

---

# Index

---

- Aaltola, M 25  
Acharya, A 451  
Ackerman, R 446, 447, 448  
Afghanistan War 276, 324  
African Union Cybersecurity Convention (AU Convention) 192, 196, 197, 200  
Ago, R 58, 233, 244  
Akande, D 274, 327  
Akehurst, M 19, 31–2, 34  
Albright, D 243, 330  
Aldrich, R 123, 361  
Alexander, K 418  
Alston, P 337  
Ambos, K 118–43, 156  
Andress, J 229  
Anonymous group 157, 213  
Antolin-Jenkins, V 248, 249  
Antonopoulos, C 28, 55–71  
Aoki, K 76  
Appelbaum, B 324  
Arcaric, M 406  
Areng, L 429, 445  
Argomaniz, J 404–5  
Arias, A 206  
Arimatsu, L 121, 149, 228, 307, 326–42, 345, 368, 398  
Armacost, M 390  
armed force and conflict  
    classification of armed *see* classification of cyber warfare, international armed conflict  
    cyber attacks as ‘armed attacks’ 263–70, 272–3, 275, 276, 279–80, 281–2  
    cyber attacks and crime of aggression 138–9  
    cyber operation as *see* cyber operations as a use of force, as armed force  
    determining whether armed force has been applied 122–3  
    existence of, cyber attacks as war crimes 121–6  
    international humanitarian law applied to cyber warfare 371–4  
    law of armed conflict (LOAC), and law of neutrality 396–9  
Arquilla, J 212  
ASEAN Convention on Counter Terrorism 162  
Asia-Pacific cyber security 446–64  
    ASEAN CERT programs 454, 460, 462  
    ASEAN Cooperation Plan 455  
    ASEAN Defence Ministers Meetings (ADMMs) 454, 455  
    ASEAN Economic Community Blueprint 453  
    ASEAN Information Infrastructure and Hanoi Plan of Action 452  
    ASEAN Political-Security Community 454  
    ASEAN Regional Forum (ARF) 455–8  
    ASEAN Telecommunications and IT Ministers (TELMIN), ICT infrastructure and capacity development 452–4, 461  
    ASEAN Telecommunications and IT Ministers (TELMIN), Mactan Cebu Declaration 454  
    cyber security confidence building measures (CBMs) 449  
    cyberspace ‘rules of engagement’ measures 463  
    e-ASEAN Framework Agreement 452  
    geopolitical landscape 447–51  
    government vulnerability concerns 463  
    non-State actors involvement 449–50  
    regional approaches 451–63  
    Singapore Declaration 452–3  
    sovereignty considerations 447–8, 463  
    technological capabilities and cyber infrastructure disparities 449–50  
Asia-Pacific cyber security, Asia-Pacific Economic Cooperation (APEC) 458–62  
    Action Agenda for New Economy 458–9  
    Cybersecurity Strategy 460–61, 463  
    e-APEC Strategy 459, 460  
    international institution cooperation 462  
    private sector engagement 461–2  
    Security and Prosperity Steering Group (SPSG) 458, 460, 461–2  
    terrorist attacks, effects of 459  
attribution  
    and anonymity problems, classification of cyber warfare 333

- of attack to one of the parties to the conflict 125–6, 129
- identification problems 296, 362–4
- methods and collateral damage 322
- problems and due diligence, law of neutrality 394–5
- State responsibility *see* State responsibility, attribution in cyberspace
- Austin, G 83, 285, 286, 288, 289, 291
- Australia 41, 43, 49, 158–9, 446, 448, 449
- Azerbaijan 392
- Baker, C 175–7
- Baker, S 262
- Balmond, L 406
- Bannelier-Christakis, K 128, 130, 161, 228, 307, 308, 311, 314, 317, 343–65, 372, 398
- Barlow, J 13, 96–7
- Barnes, S 22
- Barrett, E 307, 312
- Barriga, S 138, 140, 141
- Barron-Lopez, L 287
- Bartelson, J 17, 18
- Baruah, D 465, 466, 475, 478, 480
- Barzashka, I 330
- Beal, V 55
- Beck, L 128, 129, 135, 136
- Beitollahi, H 264
- Belk, R 307
- Bellamy, A 314
- Benatar, M 138, 281
- Bendiek, A 404, 408, 409, 419
- Bently, L 96
- Berne Convention, intellectual property rights 74, 78, 79, 84
- Besson, S 16
- Bethlehem, D 18, 278
- Blair, D 223
- Blake, D 346
- Blakeney, M 74
- Blockmans, S 423, 425
- Blommestein, M van 212, 223
- Boczek, B 390
- Boothby, W 120, 123, 124, 129, 133, 134, 135, 232, 242
- Borgmann-Prebil, Y 417
- Borneman, W 381
- Bossuyt, F 419
- Bothe, M 351, 368
- botnets and remote control 309, 313, 315, 319 *see also* hackers
- Bouwmeester, H 370
- Bowett, D 272
- Brazil 113, 178, 179–80, 184, 473
- Brenner, S 191, 196, 200
- Brierly, J 33
- Brinkel, T 219
- Brkan, M 420–21
- Broad, W 243, 261
- Brölmann, C 21
- Brown, G 247, 249, 264, 330
- Brownlie, I 32, 187, 239, 266
- Bruguière, J-M 84, 85
- Bryant, R 15
- Buchan, R 56, 65, 104, 112, 119, 149, 168–89, 224, 225, 236, 241, 282, 317, 330, 398
- Buck, S 27
- Budapest Convention 149, 162–3, 192–7, 198–9, 200, 202–5, 412, 414, 418–19
- Burnham, G 310
- Burton, C 414, 417
- Byassee, W 15
- Caballero-Anthony, A 451
- Cammack, C 137, 139
- Carrapico, H 404
- Cartwright, J 347
- Cassese, A 121
- Cathcart, B 375
- Cavelty, M 437
- Cerf, V 109, 426
- CERTs (Computer Emergency Response Teams) 221–2, 223, 411, 440–41, 454, 460, 462
- Cesana, S 164
- Chadwick, O 388
- Chesney, R 337
- Chesterman, S 185, 226
- China 70, 111, 165, 319, 370, 457, 463, 478 and cyber espionage 114, 158, 168, 169, 172, 179, 184, 241, 245–6, 333, 448 Internet censoring and monitoring 45, 112–13, 115, 323 US–China cyber security working group 490
- Chowdhury, N 404
- Christakis, T 268
- Christie, D 325
- civilian population attacks against 128, 154, 160–61, 191, 242–5, 323–4, 372 consumer protection, EU cybersecurity law 411

- infrastructure damage and indirect killing 310
- principle of distinction *see under* principle of distinction, relevance of
- principle of proportionality 372–3  
*see also* collateral damage
- Clark, R 140, 141
- Clarke, R 188, 224–5, 253, 260, 317
- classification of cyber warfare 326–42
  - actor identification problems 326
  - and international humanitarian law 326–7, 331–2, 335, 336, 339–40
- classification of cyber warfare, international armed conflict 328–35
  - anonymity and attribution problems 333
  - armed force use 328–32
  - by a State against another State 332–5
  - critical infrastructure and essential services, harm to 330–32
  - Distributed Denial of Service (DDoS) attacks 331
  - hactivist involvement 334–5
  - intensity and duration of violence, relevance of 330, 332
  - private sector actors' involvement 334–5 and State effective control 330, 334–5
- classification of cyber warfare, non-international armed conflict 336–41
  - definition 336, 339–40, 362
  - extension of weapons treaties to 327
  - geographical scope and territorial boundaries 337
  - intensity of hostilities 340–41
  - and international humanitarian law 339–40
  - organized armed group, involvement of 337–40
  - 'virtual group' involvement 338–40
- Clinton, H 109, 184
- Clough, J 190, 194, 195
- coercion use 181–3, 249, 250–52, 253
- Cohen, J 14–15, 22
- Cohen, M 76
- Colarik, A 229
- Coleman, G 213, 217
- collateral damage
  - and cyber weapons *see* ethical challenges of cyber weapons, collateral damage
  - dual use function and collateral effects 377–8
  - international humanitarian law applied to cyber warfare 373
  - principle of distinction *see under* principle of distinction
  - principle of proportionality 134–6  
*see also* civilian population
- Computer Emergency Response Teams (CERTs) 221–2, 223, 411, 440–41, 454, 460, 462
- Computer Incident Response Capability (NCIRC), NATO 429, 433, 444
- computer systems
  - botnets and remote control 309, 313, 315, 319
  - and computer companies as targets, and principle of distinction 360–61
  - copyright protection of software *see* cyberspace, intellectual property rights, copyright protection of computer software
  - 'digital divide' and right to development 107–8, 109–10
  - Distributed Denial of Service (DDoS) 242, 249–50, 259–60, 264, 265, 331, 392
  - evidence requirements and territorial location 63–5
  - facilities, law of neutrality 397, 399
  - forgery and fraud 196
  - hackers *see* hackers
  - identification and attribution 62–3, 69–70
  - integrity crimes 191
  - interconnectivity between military and civilian systems 131–3
  - malware 252–3, 257, 261, 308, 309, 312, 313, 444
  - network attacks 118–20, 186–8, 194
  - viruses *see* viruses
  - WIPO Model Provisions on the Protection of Computer Programs 84  
*see also* cyber attacks; Internet
- Connolly, K 52
- Constantinou, A 266
- Conti, G 232
- Cook, K 339
- copyright issues 48, 193, 197
  - protection of computer software *see* cyberspace, intellectual property rights, copyright protection of computer software
- Corn, G 327
- Cornish, P 227
- Correa, C 74
- Corten, O 237, 243
- Costa, J-P 356
- Crawford, J 19, 56
- Cremona, M 405, 422

- crime *see* cybercrime; international criminal responsibility
- Croom, C 230
- Cubby, B 159
- Curran, J 31
- Currie, R 182
- cyber attacks
  - as adjunct to traditional means 370–71
  - as ‘armed attacks’ 263–70, 272–3, 275, 276, 279–80, 281–2
  - definitions 346–7, 348
  - duration of attack 124–5, 129, 330, 332
  - hackers *see* hackers
  - viruses *see* viruses
  - see also* computer systems; individual countries; Internet
- Cyber Conflict Studies Association (CCSA) 289, 296
- cyber defence and NATO *see* NATO and cyber defence
- cyber deterrence, and international cooperation, need for strengthening 166
- cyber deterrence and public international law 284–304
  - consequence based approach 300–301
  - and critical infrastructures 302–3
  - cyber attacks in support of military attack with conventional means 285
  - cyber weapons’ use 284
  - EastWest Institute, *A Measure of Restraint in Cyberspace* 288–9
  - imminence of attack 301–2
  - NATO’s collective defence 291
  - nuclear-deterrence *see* nuclear deterrence
  - protection via deterrence 290–91
  - retaliation via offensive means 291
  - security against cyber treats 286–90
  - UN Charter on the threat and use of force 299–302
  - UN General Assembly (UNGA) and protection of critical information infrastructures 288
  - US Presidential Decision Directive on cyber capacity 284, 297–8
- cyber deterrence and public international law, cyber deterrent feasibility and technical considerations 295–8
- nuclear deterrence, differences from 296–7, 299
- potential adversaries, identification problems 296
- self-defence, both passive and active 297–8, 299, 300–302, 304
- terminology problems 297–8
- cyber deterrence and public international law, security of critical infrastructures 287–90
- Critical Information Infrastructure (CII) 288–9
- military security and nuclear power plants 288–9
- peacetime protection of critical infrastructures 289
- cyber espionage 212, 219–20, 222, 224–6, 230, 311, 316–17, 369, 398–9, 408
- cyber espionage and international law 168–89, 180–88
  - accessing and copying of electronic information 171
  - coercion and violation of territorial integrity 181–3
  - definition 170–74
  - espionage as permissible exception to non-intervention principle 185
  - Google cyber attack 168, 184
  - international humanitarian law 172
  - Mandiant Report 168, 169, 333
  - non-State actors 172–4
  - in peacetime 172
  - principle of non-intervention 180–86
  - prohibition against use of force and argument for inclusion of computer systems 186–8
  - sovereignty over information in cyberspace 183–4, 186
  - sovereignty as protection of territorial and political integrity 182, 183
  - States’ refusal to accept responsibility for espionage when accused 195–6
  - Tallinn Manual *see* Tallinn Manual
  - transboundary espionage 171–2
  - UN Charter and prohibition against use of force 186–8
  - US spy plane incident (Gary Powers) 177
- cyber espionage and international law, as threat to international peace and security 174–80
- confidential information from private companies 179
- espionage inhibits and deters functional cooperation claim 177–8
- espionage as tool that enables functional cooperation argument 175–7
- human rights violations 179–80
- increased knowledge of other States’ capabilities argument 174–5

- information storage and speed of access 178–9
- international agreements, compliance and verification mechanisms 176–7
- national infrastructure information 179
- sovereign equality of States 175, 177–8, 179–80
- cyber exploitation and cyber attacks, difference between 240–42
- cyber network attack (CNA) definition 264
- cyber operations 211–32
  - ‘air gap’ protection 212
  - Budapest Convention (Council of Europe Convention on Cybercrime) 149, 162–3, 192, 193–4, 412, 414, 418
  - common operational means and methods 217–18
  - cyber sabotage (cybotage) 212
  - cyberspace virtual layers 221–2
  - diversity in strategic objectives 215–17
  - hackers *see* hackers
  - military cyber operations 212–13, 214, 226–32
  - military cyber operations, operationalizing 230–32
  - military cyber operations, ‘targeting’ process 232
  - national security strategy 215–16
  - non-profit organizations and pressure groups 217
  - operationalizing cyber operations 229–32
  - private enterprises digitally collecting and providing information 211–12, 222
  - private enterprises supplying tools to enable cyber activities 216, 222
  - software monitoring 218
  - State’s critical infrastructure, digital nature of 216
- cyber operations, State-level cyber paradigms 218–29
  - CERTs (Computer Emergency Response Teams) 221–2, 223, 411, 440–41, 454, 460, 462
  - governance and public-private involvement 222, 223
  - intelligence and counter-intelligence 224–6, 230
  - Internet governance and diplomacy 220–21
  - law enforcement 222–4, 230
  - military operations 226–9
  - military operations, ‘adequate’ legal basis requirement 228–9
  - protection of (critical) infrastructure 221–2
  - securitization and digital surveillance 219–20, 222
  - see also* ‘State’ headings
- cyber operations as a use of force 233–54
  - Distributed Denial of Service (DDoS) 242, 249–50
  - HPCR Manual on International Law Applicable to Air and Missile Warfare* 238, 240
  - UN General Assembly conditions 234–5
  - UN General Assembly’s Declaration on the Definition of Aggression 237
- cyber operations as a use of force, as armed force 235–40
  - arming and training of armed groups as use of force 238
  - cyberspace as fifth domain of warfare 239–40
  - effects of the action and direct destructive effects on property 236–7
  - identified by reference to instruments used 237
  - instrument-based approach and use of weapons 236
  - and intention to coerce 236–8
  - malware as weapon 238–9, 243, 244–5
  - target-based approach, conducted against national critical infrastructure (NCI) 236
  - weapons definition 238
- cyber operations as a use of force, UN General Assembly (UNGA) prohibition of use of force 235–6, 237, 238, 240–53
  - conduct related to cyber attacks and malware supply 252–3
  - cyber attacks causing physical damage to property, or injury of persons 242–5
  - cyber attacks severely disrupting the functioning of infrastructures and security 245–50
  - cyber exploitation and cyber attacks, difference between 240–42
  - cyber exploitation as violation of sovereignty 241
  - cyber infrastructure used to launch cyber attack 253
  - data deletion as use of force, but without physical damage 244–5
  - disruptive cyber operation as use of force, need to establish 248
  - economic targets as economic coercion 249
  - minimum threshold of gravity debate 243–4

- serious disruption of essential services
  - without destroying infrastructures 247
- significant disruption of essential services 249–50
- violation of the principle of
  - non-intervention and use of coercion 250–52, 253
- virus attacks 244–5
- website defacement 252
- cyber security
  - Asia-Pacific *see* Asia-Pacific cyber security
  - cyber attacks severely disrupting, UNGA 245–50
  - human rights 112–15
  - intelligence information 224–6, 230, 259
  - law, EU *see* EU cybersecurity law
  - UN regulation *see* UN and the regulation of cyber security
  - see also* cyber deterrence; cyber terrorism
- cyber terrorism 147–67
  - comprehensive instrument and regulation need 163–7
  - concept 147–51
  - data retention schemes 167
  - definition, lack of an agreed legal 147–8, 152
  - facilitative acts of terrorism 150–51
  - and general Internet use by terrorist groups 150
  - hacking techniques 157, 158
  - international humanitarian law applied to cyber warfare 369–70
  - International Telecommunication Union (ITU), model cyber crime legislation 165
  - international treaty, lack of 149
  - as new terrorist tactic 148
  - political motive element and organised crime overlap 149–50
  - prohibited harms to protected targets 153–4
  - as prohibited intervention 148–9
  - regional and national instruments 149, 162–3, 166–7
  - supervisory control and data acquisition (SCADA) systems 147
  - Tallinn Manual *see* Tallin Manual
  - technical measures, possible necessary 165–6
  - terrorist groups, lack of perceived threat from 164
  - UN Draft Comprehensive Anti-Terrorism Convention, terrorist offences
    - definition 155–7, 158, 159, 160, 161–2
    - UN Global Counter-Terrorism Strategy 151
    - US excessive intelligence collection
      - methods, criticism of 167
    - see also* cyber security
- cyber terrorism, cyber attacks and general international crime of terrorism 155–62
  - civilian population, spreading terror among 160–61
  - customary international law crime of transnational terrorism 155–6, 158
  - industrial protest as terrorism, problems with 159–60
  - international humanitarian law and principles of distinction and proportionality 160–61
  - private motivation for attacks 158–9
  - ‘special intent’ element 158
  - State-sponsored cyber attacks 158, 161–2, 164
- cyber terrorism, ‘sectoral’ international anti-terrorism conventions 151–5
  - attacks against protected persons 154
  - cyber ‘weapon’ concept 154
  - ‘physical attack’ question 153–4
  - violence understood as physical force 154
- cyber warfare 119–20, 408, 436–7, 438
  - classification *see* classification of cyber warfare
  - and humanitarian law *see* international humanitarian law applied to cyber warfare
  - war crimes *see* international criminal responsibility, cyber attacks as war crimes
- cyber weapons
  - concept 154, 284
  - ethical challenges *see* ethical challenges of cyber weapons
  - international criminal responsibility 139
  - treaties, extension of 327
- cybercrime
  - Cybercrime Convention of the Council of Europe 118
  - definition 118, 407–8
  - EU Cybercrime Centre (EC3), EU cybersecurity law 409, 413
  - EU Cybercrime Convention Committee (T-CY) 418–19
  - Eurojust cross-border prosecution 409, 412, 413
  - UN Office on Drugs and Crime (UNODC) 489
  - see also* international criminal responsibility

- cybercrime, international legal dimensions
  - 190–207
  - adjudication and enforcement 201
  - awareness-raising campaigns 205
  - child pornography 196–7
  - comprehensive multilateral instrument, need for 206
  - computer integrity crimes 191
  - computer-related forgery and fraud 196
  - cooperation between States 198–9
  - copyright issues 193, 197
  - ‘crimes’ committed in virtual worlds 191
  - cybercrime definition 190–92
  - data retention requirements 203
  - denial of service attacks 195
  - EU Council of Europe Convention on Cybercrime (Budapest Convention) 149, 162–3, 192–7, 198–9, 200, 202–5, 412, 414, 418–19
  - EU Framework Decision 162, 192–3, 202–3, 415
  - harm to property or persons 191
  - human rights and liberties protection 199, 203–4
  - illegal interception and protection of
    - privacy of electronic communication 194–5
  - intellectual property issues 193
  - international regime to fight cybercrime 198–200
  - international substantive law 192–8
  - jurisdiction problems 200–203, 206–7
  - mutual assistance and extradition 199–200
  - national legislation and fragmentation 201
  - offences where a computer system is
    - targeted intentionally 194
  - penalties for illegal access 194
  - personal data protection 204
  - privacy rights 203–4
  - production and distribution of devices used to commit offences 195–6
  - safe havens, need for elimination of 206
  - search and seize powers and territorial issues 199
  - self-regulation 204–5
  - service providers, liability and responsibility 203, 205
  - similar activities with different legalities in different countries 193
  - sovereignty issues 196–7
  - spamming 195
  - State of origin and State of destination
    - conflict 202–3
    - system interference 195
    - technical means of protection and preventive measures 204–5
    - territoriality principle of regulation and enforcement 198–200
    - UN Convention against Transnational Organized Crime (Palermo Convention) 198, 199
- cyberspace
  - data protection *see* data protection
  - definition 14–24
  - as global commons *see* cyberspace, legal status, cyberspace as global commons
  - human rights *see* human rights
  - law of neutrality *see* law of neutrality
  - virtual layers 15, 221–2
- cyberspace, infrastructure
  - ASEAN, ICT infrastructure and capacity development 452–4, 461
  - collateral damage and malfunction of civilian facilities 349–50, 354
  - critical infrastructure and essential services, serious disruption of 245–50, 268–70, 302–3, 310, 330–32
  - cyber infrastructure used to launch cyber attack 253
  - dual-use of cyber infrastructure and principle of distinction 131–3
  - property, harm to property or persons, cybercrime, international legal dimensions 191
  - protection of critical 221–2
  - secure ICT infrastructure, NATO and cyber defence 433–4
  - security of critical *see* cyber deterrence and public international law, security of critical infrastructures
  - State’s critical infrastructure, digital nature of 216
  - technological capabilities and cyber infrastructure disparities 449–50
  - UN General Assembly (UNGA), cyber attacks causing physical damage to property 242–5
- cyberspace, intellectual property rights 72–93
  - Berne Convention 74, 78, 79, 84
  - cybercrime, international legal dimensions 193
  - EU intellectual property laws 80–83
  - EU Unitary Patent Regulation 81, 84
  - European Patent Convention (EPC) 78, 81, 83–4, 91
  - in international law 73–7

- Paris Convention 74, 78, 80
- property and sovereignty, distinction in law 75–7
- trade marks and domain names 91–2
- TRIPs Agreement 74, 79, 80, 84
- Uniform Domain Name Dispute Resolution Policy (UDRP) 74, 92
- cyberspace, intellectual property rights,
  - copyright protection of computer software 83–91
  - ‘author’s own intellectual creation’ 85–7
  - EU Database Directive 84–5
  - EU Information Society Directive 90–91
  - EU Software Directive 84, 85–7, 88, 90
  - idea–expression dichotomy principle 88–9
  - ISPs and ‘notify-and-take down’ approach 87–8
  - non-literal copying of software 88
  - permitted acts with regard to computer programs 90–91
  - possible cyber attacks and response of international law 89–90
  - protection of computer-related inventions by patent 1 91
  - software originality definition 85–6
  - WIPO Copyright Treaty 74, 84
- cyberspace, intellectual property rights, territorial nature 77–83
  - EU copyright law and territoriality principle 81–2
  - EU supranational laws and harmonisation of intellectual property laws 80–82
  - international conventions 78–9
  - lex loci protectionis* 79, 82–3
  - private international law 82–3
  - in public international law and intellectual property law 77–82
  - relaxation of territoriality principle 79
- cyberspace jurisdiction 30–54
  - competence under public international law 31–5
  - enforcement jurisdiction 51–3
  - international law scope 31–3
  - jurisdictional principles versus legal harmonisation 34–5
  - piracy sites, blocking 52–3
  - self-censorship 53
  - States claiming regulatory competence in parallel 33–4
  - territorial fragmentation of the internet 52–3
  - territoriality principle and sovereignty 33
  - transnational corporations, power and interests of 31
  - transnational online publishing 30–31
  - see also* cyberspace, legal status; legal dimensions
- cyberspace jurisdiction,
  - adjudicative/legislative jurisdiction 35–51
  - advertising and selling drugs 39, 50
  - copyright claims 48
  - defamation and data protection 43–5, 47
  - democratic legitimacy problems 38
  - destination approach and accessibility 38–44
  - destination approach and targeting 44–7, 48–9
  - destination approach under customary international law 47–9
  - effects doctrine 48
  - ‘everything that is not prohibited is permitted’ approach 36–7
  - free trade commitments 42–3
  - online gambling 40–42, 47
  - origin approach 49–51
  - publishing pornography 39
  - State’s legal standards 35–6
  - surfers purchasing artefacts from third parties 38–9
  - territoriality principle within non-territorial cyberspace 37–51
  - trademark owners 45–6
  - US due process requirement 47
  - voluntary compliance or enforcement via local intermediaries 49
- cyberspace, legal status 13–29
  - cyberspace definition 14–24
  - cyberspace global domain within the information environment 15
  - cyberspace layers 15, 221–2
  - future challenges 28–9
  - see also* cyberspace jurisdiction; legal dimensions
- cyberspace, legal status, cyberspace as global commons 24–8
  - Antarctica, legal status as example 26–7
  - cyberspace differences from other global commons 28
  - high seas designation 25–6
  - and Outer Space Treaty 26
  - and sovereignty principle 27–8
- cyberspace, legal status, sovereignty and international law 16–24
  - activities endangering important national interests 20
  - cyberspace as sovereign entity, and self-determination by community 22–4

- deterritorialisation as detachment of
  - regulatory authority from a specific territory 21–2
- effects doctrine 20
- external sovereignty power 17–18
- extraterritorial extension 16–17, 19
- indirect exercise 20–21
- jurisdiction 18–22
- no-sovereignty thesis and self-regulation 16
- power concept 18
- spill over effects 21
- technology regulation 21
- territory as element of sovereignty 18, 21
- cyberspace, self-defence in 255–83
  - ad hoc international institutions and rules for the Internet, need for 282–3
  - against non-State actors 276–80
  - against non-State actors, and private trans-border harm, difference between 279–80
  - anticipatory self-defence 270–73
  - collective self-defence 260, 270, 275–6, 434–7
  - conditions concomitant to exercise of 273–5
  - cyber attacks preceded/accompanied a conventional attack 260, 261–2
  - cyber attacks and unlawful use of force 263
  - cyber network attack (CNA) definition 264
  - cyber sanctions 281
  - cyber security intelligence information
    - sharing with private sector companies, call for 259
  - cyberspace as interconnection of electronic pathways 256
  - Distributed Denial of Service (DDoS) 259–60, 264, 265
  - EU Directive on attacks against information systems 269
  - immediacy, understanding of 275
  - industrial control systems, programmable logic controllers 261
  - information requests and use of
    - private-sector ISPs 264
  - Institut de Droit International, Santiago
    - Resolution on self-defence 266, 270–71, 277
  - jus ad bellum* legal approach 262–3
  - legal doctrine, prevailing approaches 262–3
  - malware 257, 261
  - National Strategies and Policies on cybersecurity 258–9
  - NATO, 2010 Strategic Concept 257–8
  - NATO, 2020 Report on cyber defence 274, 275
  - NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) 258
  - NATO and security challenges to critical infrastructure 270
  - Non-Aligned Movement (NAM) and anticipatory self-defence 271, 272
  - proportionality test 274–5
  - in response to armed attack 369
  - scepticism over 281–3
  - and Tallinn Manual *see* Tallinn Manual
  - topicality of cyber security 257–9
  - UN General Assembly Resolution on misuse of information technologies 280
  - UN Security Council and inherent right to self-defence 277–8
  - US Patriot Act 269–70
  - and violation of the principle of non-intervention 261–2
- cyberspace, self-defence in, UN Charter
  - Article 51 255, 261
  - and anticipatory self-defence 271–3
  - ‘critical infrastructure’ targeted by cyber attacks 268–70
  - customary law applying ‘separately from international treaty law’ 267–8
  - cyber attacks as ‘armed attacks’ 263–70, 272–3, 275, 276, 279–80, 281–2
  - and ‘use of force’ 265, 267
- cyberspace sovereignty
  - considerations, Asia-Pacific cyber security 447–8, 463
  - and cyber espionage 175, 177–8, 179–80, 182, 183–4, 186
  - cyber exploitation as violation of 241
  - and cybercrime, international legal dimensions 196–7
  - and cyberspace as global commons 27–8
  - and human rights 100–101
  - and intellectual property, distinction in law 75–7
  - and international law *see* cyberspace, legal status, sovereignty and international law
  - Internet freedom and Internet sovereignty
    - contrasts 111
    - and non-intervention policies 97
    - and territoriality principle 33
  - violations, and law of neutrality 380–81, 389, 394–5, 397–8
  - see also* State practice; State responsibility; territoriality

- Danton, J 80
- Dashwood, A 422
- d'Aspremont, J 173
- data protection 131, 204, 318, 416–17
- backup data use 316
  - data destruction, and principle of proportionality 375–6
  - deletion as use of force, but without physical damage 244–5
  - European Data Protection Supervisor (EDPS) 407–8
  - Internet and data transmission 398, 399
  - jurisdiction and defamation 43–5, 47
  - privacy rights 203–4
  - retention schemes, and cyber terrorism 167
  - supervisory control and data acquisition (SCADA) systems 147
- Davidson, O 354, 359
- Davis, J 260
- DDoS (Distributed Denial of Service) *see under* computer systems
- De Hert, P 193, 195, 202
- Deconinck, G 264
- Deeks, A 337
- Dehghan, S 261
- Dekker, I 295
- Delupis, I 185
- Demarest, G 170
- DeNardis, L 220
- Denmark, A 24
- Denning, D 157, 164, 312, 314
- Derclaye, E 86
- Derejko, N 337
- Dervan, L 132, 134
- deterrence *see* cyber deterrence
- 'digital divide' and right to development 107–8, 109–10
- Dinniss, H 119, 122–39*passim*, 143, 236, 263, 345, 346, 347, 351, 356, 361
- Dinstein, Y 123, 149, 237, 238, 240, 265, 267, 271, 273, 274, 285, 301–2, 303, 347, 382, 387
- Dinwoodie, G 73, 75, 78, 79, 80, 82
- Dipert, R 309
- Distefano, G 355
- Doerr, O 139
- Döge, J 263
- domain names 21–2, 74, 76, 79, 92, 116
- Dörmann, K 120, 124, 128, 129, 131, 133, 263, 329, 343, 348, 352
- Dörr, O 236, 237
- Doswald-Beck, L 238, 327, 348, 385, 387
- Drahos, P 72, 74
- Dreier, T 74, 78
- Droege, C 119–26*passim*, 129, 130, 131, 133, 136, 137, 143, 329, 341, 343, 347, 352, 353, 360, 364
- Drummond, D 168
- dual-use function 115, 131–3, 358–62, 377–8
- Ducheine, P 119, 211–32, 240, 366, 370, 407
- Dulles, J 292
- Dunlap, C 262, 359
- Dupert, R 261
- duration of attack 124–5, 129, 330, 332
- Easton, C 72
- EastWest Institute, *A Measure of Restraint in Cyberspace* 188–9, 288–9
- Eaton, J 62
- economic cooperation *see* Asia-Pacific cyber security, Asia-Pacific Economic Cooperation (APEC)
- economic, social and cultural rights 104–8
- economic targets as economic coercion 249
- Edwards, L 88
- Edwards, S 109
- Elisan, C 309
- Emerson, R 23
- Erdbrink, T 361
- Erlank, W 76
- espionage *see* cyber espionage
- essential services, serious disruption of 245–50, 268–70, 302–3, 310, 330–32
- see also* cyberspace, infrastructure
- Estonia, cyber attacks 56, 64, 221, 259–60, 262, 276, 335, 349–50, 429, 437–8, 475–6
- Estrin, D 341
- ethical challenges of cyber weapons 307–25
- autonomous propagation methods, avoidance of 317
  - backup data use 316
  - botnets and remote control 309, 313, 315, 319
  - cyber attack damage repair 316–17
  - cyber espionage to cyber attack escalation 311, 316–17
  - cyber weapons definition 309–10
  - infrastructure damage and indirect killing 310
  - justification for cyber attack 312
  - malware 308, 309, 312, 313
  - overkill tendencies 315
  - peculiarities of cyber weapons and differences from traditional weapons 310–11

- precision, lack of 308
- principle of responsibility for conduct in warfare 316–17
- product tampering and perfidy 312–14
- prolonged effect of damage 316
- system interdependence challenges 311
- targeting errors 314–15
- traditional counterattacks, combining with 312
- unreliability of cyber weapons 314–15
- ethical challenges of cyber weapons, collateral damage 317–25
- analysis costs and development of mitigation procedures 321–3
- attack propagation costs 320–21
- attribution methods 322
- blocking network services 323
- bulletin boards and blogs, use of 322
- denial-of-service attacks 319
- direct damage, costs of recovering from and costs of repair 320
- economic value of attacks 324–5
- and information extraction problems 318–19, 321
- psychological damage 323–4
- types 317–18
- vulnerability analysis 323
- EU
  - Copyright Directive 45, 86
  - copyright law and territoriality principle 81–2
  - Council of Europe Convention on Cybercrime (Budapest Convention) 149, 162–3, 192–7, 198–9, 200, 202–5, 412, 414, 418–19
  - Data Protection Directive 44
  - Database Directive 84–5
  - Directive on attacks against information systems 269
  - Electronic Commerce Directive 39, 41, 50–51
  - Europe-only communication network suggestion 53
  - exclusive origin rule 50–51
  - and facilitative acts of terrorism 150–51
  - Framework Decision on Attacks against Information Systems 162, 192–3, 202–3, 415
  - Information Society Directive 90–91
  - intellectual property laws 80–83
  - Online Music Recommendation 81
  - privacy and personal data protection 103
  - Software Directive 84, 85–7, 88, 90
  - Television Without Frontiers Directive 50
  - Trade Mark Directive 80
  - Unitary Patent Regulation 81, 84
  - website blocking 52
- EU cyber security law 403–25
  - anti-terrorism measures 424
  - Area of Freedom, Security and Justice (AFSJ) 405, 410–11, 413, 415, 420, 421, 424
  - CERT (Computer Emergency Response Team) 411
  - Common Foreign and Security Policy (CFSP) 413, 414, 419, 421–4
  - Common Security and Defence Policy (CSDP) 403, 413, 420–24
  - consumer protection 411
  - core EU values, inclusion of 411
  - Council of Europe Convention on Cybercrime (Budapest Convention) 149, 162–3, 192–7, 198–9, 200, 202–5, 412, 414, 418–19
  - cyber espionage 408
  - cyber resilience 408, 412
  - cyber security and cybercrime definitions 407–8
  - cyber war 408
  - Cybercrime Convention Committee (T-CY) 418–19
  - cybercrime reduction strategies 412–13
  - differing policy fields, need for combination of 405
  - Digital Agenda for Europe (DAE) 411
  - EU Commission Communication, ‘Network and Information Security’ 410, 411
  - EU Cybercrime Centre (EC3) 409, 413
  - EU Cybersecurity Strategy 411–14
  - Eurojust cross-border prosecution of cybercrime 409, 412, 413
  - European Data Protection Supervisor (EDPS) 407–8
  - European Information Sharing and Alert System (EISAS) 409
  - European Network and Information Security Agency (ENISA) 409, 411, 412
  - European Police College (CEPOL) 413
  - European Public-Private Partnership for Resilience (EP3R) 410
  - European Security Strategy 411
  - Europol support 408–9, 412, 413
  - EU–US Working Group on Cyber-Security and Cyber-Crime (WGCC) 408, 411, 414

- information sharing and mutual assistance 412
- institutional framework 408–10
- international cyberspace policy, establishment of coherent 414
- Internet regulation 406
- Lisbon Treaty 403–4, 413, 416, 420–21
- policies on cybercrime and cybersecurity 410–14
- principle of conferral 405, 419–20
- private actor involvement 410, 412
- States' operational capability, strengthening 412
- Stockholm Programme 410
- technological resources, development of 413–14
- TEU mutual defence clause 418
- TEU 'non-contamination clause' 421–3
- TEU, 'Union's External Action' 413
- TFEU data protection rules 416–17
- TFEU on establishment and functioning of the internal market 416
- TFEU on judicial cooperation in criminal matters 415
- TFEU solidarity clause 417–18  
*see also* European Court of Human Rights (ECtHR); European Court of Justice (CJEU)
- EU cyber security law, legal basis choice and role of Court of Justice 419–24
  - 'centre of gravity' approach' 423
  - comprehensive approach, need for 421–4
  - cyber defence issues 423, 424
  - principle of consistency 420
- EU cyber security law, legal instruments, fragmentation in 414–19
  - Directive proposal for measures to ensure a high common level of network and information security 415–16
- EU Framework Decision on attacks against information systems 415
- European Parliament and solidarity clause 417–18
- General Data Protection Regulation proposal 416–17
- judicial cooperation 415
- mainstream cyberspace issues into EU external relations proposal 419
- Regulation proposal on electronic identification and trust services for electronic transactions 416
- European Convention on Human Rights (ECHR) 100, 199, 204
- European Court of Human Rights (ECtHR)
  - Balan v Moldova* 72
  - Infopaq* 82, 86
  - intellectual property rights 77
  - national differences on freedom of expression 100, 101
  - originality for computer programs and databases 86
  - Yildirim v Turkey* 53, 101  
*see also* EU cybersecurity law
- European Court of Justice (CJEU)
  - Donner (Free Movement of Goods)* 45
  - ECOWAS (Small Arms and Light Weapons)* 422
  - European Parliament v Council of the European Union* 424
  - Gambelli* 41–2
  - Google Spain v Agencia Española de Protección de Datos* 44–5
  - L'Oréal v eBay International* 45
  - Mauritius* 419, 423
  - Pammer and Hotel Alpenhof* 45–6
  - Pinckney v KDG Mediatech* 46
  - role of *see* EU cybersecurity law, legal basis choice and role of Court of Justice
  - Wintersteiger v Products 4U* 48  
*see also* EU cybersecurity law
- European Network and Information Security Agency (ENISA) 258
- European Parliament and solidarity clause 417–18
- European Patent Convention (EPC) 78, 81, 83–4, 91
- extradition 199–200  
*see also* Snowden (Edward) revelations
- Fanelli, R 232
- Fassbender, B 175
- Fawcett, J 72, 73, 82, 83
- Feakin, T 446, 449, 457, 458, 463
- Fedosov, S 436
- Feinstein, L 277
- Fenrick, W 132
- Ficsor, M 74
- Fidler, D 94–117, 172, 174, 178, 179, 188, 189, 203, 223, 226
- Fildes, J 261
- Finnemore, M 489
- Fitzmaurice, G 32
- Fleck, D 226, 382, 384, 386
- Fleming, P 148, 150
- Flory, P 293

- Focarelli, C 75, 148, 188, 226, 228, 241, 255–83, 300, 312
- Føllesdal, A 404
- Foltz, A 330
- force
- armed force and conflict *see* armed force and conflict
  - cyber operations as use of *see* cyber operations as use of force
- Forcese, C 185
- Ford, C 468
- Forowicz, M 134
- Forseberg, T 18
- France 38, 78, 110
- Franck, T 277
- Franzese, P 182
- Freedman, L 215
- Friedman, A 213
- Gable, K 165
- Garcia-Mora, M 185
- Gardam, J 301
- Garside, J 52
- Gasser, H-P 161
- Gattegno, I 164
- Gazmin, V 450
- Geers, K 342
- Geiss, R 125, 132, 133, 134, 135, 137, 341
- Gellman, B 115
- Geneva Conventions
- armed conflict and attack 122, 123–4, 142, 241–2, 282, 327, 328, 329, 352, 367–8, 371–2, 376, 398
  - civilians taking ‘direct part in hostilities’ 128
  - collateral damage to civilian objects 373, 374
  - and international humanitarian law 120, 129, 130, 131, 134, 135, 136, 137, 172, 343, 371–2
  - non-international armed conflict 126, 161, 336, 339–40, 362
  - principle of distinction 130, 133, 344, 345, 362
  - principle of precaution 136, 137
  - principle of proportionality 134, 135
- Georgia, cyber attacks 56, 243, 260–62, 277, 319, 349–50, 391–2, 439, 466, 475–6
- Germany 38, 39–40, 41, 43
- and US NSA cyber espionage 62–3, 113, 178, 179–80, 184, 473
- Gervais, M 138–9
- Gharibi, H 234
- Gibson, W 22
- Gill, T 134, 149, 161, 183, 214, 224, 226, 228, 307, 308, 311, 314, 316, 361, 366–79
- Gillet, M 138
- Gioia, A 390
- Gjelten, T 97, 307, 309, 436
- Glennon, M 278, 346
- global commons *see* cyberspace, legal status, cyberspace as global commons
- Global Network Initiative (GNI) 115
- Goel, S 307
- Goetz, M 212
- Goldsmith, J 13, 16, 21, 119, 125, 126, 131, 139, 187, 241
- Gombeer, K 281
- Goodman, S 448
- Google cyber attack 168, 184
- Gorman, S 324, 332
- Gosnell Handler, S 236
- Govaere, I 404
- Graber, C 21
- Graham, M 256
- Gray, C 271, 274
- Green, L 385
- Greenberg, L 358, 361
- Greenwald, G 284, 297
- Greenwood, C 120, 277, 329, 368
- Griller, S 420
- Grimm, D 23
- Gross, D 256
- Gross, M 308
- Grotius, H 25, 76
- Guelff, R 385
- Guitton, C 330
- Haaster, J van 23, 211, 227, 230, 231
- hackers 56, 157, 158, 213, 334–5, 348–9, 398
- see also* botnets and remote control; malware; virus attacks
- Hagopian, A 310
- Hague Convention 134, 327, 385–7, 391, 393, 394, 396–7, 398, 399
- Hanifah, A 448
- Hankel, G 134
- Hanspach, M 212
- Hardin, G 28
- Hardin, R 339
- Hardt, S 228
- Haslam, E 123, 124
- Hathaway, O 118, 122, 125, 126, 127, 131, 135, 139, 347, 466, 476, 478
- Healey, J 219, 223, 428
- Heath, K 75, 147–67, 191

- Heckathorn, D 339  
 Heintl, C 447, 449, 450, 453, 455  
 Heinsch, R 140  
 Heintschel von Heinegg, W 241  
 Heliskoski, J 422  
 Henckaerts, J-M 130, 238, 327, 348  
 Henderson, C 257, 432, 460, 465–90  
 Herdegen, M 246  
 Herman, M 174  
 Hern, A 331  
 Herrera, G 21  
 Hervik, P 35  
 Hessbruegge, J 66  
 Hestermeyer, H 355  
 Hider, J 261  
 Hildebrandt, M 26  
 Hillion, C 405, 420, 421, 423  
 Hinkle, K 123, 125, 126  
 Hmoud, M 280  
 Hong, X 79  
 Hörnle, J 50, 82  
 Horsley, T 420  
*HPCR Manual on International Law  
 Applicable to Air and Missile Warfare*  
 238, 240  
 Hugenholtz, B 78, 81  
 human rights 94–117  
   cybercrime and liberties protection 199,  
   203–4  
   cyberspace and general principles of  
   international law 98–9  
   ‘digital divide’ and right to development  
   107–8, 109–10  
   economic, social and cultural rights 104–8  
   International Covenant on Economic, Social  
   and Cultural Rights (ICESCR) 104–7  
   Internet access as new human right 109–10  
   right to freedom of expression and national  
   differences 100–102, 110  
   and sovereignty 100–101  
   UN ‘Right to Privacy in the Digital Age’  
   draft resolution 113  
   violations, and cyber espionage 179–80  
   *see also* international humanitarian law  
 human rights, civil and political rights 99–104  
   authoritarian government restriction 102  
   Freedom House report 102, 114  
   Internet censorship 100–102  
   right to privacy and national differences  
   103–4  
 human rights, international relations and  
   cyberspace 110–16  
   authoritarian government threats 112–13  
   cyber security 112–15  
   extraterritorial application of right to  
   privacy 114  
   Global Network Initiative (GNI) 115  
   Internet freedom and Internet sovereignty  
   contrasts 111  
   Internet governance 111–12  
   private enterprise and cyber technologies  
   115–16  
   Wassenaar Arrangement on Export Controls  
   and ‘dual use’ ICT technologies 115  
 human rights, Internet technology and  
   international politics  
   communication technologies, evolution of  
   95–6  
   cyberspace connection with human rights  
   96–7  
   military potential of the Internet 97  
   packet switching 95–6  
   sovereignty and non-intervention policies  
   97  
   US political dominance 96, 97, 113–14  
 Hunter, D 24  
 Huntley, T 187  
 Huntsman, J 223  
 Hurt, C 40  
 Hutchins, E 229–30  
 ICANN (Internet Corporation for Assigned  
 Names and Numbers) 21–2, 74, 76, 79,  
 116  
 ICRC *see* International Committee of the Red  
 Cross (ICRC)  
 identification problems *see* attribution  
 Imburgia, J 346  
 indiscriminate attacks *see* principle of  
 distinction, relevance of, prohibition of  
 indiscriminate attacks in cyberspace  
 industrial protest as terrorism, problems with  
 159–60  
 information  
   access, cyber espionage and international  
   law 171, 178–9  
   Critical Information Infrastructure (CII)  
   288–9  
   EU Commission Communication, ‘Network  
   and Information Security’ 410, 411  
   EU Directive proposal on information  
   security 415–16  
   European Information Sharing and Alert  
   System (EISAS) 409

- European Network and Information Security Agency (ENISA) 409, 411, 412
- extraction problems, and ethical challenges 318–19, 321
- illegal interception and protection of privacy 194–5
- industry cooperation and information sharing 444
- NATO Communications and Information (NCI) Agency 431–2
- private sector involvement in information sharing 179, 211–12, 222, 259, 264
- sovereignty over 183–4, 186  
*see also* cyber security
- infrastructure *see* cyberspace, infrastructure
- Inkster, N 112
- Institut de Droit International, Santiago  
Resolution on self-defence 266, 270–71, 277
- intellectual property rights *see* cyberspace, intellectual property rights
- intelligence *see* cyber espionage
- intensity of attack 124–5, 330, 332, 340–41
- Inter-American Court of Human Rights  
idea–expression dichotomy 89  
*Velasquez-Rodriguez* 66–7
- international armed conflict, classification *see* classification of cyber warfare, international armed conflict
- International Committee of the Red Cross (ICRC)  
armed conflict definition 329  
customary law status 136  
'effective contribution' requirement 130–31, 134, 335  
intensity threshold 340–41  
*Interpretive Guidance on the Notion of Direct Participation in Hostilities* 362–3, 372  
non-international armed conflict 336–7, 340  
weapons definition 238
- International Court of Justice (ICJ)  
*Armed Activities in Congo* 270  
*Arrest Warrant Case (Democratic Republic of Congo v Belgium)* 19, 20  
'author's own intellectual creation' 86–7  
*Bosnian Genocide* 57, 59, 60, 68, 70, 278, 334, 352  
*Congo v Uganda* 67–8  
*Corfu Chanel Case (UK v Albania)* 17, 63–4, 66, 67, 182, 250, 254, 279, 333, 394–5
- Declaration of Independence of Kosovo* 37, 65
- due diligence disputes 67–9, 394–5
- Fisheries Jurisdiction (Spain v Canada)* 244
- Gabčíkovo-Nagymaros Project (Hungary/Slovakia)* 279, 355
- Legality of the Threat or Use of Nuclear Weapons* 123, 235, 238, 265, 267, 271–2, 279, 293–5, 299, 301, 303, 343–4
- Martens Clause and protection and authority of the principles of international law 344
- Navigational and Related Rights (Costa Rica v Nicaragua)* 246–7, 355
- Nicaragua* 60, 64, 65, 126, 175, 180–81, 182, 186, 233, 236–8, 242–3, 250, 252, 253–5, 266, 267, 273–5, 278, 301, 334, 376–7
- Nottenbohm Case (Lichtenstein v Guatemala)* 19
- Oil Platforms (Islamic Republic of Iran v United States)* 265, 267, 273, 275
- on principle of non-intervention 251, 253
- Pulp Mills (Argentina v Uruguay)* 69, 279
- SAS Institute v World Programming Ltd* 90
- on self-defence against non-State actors 276, 277
- US Diplomatic and Consular Staff in Tehran* 57, 67, 333, 335
- International Covenant on Civil and Political Rights (ICCPR) 100, 101, 103–4, 114, 199
- International Covenant on Economic, Social and Cultural Rights (ICESCR) 104–7
- international crime of terrorism *see* cyber terrorism, cyber attacks and general international crime of terrorism
- International Criminal Court (ICC)  
'act of aggression' 137, 138–41  
crimes against humanity 141–2  
jurisdiction 120, 126  
war crimes definition 121
- international criminal responsibility 118–43  
attribution of attack to one of the parties to the conflict 125–6, 129
- computer network attacks (CNAs), overview 118–20
- cyber attacks and crimes against humanity 141–2
- cyber warfare definition 119–20
- cybercrime definition 118

- International Criminal Court *see* International Criminal Court (ICC)
- international criminal responsibility concept 120
- jurisdiction for cyber attacks 120
- Tallinn Manual *see* Tallin Manual
- see also* cybercrime
- international criminal responsibility, cyber attacks and crime of aggression 120, 137–41
  - ‘act of aggression’ 137, 138–41
  - leadership clause 137–8
  - use of any weapons 139
  - use of armed force 138–9
- international criminal responsibility, cyber attacks as war crimes 121–37
  - armed conflict, existence of 121–6
  - civilians lose immunity from attack if they take ‘direct part in hostilities’ 128
  - cyber attacks causing excessive collateral damage and principle of proportionality 134–6
  - data as a protected object 131
  - delimitation problems and principle of distinction 130–31
  - determining whether armed force has been applied 122–3
  - dual-use of cyber infrastructure and principle of distinction 131–3
  - duration of participation 124–5, 129 and Geneva Convention *see* Geneva Convention
  - geographical scope of armed conflict 126–7
  - intensity of attack 124–5
  - interconnectivity between military and civilian computer systems 131–3
  - international humanitarian law (IHL) principles 129–37
  - minor disruptions 124
  - principle of distinction 130–33, 135
  - principle of precaution 136–7
  - principle of proportionality 134–6
  - prohibition of indiscriminate attacks and principle of distinction 133
  - quality of attacks 124–5
  - responsible agent 127–9
  - violent effects of CNA producing lasting harmful result 123–4
- International Criminal Tribunal for the Former Yugoslavia (ICTY)
  - armed conflict definition 121–2
  - Prosecutor v Galic* 135, 161, 373
  - Prosecutor v Tadić* 60, 121, 125, 126, 127, 278, 327, 328, 334, 335, 336–7, 345, 348, 368, 384
- international humanitarian law
  - and classification of cyber warfare 326–7, 331–2, 335, 336, 339–40
  - international criminal responsibility, cyber attacks as war crimes 129–37
  - principal of distinction *see* principle of distinction
  - see also* human rights
- international humanitarian law applied to cyber warfare 366–79
  - attacks of a perfidious nature, banning of 374
  - collateral effects and feasible precautions 373
  - conducting of attacks, law of armed conduct relating to 371–4
  - cyber attacks as adjunct to traditional means 370–71
  - cyber surveillance and espionage 369
  - cyber terrorism 369–70
  - Geneva Convention *see* Geneva Convention
  - geographical scope of armed conflict 368–9
  - International Humanitarian Law or Law of Armed Conflict (IHL/LOAC) 366–71
  - non-international armed conflicts 368
  - principle of distinction 372
  - principle of proportionality in attacks against civilians or civilian objects 372–3
  - prohibition of means of attack not directed at specific military objectives 373–4
  - rules relating to the targeting of persons and objects 372
  - self-defence in response to armed attack 369
  - stand-alone cyber attacks 369–70
  - targeting of objects directly converted into a military function 374
  - weapons or methods of combat which would cause superfluous injury to enemy combatants, restrictions on 374
- international humanitarian law applied to cyber warfare, principle of proportionality in attacks employing cyber weapons 374–8, 379
- any attack not reasonably likely to cause physical effects upon civilians or civilian objects 376–7
- data destruction 375–6

- dual use function and collateral effects 377–8
- military ‘information operations’ not considered as attack 375
- operations considered as mere inconvenience 375
- International Law Commission (ILC) 57–9, 66, 125–6
- international law and cyber espionage *see* cyber espionage and international law
- International Multilateral Partnership Against Cyber Threats (IMPACT) 257
- international obligation breach, and State responsibility *see* State responsibility, international obligation breach
- international peace and security threat, cyber espionage *see* cyber espionage and international law, as threat to international peace and security
- international relations, and cyberspace *see* human rights, international relations and cyberspace
- international substantive law, and cybercrime 192–8
- International Telecommunication Regulations (ITRs) 111–12
- International Telecommunication Union (ITU) 165, 257
- International Tribunal of the Law of the Sea (ITLOS), due diligence concept 66
- Internet
  - access as new human right 109–10
  - blocking network services 20, 319, 323
  - censorship 100–102
  - and cyberspace, differences in meaning 55–6
  - and data transmission, law of neutrality 398, 399
  - domain names 21–2, 74, 76, 79, 92, 116
  - freedom and Internet sovereignty contrasts 111
  - general use by terrorist groups 150
  - ‘Internet sovereignty’ perspective 98
  - neutrality 476
  - online gambling 40–42, 47
  - regulation 111–12, 220–21, 406
  - service providers, liability and responsibility 203, 205
  - social networks as targets 361
  - technology, and human rights *see* human rights, Internet technology and international politics
  - territorial fragmentation 52–3
  - see also* computer systems; cyber attacks
- Iran 169, 182, 390
  - Iran–US Claims Tribunal, *Yeager v Islamic Republic of Iran* 60–61
  - Stuxnet attack 56, 133, 153, 212, 243, 261, 288, 308, 310, 315, 316, 318, 322, 324, 330, 361, 370, 376–7, 466
- Iraq 141, 350, 390–91
- Israel 276–7, 285, 341
- Jacobs, D 61
- James, A 16
- Jamnejad, M 183, 250, 252
- Janczewski, L 229
- Japan 448
- Jaycox, M 223
- Jennings, P 446
- Jennings, R 182, 186
- Jensen, E 268, 291, 327, 361, 397
- Jewkes, Y 157
- Johnson, D 2, 13, 16, 37–8
- Johnson, R 245
- Jordan, D 227
- Joubert, V 429, 435
- Joyner, C 236, 265
- jurisdiction *see* cyberspace jurisdiction
- Kaesling, K 81
- Kahn, J 296
- Kamal, A 29
- Kammerhofer, J 277
- Kanuck, S 19
- Kaplan, D 308
- Kastenberg, J 392
- Kastner, P 148, 149, 190–207, 223, 265, 407, 460, 466
- Katz, J 283
- Kaurin, P 317
- Kegel, G 78
- Keller, H 134
- Kelsey, J 343, 346, 353, 360, 361, 396
- Kemp, G 139
- Ker, P 159
- Kerr, O 201
- Kessler, O 119, 123, 125, 139
- Keyser, M 418
- Kimmel, P 324
- kinetic effects equivalency (KEE) test *see* principle of distinction, relevance of, kinetic effects equivalency (KEE) test
- Kingbury, K 324
- Kirkpatrick, D 219
- Kirsch, S 156

- Kleinwächter, W 95, 97  
 Klimburg, A 218, 418, 428, 442  
 Knake, R 188, 253, 260, 317  
 Koepsell, D 14  
 Koh, H 14, 56, 63, 187–8, 234, 242, 243, 263, 351  
 Kohl, U 18, 20, 30–54, 72, 79, 183, 190, 200, 201, 226  
 Kolasky, R 331  
 Kolb, A 88  
 Koops, B-J 223  
 Korns, S 392  
 Korzak, E 330  
 Kostic, D 140  
 Koufa, K 151, 157  
 Koutrakos, P 413, 420  
 Kramer, E 255  
 Kraska, J 119–20  
 Krasner, S 17  
 Kreß, C 140, 141  
 Kuehl, D 15  
 Kulsrud, C 380  
 Kunig, P 181, 182, 252  
 Kur, A 74, 78  
 Kurbalija, J 220  
 Kurlantzick, J 456  
 Kwon, H 449, 457
- Lahmann, H 132, 133, 134, 135, 137  
 Lanchester, J 212  
 Landler, M 259  
 Lanz, C 389  
 Larik, J 405  
 Lauterpacht, H 57, 236  
 law of neutrality 380–400  
   belligerent's right to use force to counter violations of State's neutrality 394  
   computer facilities 397, 399  
   cyber activity attribution problems and due diligence 394–5  
   cyber context 391–9  
   cyber context, expressly applicable rules 392–4  
   cyber espionage and communication with belligerents 398–9  
   Georgia, South Ossetia War and website hacking 381–2  
   Hague Convention 134, 327, 385–7, 391, 393, 394, 396–7, 398, 399  
   Internet and data transmission 398, 399  
   Iraqi invasion of Kuwait and modified nature of neutrality 390–91  
   law of armed conflict (LOAC) 396–9  
   neutrality definition 382–4  
   non-belligerency practice 384  
   non-discrimination principle 387, 388–9  
   non-participation principle 387–8  
   permanent neutrality position 382–3  
   sources in customary international law 381, 385–7  
 Tallinn Manual *see* Tallinn Manual  
 temporary neutrality 383–4  
 territorial sovereignty violations 380–81, 389, 394–5, 397–8  
 UN Charter regime and Security Council Resolution effects 389–91, 393, 394, 395
- Lawson, S 222, 370  
 League of Arab States Convention 196, 197, 200, 202–3  
 Lee, D 250  
 Lee, Y 448  
 legal dimensions  
   of cybercrime *see* cybercrime, international legal dimensions  
   law of neutrality *see* law of neutrality  
   military operations, 'adequate' legal basis requirement 228–9  
   self-defence in cyberspace 262–3  
   *see also* cyberspace jurisdiction; cyberspace, legal status
- Leiner, B 95  
 Lemley, M 75  
 Lessig, L 15, 16  
 Levie, H 329–30  
 Lewis, J 446, 449, 463  
 Libicki, M 290, 297, 323  
 Lieber, F 344  
 Lieber, K 293  
 Liefländer, T 274  
 Lin, H 118, 119, 122, 123, 132, 241, 249, 269, 308  
 Liptak, A 36  
 Lisbon Treaty, EU cybersecurity law 403–4, 413, 416, 420–21  
 Loewenheim, U 84  
 Lombois, C 34  
 Lotrionte, C 236, 265  
 Lowe, A 48  
 Lowe, V 37, 397  
 Lubell, N 119, 120, 123, 124, 129, 131, 276, 337  
 Lucarelli, E 256  
 Lucas, G 261  
 Luijff, E 219, 223  
 Lülff, C 120, 123, 127

- Lynch, C 113  
Lynn, W 258
- MacAskill, E 284, 297  
McBurney, P 240  
McClure, R 119  
McConnell, B 285, 286, 288, 289, 291  
McConnell, M 262  
Malin, C 309  
malware 252–3, 257, 261, 308, 309, 312, 313, 444  
    *see also* hackers  
Mandiant Report 168, 169, 333  
Mann, F 19, 32  
Marauhn, T 427  
Markoff, J 255, 259, 392  
Marsden, C 406  
Martin, C 190  
Masli, U 449  
Mason, S 358  
Matera, C 406  
Maurer, T 468, 470, 471, 474, 475, 481, 487, 488  
Maybaum, M 229  
Mayer, F 406, 418  
Mégret, F 148, 149, 190–207, 223, 265, 407, 460, 466  
Melnitzky, A 179, 187  
Melzer, N 119, 122, 123, 124, 125, 128, 129, 131, 138, 244, 247, 329, 348, 353, 354, 362, 363  
Mendez, F 410  
Meyer, D 256  
Meyer, J 359  
Meyer, P 466, 473, 481  
military operations  
    cyber attack in support of conventional 260, 261–2, 285  
    cyber operations directed against civilians  
        *see* principle of distinction, relevance of, prohibition of military cyber operations directed against civilians  
    cyber operations, notion of 212–13, 214, 226–32  
    ‘information operations’ not considered as attack 375  
    and Internet technology 97  
    principle of distinction 358–9  
    security against cyber treats 286, 288–9  
    targeting of objects directly converted into military function 374  
Miquelson-Weismann, M 197, 199, 204  
Mirtl, P 218  
Miryousefi, A 234  
Monar, J 405  
Moore, J 271, 388  
Morgan, P 290, 303  
Morley, D 30  
Morozov, E 102  
Morris, N 63  
Moseley, A 311  
Mueller, B 189  
Müllerson, R 233  
Mulvenon, J 24, 287, 289, 296  
Murphy, J 180, 189, 244  
Murphy, T 25  
Mutz, G 32  
Myers, S 277  
Myjer, E 256, 284–304
- Nakashima, E 115, 249, 333, 361  
Nasu, H 446–64  
national involvement *see* State practice; State responsibility  
NATO  
    2010 Strategic Concept 257–8  
    2020 Report on cyber defence 274, 275  
    collective defence 291  
    collective self-defence 260, 270  
    Cooperative Cyber Defence Centre of Excellence (CCDCOE) 258  
    information security initiatives 70  
NATO and cyber defence 426–45  
    Allied Command Operations (ACO) 432  
    CERTs (Computer Emergency Response Teams) 440–41  
    Communications and Information (NCI) Agency 431–2  
    Computer Incident Response Capability (NCIRC) 429, 433, 444  
    Consultation, Control and Command (NC3) Board 431  
    Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) 441, 442  
    Cyber Defence Management Board (CDMB) 431, 432, 439  
    Cyber Defence Programme (Prague Capabilities Commitment) 429  
    Euro-Atlantic Disaster Response Coordination Centre (EADRCC) 438  
    exercises 432, 440–41, 443  
    governance 430–32  
    industry cooperation and information sharing 443, 444

- international organizations, liaison with  
432, 442, 443
- Malware Information Sharing Platform  
(MISP) 444
- NATO decision and NATO operation,  
meanings of 428
- North Atlantic Council (NAC) 430–31, 435,  
437
- Policy on Cyber Defence 429, 430, 437–8,  
439–40, 442
- Rapid Reaction Teams (RRTs) 439–40
- Science for Peace and Security Programme*  
442
- Strategic Concept for the Defence and  
Security of the Members of NATO*  
429–30, 432, 434–6
- see also* Estonia; Georgia
- NATO and cyber defence, key aspects 432–43
- assistance to Member States and  
Memoranda of Understanding (MoUs)  
439–40
- civil crisis management 438–9
- collective self-defence 434–7
- consultation 437–8
- cyber crisis management 434–40
- cyber defence cooperation 442–3, 444
- cyber warfare perceptions 436–7, 438
- defence of NATO's own networks 432–4
- exercises to ensure preparedness 440–41
- secure ICT infrastructure 433–4
- strategic ambiguity on concept of 'armed  
attack' 435
- training, education, and research 441–2
- Nemerofsky, J 186
- Netherlands 41, 216, 225, 227, 331
- Neumann, P 215
- neutrality law *see* law of neutrality
- New Zealand 41, 448
- Newton-Small, J 253
- Nollkaemper, A 61
- Non-Aligned Movement (NAM) and  
anticipatory self-defence 271, 272
- non-international armed conflict
- classification of cyber warfare *see*  
classification of cyber warfare,  
non-international armed conflict
- international humanitarian law applied to  
cyber warfare 368
- non-intervention principle *see* principle of  
non-intervention
- non-State actors involvement 172–4, 276–80,  
449–50
- Noyes, M 307
- nuclear deterrence
- differences from cyber deterrence 296–7,  
299
- strategy *see* cyber deterrence and public  
international law, nuclear-deterrence  
strategy (strategy of massive  
retaliation)
- nuclear security 272, 288–9
- Nunziato, D 100
- Nye, J 28, 286
- Obama, B 164
- O'Connell, M 56, 70, 255, 261, 263, 278,  
281, 282, 289, 437
- O'Donnell, B 119–20
- O'Driscoll, M 384, 388
- Oehmichen, A 156
- Oeter, S 131
- Olásolo, H 134
- Olzak, T 229
- Omanovic, E 115
- Onuf, N 17
- operations, cyber *see* 'cyber operations'  
headings
- Ophardt, J 137, 140, 346
- Opsahl, K 223
- Owens, W 242, 247, 286
- Palojärvi, P 242
- Panetta, L 333
- Paris Convention, intellectual property rights  
74, 78, 80
- Parizo, E 259
- Parks, W 175
- Pastukhov, O 92
- Pateraki, A 414, 417
- Pauli, D 147
- Paulus, A 139–40, 141
- peacetime
- cyber espionage and international law in  
172
- protection of critical infrastructures 289
- Pelican, L 176–7
- perfidy 129, 312–14, 357
- Permanent Court of International Justice  
(PCIJ)
- Factory at Chorzów (Indemnities)* 57
- Lotus* 18, 19, 20, 21, 36, 37, 48, 51, 65,  
181, 344
- Oder River Commission* 279
- S.S. 'Wimbledon'* 28
- Pernik, P 398
- persons, attacks on *see* civilian population

- Peters, A 65, 113  
 Peterson, A 115  
 Philippines 204  
 Pictet, J 124, 127, 368  
 Pila, J 80  
 Pillay, N 108  
 Pilloud, C 130, 133, 136, 329, 336, 338, 339, 340, 362  
 Pirker, B 182, 224, 226  
 Pocar, F 201  
 Poellet, K 247, 249  
 PoKempner, D 225  
 political motive for terrorism, and organised crime 149–50  
 political rights *see* human rights, civil and political rights  
 Porcedda, M 408  
 pornography 39, 196–7  
 Porter, A 404, 408, 409, 419  
 Portnoy, M 448  
 Post, D 2, 13, 16, 37–8  
 Pouw, E 228  
 Prakash, R 465, 466, 475, 478, 480  
 Press, D 293  
 principle of conferral, EU cybersecurity law 405, 419–20  
 principle of distinction  
   and dual-use of cyber infrastructure and principle of distinction 131–3  
   international criminal responsibility, cyber attacks as war crimes 130–33, 135  
   international humanitarian law 160–61, 372  
 principle of distinction, relevance of 343–65  
   armed conflict law 345  
   cyber attack definitions 346–7, 348  
   cyber-psychological operation (PSYOP) and denial of services 354  
   effectiveness in cyberspace 347–8  
   Geneva Conventions 130, 133, 344, 345, 362  
   Lieber Code 344  
   Martens Clause 344, 356  
   prohibition of cyber attacks against the civilian population and objects 346–53  
   prohibition of military cyber operations directed against civilians 353–7  
 principle of distinction, relevance of, kinetic effects equivalency (KEE) test 348–9  
   acts of violence 348–9  
   collateral damage and malfunction of civilian facilities 349–50, 354  
   computer system hacking as attack 348–9  
   critical date for assessment of existence of attack 350  
   interference with functionality as damage 351–2  
   limits of 349–53  
   problem of assessment of damage 349–51  
 principle of distinction, relevance of,  
   prohibition of indiscriminate attacks in cyberspace 357–64  
   ‘civilianization’ of war 358  
   computers and computer companies as targets 360–61  
   ‘direct participation in hostilities’ interpretation 362–4  
   dual-use objects, distinction between civilian objects and military objectives 358–62  
   identification problems and protection of civilians 362–4  
   Internet and social networks as targets 361  
   military objectives definition 358–9  
   prohibition of perfidy 357  
   ‘war-sustaining’ installations 359–60  
 principle of non-intervention  
   cyber espionage and international law, international law application 180–86  
   law of neutrality 387–8  
   sovereignty and non-intervention policies 97  
   violation 250–52, 253, 261–2  
 principle of precaution, cyber attacks as war crimes 136–7  
 principle of proportionality  
   cyber attacks as war crimes 134–6  
   international crime of terrorism 160–61  
   and international humanitarian law *see* international humanitarian law applied to cyber warfare, principle of proportionality in attacks employing cyber weapons  
   self-defence in cyberspace 274–5  
 Prislán, V 26  
 private motivation for attacks 158–9  
 private persons or entities, acts of, and State responsibility 60, 61  
 private sector  
   classification of cyber warfare 334–5  
   cyber espionage and confidential information sharing 179, 259, 264  
   and cyber technologies 115–16, 195–6, 211–12, 216, 222, 223

- engagement, Asia-Pacific Economic Cooperation (APEC) 461–2  
involvement, EU cybersecurity law 410, 412
- property  
infrastructure *see* cyberspace, infrastructure  
intellectual *see* cyberspace, intellectual property rights
- public international law  
and cyber deterrence *see* cyber deterrence and public international law  
and intellectual property 77–82
- Rahmatian, A 72–93, 226  
Randelzhofer, A 139  
Raymond, D 318  
Reed, T 351  
Rees, N 447, 450, 457
- regulation  
comprehensive multilateral instrument, need for 206  
cyber terrorism, comprehensive instrument and regulation need 163–7  
Internet 111–12, 220–21, 406  
*see also* ‘legal’ headings
- Reinold, T 276, 277  
Reitman, R 112  
Reydam, L 34  
Rid, T 232, 240, 243, 285, 288, 289–90, 296, 298, 367, 369, 370, 377, 437  
Roberts, A 385  
Robins, K 30  
Robinson, N 404  
Rona, G 278  
Ronzitti, N 233, 390  
Rosati, E 86  
Roscini, M 75, 148, 187, 224, 226, 228, 233–54, 262, 263, 264, 265, 268, 275, 282, 299, 312, 331, 466  
Ross, M 417  
Rothman, M 219  
Rowe, N 307–25  
Ruggie, J 18  
Russia 70, 111, 114, 277–8, 457, 478  
*see also* Estonia; Georgia  
Russo, F 390  
Ryngaert, C 20, 32, 33
- Safferling, C 140  
Sanger, D 212, 218, 360  
Sassòli, M 360  
Satzger, H 139  
Saudi Arabia 244–5, 330
- Saul, B 75, 147–67, 191  
Scassa, T 182  
Schabas, W 141  
Schachtman, N 262, 426, 436  
Schaller, C 175  
Schell, B 190  
Schiller, H 30, 31  
Schjolberg, S 206  
Schmitt, E 334  
Schmitt, M 1–9, 118, 123–31 *passim*, 138, 139, 149, 187, 214, 240, 246, 253, 255, 263, 264, 267, 268, 270, 273, 276, 280, 299–301, 302, 326, 329, 338, 339, 341, 347, 352, 353–4, 359, 361, 363–4  
Tallinn Manual *see* Tallinn Manual
- Schreier, F 240  
Schricker, G 84  
Schrijver, N 26  
Schultz, T 20, 398  
Schwartz, P 104  
Scoville, H 175  
security *see* cyber security  
Segal, A 311  
Segura-Serrano, A 246  
Seidl-Hohenveldern, I 78  
self-censorship, jurisdiction in cyberspace 53  
self-defence in cyberspace *see* cyberspace, self-defence in  
Serbia and Montenegro 350  
Shachtman, N 392  
Shackelford, S 263  
Shafer, G 332  
Shakarian, P 392  
Shamah, D 332  
Shanahan, L 160  
Shanker, T 334  
Sharp, W 236  
Shaw, M 32, 394  
Shearer, I 34  
Sheldon, J 436  
Shelling, T 296  
Sherman, B 86  
Sikkink, K 489  
Silver, D 139, 237  
Simma, B 255  
Simpson, B 381, 399  
Singel, R 262, 437  
Singer, D 426–7  
Singer, P 213, 262, 426  
Slaughter, A-M 277  
Smith, G 48  
Smith, J 185  
Smith, M 215

- Smith, T 317, 319, 325, 350
- Snowden (Edward) revelations 53, 62, 64,  
94–5, 112, 113–15, 169, 172–3, 179,  
180, 219, 224, 466, 473
- Sommer, P 212
- South Korea 448
- sovereignty *see* cyberspace sovereignty
- Spernbauer, M 423, 425
- Sri Lanka 157
- Staker, C 37, 397
- State practice
- classification of cyber warfare 330, 334–5
  - cyber espionage and national infrastructure information 179
  - cyber espionage and refusal to accept responsibility when accused 195–6
  - cybercrime and national legislation and fragmentation 201
  - operational capability, strengthening, EU cybersecurity law 412
- State-level cyber operations *see* cyber operations, State-level cyber paradigms
- State-sponsored cyber attacks 158, 161–2, 164
- States claiming regulatory competence in parallel 33–4  
*see also* cyberspace sovereignty
- State responsibility 55–71
- acts of private persons or entities 60, 61
  - Articles on the Responsibilities of States (ARS) 58–61, 66, 68
  - breach of international obligation 61–2
  - computer hacking attacks 56
  - de facto* agents 59, 60, 66
  - exercise of government authority elements in absence of State authority function 60–61
  - government authority delegation 59–60
  - Internet and cyberspace, differences in meaning 55–6
  - requirements 57–62
- State responsibility, attribution in cyberspace 62–5
- acts emanating from location under exclusive jurisdiction of another State 65
  - ambiguity and margin of discretion 63
  - computer identification 62–3, 69–70
  - electronic surveillance 62–3, 64, 65
  - evidence requirements and territorial location of computers 63–5
  - personal identification problems 62, 63
  - Tallinn Manual *see* Tallinn Manual
- State responsibility, international obligation
- breach 65–70
  - cooperation and concerted action, need for 70, 71
  - due diligence violation 66–9, 71
  - grounds for establishing responsibility 66
  - lack of consensus on 65
  - notification selection criteria 69–70
- Steiger, D 131–2, 247
- Stohl, M 148, 150
- Stone, J 175
- Stone Sweet, A 409, 420
- Stout, C 324
- Strate, L 22
- Strawser, B 312, 314
- Sulmasy, G 185
- Swaine, J 260
- Swanson, L 119, 123, 260
- Syria 158, 260, 360, 361, 370, 371, 376
- Tadjdeh, Y 427
- Tallinn Manual
- cyber attack definition 348, 374, 376
  - cyber operation as use of force 188, 242, 245, 250, 252–3, 299–301, 302, 328, 329, 330, 335
  - cyber operations against civilians 353–4, 363, 375
  - cyber terrorism 161
  - cyber warfare and the applicability of international law 366, 475
  - dual-use entities as military targets 361
  - interference with functionality as damage 351
  - international criminal responsibility 119–20, 123, 124, 127–39*passim*, 141
  - law of neutrality 386–7, 392–3, 394–5, 397, 398, 399
  - non-international armed conflicts 369
  - organization criterion 338
  - and self-defence 265, 273, 369
  - standard of the reasonable commander/combatant 373
- State responsibility, attribution in cyberspace 63, 64, 65, 69
- Taubman, A 72, 74
- Taylor, P 18
- technology
- and cyber deterrence *see* cyber deterrence and public international law, cyber deterrent feasibility and technical considerations

- cyber deterrent feasibility and technical considerations 297–8
- and cyber infrastructure disparities 449–50
- cyber terrorism and possible necessary technical measures 165–6
- cybercrime and technical means of
  - protection and preventive measures 204–5
- Internet technology and human rights *see*
  - human rights, Internet technology and international politics
- private enterprise and cyber technologies 115–16
- technological resources, development of, EU 413–14
- Temple Lang, J 406
- terminology problems, cyber deterrence and public international law 297–8
- territoriality
  - coercion and violation of territorial integrity 181–3
  - objective, cybercrime and principle of nationality 202
  - principle 33, 48, 198–200
  - search and seize powers and cybercrime 199
  - sovereignty as protection of territorial integrity 182, 183
  - territorial nature of intellectual property *see* cyberspace, intellectual property rights, territorial nature
  - territorial sovereignty violations, law of neutrality 380–81, 389, 394–5, 397–8
  - see also* cyberspace sovereignty
- terrorism *see* cyber terrorism
- Thomas, N 449, 452, 458, 461, 462
- Thomson, J 16
- Tiirmaa-Klaar, H 220, 223, 428
- Tikk, E 250, 260, 281, 350, 438
- Timberg, C 333
- Timlin, K 449
- Timofeeva, Y 38
- Tirmaa-Klaar, H 418
- Tladi, D 278
- Tobanksy, L 15
- Toebes, B 106
- Torremans, P 72, 73, 79, 82, 83
- Touré, H 147
- Townsend, M 157
- Trachtman, J 17, 28
- transnational corporations, power and interests of 31
- Trauner, F 404
- Traynor, I 260
- Treize, H 446–64
- Tsagourias, N 13–29, 33, 48, 63, 64, 72, 75, 98, 149, 224, 231, 235, 247, 261–2, 267, 278, 287, 296, 301, 394, 398, 448
- Tullos, O 264
- Turns, D 118, 127, 128, 131, 149, 349, 362, 363, 364, 380–400
- UK
  - BT v One in A Million* 92
  - computer program protection 86–7
  - Copyright, Designs and Patents Act 72, 84, 85, 86–7, 89, 90–91
  - copyright law and territoriality principle 78–9
  - cybercrime cost 1
  - cybersquatting 92
  - Digital Economy Act 75
  - Gambling Act 51
  - Harrods v Dow Jones Co* 43
  - John Richardson Computers Ltd v Flanders* 89
  - Lewis & Ors v King* 43
  - military cyber operations definition 227
  - Navitaire* 89
  - Obscene Publications Act 39
  - R v Perrin* 39, 50
  - R v Sheppard & Amor* 19
  - SAS Institute v World Programming Ltd* 89
  - Twentieth Century Fox Film Corp & Ors v British Telecommunications* 52
  - Vidal-Hall & Ors v Google Inc* 44
- UN Charter
  - self-defence in cyberspace *see* cyberspace, self-defence in, UN Charter Article 51
  - and use of force 186–8, 265, 267, 299–302
- UN Convention against Transnational Organized Crime 149, 198, 199
- UN Counter-Terrorism Implementation Taskforce (CTITF) 147, 151
- UN Draft Comprehensive Anti-Terrorism Convention, terrorist offences definition 155–7, 158, 159, 160, 161–2
- UN General Assembly (UNGA)
  - Declaration on the Definition of Aggression 237
  - and prohibition of use of force *see* cyber operations as a use of force, UN General Assembly (UNGA) and prohibition of use of force
  - protection of critical information infrastructures 288

- regulation of cyber security *see* UN and the regulation of cyber security, General Assembly (UNGA)
- Resolution on misuse of information technologies 280
- UN Global Counter-Terrorism Strategy 151
- UN Hostages Convention 154
- UN Internationally Protected Persons Convention 154
- UN Office of Drugs and Crime (UNODC), cyber terrorism definition 147, 150
- UN and the regulation of cyber security 465–90
  - differences on fundamental issues between Eastern and Western States 466
  - Economic and Social Council (ECOSOC) 484–6
  - emerging regulatory framework for cyber security 477
  - information security 467–9, 474–81
  - International Code of Conduct for Information Security 478–81
  - International Telecommunications Unit, Global Cyber-Security Agenda 487–8
  - International Telecommunications Unit, online protection for children 488
  - Internet neutrality 476
  - norms, rules and principles of responsible behaviour by States, recommendations for 480
  - UN Charter affirmation and rules on the non-use of force and self-defence 480
  - UN Global Counter-Terrorism Strategy 482
  - UN Institute for Disarmament Research (UNIDR) 488–9
  - UN Office on Drugs and Crime (UNODC) 489
  - UN Security Council (UNSC) 481–4
- UN and the regulation of cyber security, General Assembly (UNGA) 467–81
  - First Committee (Disarmament and International Security) 467–9, 474–6, 477–8, 488
  - Groups of Governmental Experts (GGEs) 469, 470, 473–81
  - Groups of Governmental Experts (GGEs), First Group 474–6
  - Groups of Governmental Experts (GGEs), Fourth Group 481
  - Groups of Governmental Experts (GGEs), Second Group 476–8
  - Groups of Governmental Experts (GGEs), Second Group, ICT disruptions and risk 477, 480–81
  - Groups of Governmental Experts (GGEs), Third Group 478–81
  - Second Committee (Economic and Financial Committee) and Global Culture of Cyber-security initiative 469–71
  - Second Committee, global culture of cyber security 470–71
  - Second Committee, voluntary self-assessment tool for national efforts 471
  - Third Committee (Social, Humanitarian and Cultural Committee) 471–3, 489
  - Third Committee (Social, Humanitarian and Cultural Committee), resolution combating the criminal misuse of information technologies 471–2
  - Third Committee (Social, Humanitarian and Cultural Committee) resolution on right to privacy in the digital age 473
  - Third Committee (Social, Humanitarian and Cultural Committee) and UN Crime Prevention and Criminal Justice Programme 472
  - Vienna Declaration on Crime and Justice 485–6
- UN Reports of International Arbitral Awards (RIAA)
  - Island of Palmas Case (US v Netherlands)* 17, 279
  - Trail Smelter* 279
- UN ‘Right to Privacy in the Digital Age’ draft resolution 113
- UN Security Council Resolutions
  - inherent right to self-defence 277–8
  - regulation of cyber security 481–4 and terrorism 150–51, 156, 158
- UN Special Tribunal for Lebanon 155–6, 158
- UN Terrorist Bombings Convention 154–5
- US
  - botnets 319
  - Cable News Network LP v cnnnews.com* 47, 52
  - Caroline* 271, 273
  - Comprehensive National Cybersecurity Initiative (CNCI) 258–9
  - CompuServe v Patterson* 19, 20
  - Computer Associates v Altai* 89
  - Computer Software Act 84
  - copyright authorship and *lex originis* 79

- Cyber Policy Review 55, 56  
 cyber security intelligence information  
   sharing with private sector companies,  
   call for 259  
 Digital Millennium Copyright Act (DCMA)  
   74–5, 90  
 drones' hacking claims 245  
 due process requirement 47  
 east coast blackout 349  
 Espionage Act 171–2  
 EU–US Working Group on Cyber-Security  
   and Cyber-Crime (WGCC) 408, 411,  
   414  
 excessive intelligence collection methods,  
   criticism of 167  
 Federal Anti-Tampering Law 312–13  
*Hartford Fire Insurance Co v California* 49  
*International Shoe Co v Washington* 20, 47  
 International Strategy for Cyberspace  
   13–14, 343  
 Iran–US Claims Tribunal, *Yeager v Islamic*  
   *Republic of Iran* 60–61  
 National Security Strategy, and anticipatory  
   self-defence 271, 285  
 NSA cyber espionage 62–3, 113, 178,  
   179–80, 184, 473  
 NSA electronic surveillance practices 62,  
   64, 65  
 Patriot Act 165, 269–70  
*People v World Interactive Gaming*  
   *Corporation* 47  
 political dominance 96, 97, 113–14  
 Presidential Decision Directive on cyber  
   capacity 284, 297–8  
 Presidential Policy Directive, cyber  
   espionage definition 170–71  
 privacy and personal data protection 103,  
   114  
*Reno v American Civil Liberties Union* 256  
 Restatement (Third) of Foreign Relations  
   Law 49  
 Snowden (Edward) revelations 53, 62, 64,  
   94–5, 112, 113–15, 169, 172–3, 179,  
   180, 219, 224, 466, 473  
 spy plane incident (Gary Powers) 177  
 Strategic Command, nuclear deterrence 296  
*T-Mobile West Corp. v Crow* 19  
 territoriality principle 80  
*The Exchange v McFaddon* 17  
*US v \$734, 578.82 in US Currency* 47  
*US v Yousef* 20  
 US–China cyber security working group  
   490  
 website blocking 52  
*Yahoo! v La Ligue contre le racisme et*  
   *l'antisémitisme* 193  
*Young v New Haven Advocate* 47  
 Vagts, D 381, 389, 391  
 Valeriano, B 427  
 Van Bochoven, L 428  
 Van Elsuwege, P 413  
 Van Ginkel, B 222  
 Van Hoboken, J 224  
 Van Vooren, B 404, 421, 422  
 Vassilaki, I 38  
 Verdelho, P 200  
 Vermeulen, M 414  
 'virtual group' involvement, classification of  
   cyber warfare 338–40  
 virtual worlds, 'crimes' committed in 191  
 virus attacks 244–5  
   malware 252–3, 257, 261, 308, 309, 312,  
   313, 444  
   Stuxnet *see under* Iran  
   *see also* hackers  
 Viscusi, W 324  
 Vité, S 326  
 Vivant, M 84, 85  
 Vogler, J 24–5  
 Von Heinegg, W 182, 186  
 Wachenfeld, M 390  
 Wala, R 278  
 Walden, I 220  
 Walker, G 397, 400  
 Wall, D 191, 194  
 Waltz, K 97, 174  
 Walzer, M 307  
 war crimes *see* international criminal  
   responsibility, cyber attacks as war  
   crimes  
 'war-sustaining' installations 359–60  
 warfare *see* cyber warfare  
 Wassenaar Arrangement on Export Controls  
   and 'dual use' ICT technologies 115  
 Waters, S 399  
 Watkin, K 214  
 Watt, H 410  
 Watts, A 182, 186  
 Waxman, M 138, 187, 236, 242, 247, 262,  
   265, 427  
 weapons *see* cyber weapons  
 Wegener, H 488  
 Weisbord, N 137  
 Weissbrodt, D 118, 119, 123, 139

- Wenger, A 358  
Werle, G 120, 127  
Werner, W 119, 123, 125, 139, 295  
Wessel, R 258, 403–25, 432  
Wikileaks *see* Snowden (Edward) revelations  
Wills, A 224, 414  
Willson, D 392  
Wilmshurst, E 249, 278, 326  
Wilson, C 92  
Winterfeld, S 229  
Woltag, J-C 149, 426  
Wood, M 183, 250, 252  
World Conference on International  
Telecommunications 111–12, 265–6  
Wortham, A 187  
Wray, R 110  
Wright, J 134, 136  
Wright, Q 181, 185  
Wriston, W 181  
WTO Appellate Body, *United States –  
Measures Affecting the Cross-Border  
Supply of Gambling and Betting Services*  
42, 52  
Wu, T 13, 22  
Yadron, D 324, 332  
Yar, M 157  
Yoo, J 185  
Younes, A 92  
Young, B 55  
Zekoll, J 405, 410  
Zhang, L 233  
Ziolkowski, K 170, 171, 178, 182, 183, 224,  
226, 238, 241, 245, 258, 426–45  
Zuckerberg, M 109

