmful interference with 294–298
- reasonableness tests/standards 49–50, 81–82, 191
- receiving States 209
  - obligations of 217–219, 226–227
- reciprocity, in diplomatic relations 212

- Red Cross/Crescent/Crystal
  - improper use prohibition 497–498
  - see also* ICRC
- regional organisations
  - enforcement of UN Security Council measures by 360–361
  - jurisdiction exercised by 155
- registration, States of
  - jurisdiction of
    - over space objects 277–278
    - over vessels and aircraft 63, 263
- religious personnel, protection in
  - armed conflict of 513–514
- remedial measures requirement 46–47, 49–50, 83
- remedy, human rights law obligations
  - to provide 200–201
- remote cyber operations 20, 168–169, 509
  - and diplomatic immunities 213–214
  - and human rights law 193
  - and State sovereignty 19–22
- rendezvous space operations 282–283
- reparations, for internationally wrongful cyber operations
  - 144–152
- repeated actions, as direct participation
  - in hostilities 432
- reporting requirements, for exercise of self-defence 355–356
- reprisals 111–112
  - Additional Protocol I on 463–464
  - belligerent 112, 124, 460–463
- requisition of property
  - in occupation 549–552
  - and targetability 447–448
- respect, duty to
  - for human rights 181, 196–202
  - of occupying powers 544–546
  - of parties to armed conflicts
    - 476–478, 513–515,
    - 534–536
  - for space activities 277–279
- responsibility
  - criminal for war crimes
    - of commanders/superiors 394, 396–400
    - individual 391–396
  - of international organisations
    - 153–167
  - of non-State actors 381
  - of States 79–81
    - for cyber operations 80–81, 84–87
    - and attribution of wrongful acts
      - 81–83, 87–100, 115–116
    - and countermeasures 82–83
    - from governmental infrastructure
      - 91–92
    - by non-State actors 94–100
    - by other States 100–104
    - in outer space 279–283
    - exceptions 104–111, 135–142
- responsible States 80
- restitution 149–150
- retaliation 353–354
- retorsion 112
- retroactive nature, of countermeasures
  - 118
- reversibility, of countermeasures 119
- right to be forgotten 195–196
- right to health 194
- right to privacy 189–193, 287
- right to visit warships 235–239
- Rome Statute *see* ICC (International Criminal Court) Statute
- rootkit 566
- ruses
  - use of 442, 501
  - legitimacy of 495–496
  - warnings as 487
- Russian Federation, cyber operations in
  - international armed conflict with Georgia (2008) by 376
- safety
  - during occupation, restoration of
    - 546–548
  - of civil aviation, and cyber operations 268–269
  - of government telecommunication
    - 287
  - of life, in telecommunication law 287
  - see also* security
- St Petersburg Declaration (1868) 420, 434–435



- sanctuary, provision of, and use of force 332
- satellites
  - earth orbits of 299
  - military 299–300
  - use of
    - dual-use 277
    - law applicable to 261, 270
- satisfaction 151–152
- SCADA (Supervisory Control and Data Acquisition) 567
- scale and effects requirement for
  - armed attacks 341–342, 344
- secrecy, of telecommunications 287
- security
  - collective
    - peace operations 361–371
    - UN Security Council's role in 327, 357–362
  - cyber, international cooperation in 131–133
  - national, and protective principle 63–64
  - of occupying powers 548–549 *see also* safety
- self-defence
  - anticipatory 118, 139, 350–354
  - armed (cyber) attacks triggering 107, 139, 339–348, 354–355
  - imminent attacks 350–354
  - collective 354–355
  - necessity and proportionality
    - principle in 348–350
  - in outer space 274–275
  - reporting requirements 355–356
- self-determination rights 383
- sending States 209
- servers/server farms 567
- severity
  - for assessments of losses 530
  - for assessments of use of force 334, 336
  - of cyber operations against States
    - and attribution 82
    - directed at critical cyber infrastructure 140–141
    - remote cyber espionage 170–171
  - for human rights infringements 204–205
- ships
  - cyber operations on board of, and right to visit 235–239
  - jurisdiction over 27–28, 232–233
  - nationality of 63
  - passage rights of 233, 241–245, 250–252 *see also* law of the sea
- Simma, Judge 126
- sniffer software 566–567
- social media
  - military use of 446
  - sovereign rights over 14–15
- social rights, in cyber context 194
- Sony Corporation 130–131
- sovereign equality, principle of 16–17
- sovereign immunity
  - over cyber infrastructure/operations 27–29
  - of vessels and aircraft 241–242, 244, 250–251
- sovereignty
  - and international organizations 13, 155–156
  - of States 11–12
    - and control over cyber infrastructure/operations 12–17, 290–292
    - and cross-border actions in self-defence 347–348
    - violations of 17–27, 173
- space *see* cyberspace; outer space
- Space Debris Mitigation Guidelines 274–275
- space law
  - and air law 259–260
  - applicable to cyber operations 270–283
- space objects 271
  - jurisdiction over 277–278
- spear-phishing 567–568
- special missions 210–211
- spies
  - combatant immunity for 409–412 *see also* espionage

- spill-over
  - of armed conflicts into neighbouring states 379
  - effects of cyber attacks in neutral territory 555
- spoofing 91–92, 120, 567
- spying *see* espionage; spies
- standards
  - of care 279
  - of constructive knowledge 40–42
  - for last window of opportunity 351–353
  - for reasonable expectations 191
- starvation of civilians prohibition 459–460
- States
  - archipelagic, rights and duties of 251–254
  - coastal
    - enforcement jurisdiction of 246–248
    - rights and duties of 240–245, 249
    - over submarine cables 14, 253–256
  - consent of
    - for peacekeeping operations 363–364
    - and preclusion of wrongfulness 104–107, 166, 323
    - to enforcement jurisdiction of another state 68–69
    - to humanitarian assistance operations 541
  - cyber capabilities of 339
  - immunity of, from foreign jurisdiction 71–74
  - injured 80
    - contribution to harm by 140–141, 147
    - rights to countermeasures 82–83, 111–116, 130–133
  - involvement of, and use of force regime 336–337
  - jurisdiction over cyber
    - infrastructure/operations 51–54, 68
    - aircraft and vessels 27–28, 63, 232–233, 246–248, 263
    - space objects 277–278
  - land-locked, access rights of 255
  - launching 271–272, 281
  - neutral 553, 557–560
  - obligations of 16
  - property of
    - cyber infrastructure as 73
    - and obligations of occupying powers 550
  - responsibility of 79–81
    - for cyber operations 80–81, 84–87
    - and attribution of acts 81–83, 87–100, 115–116
    - countermeasures permissible 82–83
    - from governmental infrastructure 91–92
    - by non-state actors 81–83, 87–100, 115–116
    - by other States 100–104
    - in outer space 279–283
    - exceptions 104–111, 135–142
  - responsible 80
  - sovereignty of 11–12
    - and control over cyber infrastructure/operations 12–17, 290–292
    - and cross-border actions in self-defence 347–348
    - violations of 17–27, 173
  - territories of 261–262
  - ultra vires* acts by 89
  - steganography 567
  - Stuxnet operations (2010) 342, 384, 567
  - subjective territorial jurisdiction 56–57
  - submarine cables
    - law of the sea applicable to 14, 252–258
    - and neutrality/occupation law 510, 551–552
    - occupation law applicable to 551–552
  - suffering, unnecessary 420, 453–455
  - superiors, criminal responsibility of 394, 396–400
  - supervision, of space activities 279–283
  - surveillance
    - of diplomatic correspondence 222–223
    - mass 170–171

- survival of civilian population
  - assurances of continued computer operations essential to 546
  - prohibition of attack on objects indispensable to 463–464, 531–533
- suspension
  - of attacks 483–484
  - of cyber communications 291–294
  - of treaties 109, 115
- Tadić* Case (ICTY) 380–381, 388, 393, 421
- Tallinn Manual
  - authority of 2–3
  - commentary 4
  - drafting of 5–6
  - ‘Hague Process’ xxvi, 2, 6–7
  - international group of experts 2
  - rules 4
  - scope of 3
  - supporters 6–7
  - terminology 4–5
- tapping of data, from submarine cables 257
- targeting rules of law of armed conflict 414–422
  - armed forces members 426
  - choice of target 481–483
  - civilian objects 434–435
  - civilians 419, 422–428
    - and direct participation in hostilities 413–414, 425, 428–432
  - government employees 427–428, 438
  - proportionality principle 481
  - cultural property 463, 485, 534–536
  - dams, dykes and nuclear electrical generating stations 529–531
  - distinction principle in 420–422
  - dual-use objects 445–447, 491
  - levée en masse participants 425, 428
  - medical personnel, units and transports, computers, networks and data 513–515, 517–519
  - military objectives 435–445, 469–470
  - natural environment 537–539
  - objects indispensable to survival of civilian population 463–464, 531–533
  - organised armed group members 426–428
  - religious personnel 513–514
  - UN personnel and equipment 368–371
  - verification of target 478–479 *see also*
    - combatant immunity;
    - proportionality principle;
    - protections in armed conflict
- Tehran Hostages* Case (*United States v. Iran*, ICJ) 99–100, 125, 382
- telecommunication law, international 273, 284–287
  - duty to establish, maintain and safeguard international telecommunication infrastructure 288–291
- harmful interference with wireless cyber communications/services 294–298
- military radio installations
  - exemption 298–300
- suspension or stoppage of cyber communications 291–294
- termination
  - of cyber attacks 353–354
  - of cyber communications 291–294
  - of direct participation in hostilities 431
  - of internationally wrongful cyber operations 142, 149
  - of military use of civilian objects 450–451
  - of occupation 544
  - of treaties 109, 115
- terminology problems 4–5
- territorial jurisdiction 52
  - objective/subjective 56–57
  - over cyber operations 55–60 *see also* extraterritorial jurisdiction

- territorial sea
  - cyber operations in, law of the sea
    - applicable to 241–248
  - rights over submarine cables in 253
- territories
  - neutral 553
    - cyber operations on 42–43, 556–558
  - inviolability of 555
  - occupied 543
  - physical control of, and precautions
    - against cyber attacks 489
  - of states 261–262
- terror, prohibition of spreading of 433–434
- terror spreading prohibition 434
- terrorism/terrorist groups
  - cyber attacks qualifying as 433–434
  - cyber operations by 18
    - and countermeasures 113–114
    - qualifying as armed attack 345
    - and responsibility of international organisations 164–165
    - state responsibility for 43–44, 47–48, 56–57
  - use of internet/social media 15, 199
    - for recruitment purposes 65 *see also* counterterrorism measures
- third parties
  - cyber activities directed against, and innocent passage regime 243
  - cyber operations by 32
    - and due diligence principle 42
  - effects of countermeasures on 133–134
  - obligations of, in diplomatic law 221–222
- threats
  - as prohibited intervention 322–323
  - to peace 327, 357–360
  - of use of force 338–339 *see also* force, use/threats of
- thresholds
  - of control, tests for 96–97, 380–382
  - of doubt, about civilian status 424
  - of harm 36–40, 416
  - of internationalization of armed conflicts 381–382, 386
  - of use of force 331, 333–337
  - of violence
    - for existence of armed conflict 370–371, 383–384
    - for existence of non-international armed conflict 388–389
- Trail Smelter* Arbitral Award 36–37
- transit
  - of aircraft 262–264, 266
  - military 264–265, 267
  - of data, and territorial jurisdiction 55–56
  - of diplomatic/consular
    - correspondence 221
  - States of, and obligations of States 33–34
  - of vessels, passage rights 233, 241–245, 250–252
- treaties
  - dispute resolution mechanisms in 310–311
  - enforcement jurisdiction provisions in 68–69
  - on human rights 179–180, 200
    - derogation provisions in 207–208
  - on international cooperation in law enforcement 75–77
  - obligations of 367–368
    - countermeasures for breaches of 114–115
    - and due diligence principle 35
- Turkey, publication of diplomatic correspondence in 226
- ultra vires* acts
  - by international organisations 159
  - by non-State actors 97–99
  - by States/organs of State 89–91, 94
- UN Charter
  - binding nature of 156–157
  - on good faith requirement 308
  - on international peace and security 305–306, 357, 359
  - intervention prohibition in 312, 325–327

- on peaceful dispute settlement
  - obligation 303–304, 308
- prohibition on threat or use of force
  - in 329
- on self-defence right 339, 355–356
- UN Emblem, improper use prohibition 499
- UN Guiding Principles on Business and Human Rights 200
- UN Office on Drugs and Crime, on terrorist use of Internet 199
- UN personnel and equipment, protection of 368–371
- UN Safety Convention 368–369
- UN Security Council
  - collective security role of 327, 357–360, 362
  - enforcement by regional organisations 360–361
  - enforcement jurisdiction powers granted by 69
  - resolutions
    - obligations to comply with and implement 110, 562
    - status of 114, 358
- unilateral actions, in dispute resolution 307
- United Kingdom, Additional Protocol Ratification Statements of 463, 475, 529, 532
- United States
  - agreement with China on cyber espionage 169
  - countermeasures policies of 82
  - cyber warfare policies of 473
  - DoD Military Manual 530, 547
  - harmful cyber operations against 118–119, 130–131
  - space policies 276
- Universal Declaration of Human Rights 179
- universal jurisdiction, over cyber crime 65–66
- unprivileged belligerents/belligerency 407
  - mercenaries 412–413 *see also* combatant immunity
- use criterion for military objectives 438–439, 448
- use of force
  - and armed attacks 332–333, 337, 341
  - in countermeasures 125–127, 140
  - cyber operations as 364–365
  - prohibited 233–234, 328–330
    - cyber operations qualifying as 330–339
  - in outer space 273–277
- UN Security Council authorisations for 359 *see also jus ad bellum*
- validity, of consent 104–107
- verification of target, duty of 478–479
- vessels *see* ships
- Vienna Convention on Diplomatic/Consular Relations 209
  - on free communication 226
  - on immunity 216, 231
  - on protection of archives, documents, and correspondence 221
  - on wireless communication equipment 230
- Vienna Convention of the Law of Treaties
  - on invalidity notion 107
  - on peremptory norms of international law 124
  - on suspension/termination of treaties 109
- violations
  - of human rights law 181–182
    - and remedy obligations 200–201
  - of international law
    - by cyber espionage 169–172
    - erga omnes* obligations 152–153
    - peremptory norms 110–111, 124
      - see also* wrongful acts
  - of law of neutrality, remedies available 560–561
  - of State sovereignty
    - by cyber espionage 173
    - by cyber operations 17–27
    - by non-State actors 17–18

- violence 415–416
  - consequences of 415–416
  - protracted 388
  - thresholds of
    - for existence of armed conflict 370–371, 383–384
    - for existence of non-international armed conflict 388–389
- virtual armed groups 390
- virtual confiscation/requisition 551
- virtual embassies 216 *see also* digital embassies
- virtual inspections, of ships 238–239
- visit, right to, and cyber operations 235–239
- Wall Advisory Opinion (Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, ICJ)* 152
- wanton destruction 538
- war correspondents 527
- war crimes, criminal responsibility for
  - of commanders and superiors for 394, 396–400
  - individual 391–396
- war-sustaining activities/objects,
  - targetability of 441–442
- warnings
  - duty of issuing of 484–487
  - effectiveness of 484–487
- warships
  - carrying neutral or enemy flags,
    - cyber attacks/operations from 502
  - right of visit 235–239
- weapons 452
  - cyber 406
    - testing of 242
    - transmission across neutral territory of 557–559
    - use of 268–269
  - of enemy, acquiring control of 451–452
  - obligations of review of 464–467
- Whaling Case (Australia v. Japan, New Zealand intervening) (ICJ)* 81–82
- wireless communication equipment/
  - networks
    - on board ships, and innocent passage regime 242–243
  - in diplomatic missions and consular posts 230
  - harmful interference with 294–298
- worship
  - protection of places of 514 *see also* religious personnel
- wrongful acts *see* internationally wrongful acts
- Yamashita Case (US Military Commission)* 398
- Zakharov v. Russia Case (ECtHR)* 207
- zones, operational 507–508
  - cyber operations in support of 510–511
  - penetration of 508