

Cambridge University Press

978-1-107-02443-4 - Tallinn Manual on the International Law Applicable to Cyber Warfare:
Prepared by the International Group of Experts at the Invitation of the NATO Cooperative
Cyber Defence Centre of Excellence

Michael N. Schmitt

Index

[More information](#)

INDEX

- active cyber defences 257
- Additional Protocols to Geneva Conventions
 - Additional Protocol II type conflicts 90–1
 - on criminal responsibility of commanders and superiors 92
 - on perfidy 180–1
 - on precautions in attack 164
 - reprisals forbidden under Additional Protocol I 152–3
 - on threshold for non-international conflicts 86
- aerial blockades 196
 - cyber warfare used for enforcement of 200–1
- aggregation of incidents, amounting to armed attacks 56
- aircraft, nationality of 23
- airspace, international 21
 - cyber infrastructure in 21–2
- AMW manual (air and missile warfare) 7, 9
- anticipatory self-defence 63–6
- archives, diplomatic, protection in armed conflict of 25–6, 233–4
- armed attacks
 - cyber operations qualifying as 17
 - and self-defence rights 54–62
 - anticipatory 63–6
 - collective 67–8
 - objects of 113–18
 - see also* targeting rules of law of armed conflict
 - and use of force 45–7, 52, 55
 - see also* cyber attacks
- armed conflicts 75
 - international
 - categorizations of 79–82
 - criteria for existence of 79–84
 - and neutrality 15
 - and sovereign immunity 25
 - see also* non-international armed conflicts
 - and neutrality 248–9
 - thresholds for existence of 82–3
 - see also* law of armed conflict
- armed forces
 - conscription/enlisting of children prohibited in 218–20
 - involvement not required for existence of armed conflict 83
- irregular 97
- law enforcement agencies/paramilitary groups incorporated into 100–1
- targetability and combatant immunity of members of 96–102, 116
- armed groups *see* organized armed groups; virtual armed groups
- Articles on State Responsibility (ILC)
 - on countermeasures permissible for injured States 36–41
 - on retroactive attribution of wrongful acts to States 34
 - on State responsibility for wrongful acts by non-State actors 32
- attacks 7
 - indiscriminate 125, 156–9
 - precautions in 164–5, 176–80, 224
 - cancellations/suspensions of attacks 172–3

Cambridge University Press

978-1-107-02443-4 - Tallinn Manual on the International Law Applicable to Cyber Warfare:
Prepared by the International Group of Experts at the Invitation of the NATO Cooperative
Cyber Defence Centre of Excellence

Michael N. Schmitt

Index

[More information](#)

- attacks (cont.)
 - choice of targets duty 170–2
 - constant care duty 165–7, 173
 - means and methods of warfare
 - choice 168–70
 - and proportionality 170
 - verification of targets duty 167–8
 - warnings duty 173–6
 - see also* armed attacks; cyber attacks
- attribution of wrongful acts to States
 - 29–31
 - and governmental authority 31
 - and non-State actor cyber operations
 - 32–3, 35
 - and organs of State concept 31
 - retroactive 34
- authority, governmental, and organs of State 31
- belligerent nexus
 - criterion for direct participation in hostilities 120
 - not present in activities on neutral territory 254
- belligerent reprisals 41, 149–52
- belligerent rights, exercise of 249–50
 - on neutral territory
 - and obligations of neutral States 252–4
 - prohibition of 251–2
 - remedies against failure to stop 254–5
 - prohibited against neutral infrastructure 250
- bleed-over effects, and self-defence
 - rights 57
- blockades
 - cyber 195–8, 201
 - naval/aerial, cyber warfare used for enforcement of 200–1
- booby traps, cyber 146–8
- botnets 33, 257
- breaches of international law
 - see* violations, of international law
- cables, submarine
 - and neutrality 250–1
- ownership of 23
- rights of coastal States over 17–18
- rules on seizure and destruction of, in occupation 247
- camouflage, permissibility of 185
- cancellations of attacks 172–3
- capabilities
 - cyber 53
 - nuclear, of Iran, cyber operations directed against (Stuxnet, 2010) 58, 83–4, 170, 262
- capture, legitimacy of perfidious acts leading to 180–1
- Caroline* incident 63–4
- censorship in armed conflict, legitimacy of 221–2
- children in armed conflict, protection of 218–20
 - in occupation 241
- civilian morale, targeting decline of 133
- civilian objects 125–34
 - feigning status of 183
 - military use of 128–9
 - assessment of 137–40
 - intentions to 129
 - segregation of civilian and military use 177–8
 - see also* dual-use objects
- natural environment as 232
- precautions in attack principles
 - applied to 165–8
 - proximity to military objectives 179
- proportionality principle in attacks
 - on 159–64
- targeting rules applicable to 110, 124–5
- civilians in armed conflict
 - determination of status of 114–15
 - feigning status of 183
 - occupation 240–2
 - protection of objects indispensable to survival of 225–7
 - reprisals against 152–3
 - starvation of, as methods of warfare 148–9, 226
 - targeting rules applicable to 110, 113–14

Cambridge University Press

978-1-107-02443-4 - Tallinn Manual on the International Law Applicable to Cyber Warfare:
Prepared by the International Group of Experts at the Invitation of the NATO Cooperative
Cyber Defence Centre of Excellence

Michael N. Schmitt

Index

[More information](#)

INDEX

265

- distinction principle 110–12
- government employees 118
- proportionality principle 159–64, 170
- see also* direct participation in hostilities; precautions in attack
- close access operations 257
- cloud computing 78, 257
- coastal States, rights over submarine cables 17–18
- coercion
 - economic and political 46
 - necessary element of intervention 44–5
- collateral damage 109, 159–61
 - excessive 161, 223–4
 - obligation to minimize 168–70
 - uncertainty about 163
- collective punishments, prohibition of 234–6
- collective security 72
- collective self-defence 67–8
- collectives, informal groups
 - acting as 90
- combatant immunity 95–102
 - for cyber operations participants 98
 - for *levées en masse* participants 102–3
 - for organized armed group members 97–8, 116–17
 - for spies 195
 - see also* targeting rules of law of armed conflict; unprivileged belligerency
- commanders, criminal responsibility of 91–4
- Commander's Handbook (United States) 8–9, 130–1
- communications, diplomatic,
 - protection in armed conflict of 25–6, 233–4
- compliance
 - with international law, and sovereign immunity 24–5
 - with UN Security Council resolutions, obligations to 255–6
- Computer Emergency Response Teams (CERTs) 31–2, 258
- computer network exploitation (CNE) 193
- computers, computer systems,
 - computer networks 258
 - camouflage of 185
 - medical, protection in armed conflict of 206–10
 - qualifying as weapons 100
 - of UN, protection in armed conflict of 210–13
 - see also* cyber infrastructure
- concurrent jurisdiction, of several States over cyber operations 20–2
- confidence 182
- confiscation of property, in occupation 245–7
- conscription of children into armed forces, prohibition of 218–20
- consensus, on *Tallinn Manual* Rules 6
- consent, of States to conduct cyber operations on its territory 17
- consequences
 - of cyber operations 56–7
 - foreseeable 181, 250
 - immediacy of 49
 - measurability of 50
 - violent 106–8
- constant care duty 165–7, 173
- constructive knowledge of cyber operations 28, 253
- continental shelves, rights over submarine cables in 17–18
- continuous combat function 116–17
- Corfu Channel* case (*United Kingdom v. Albania*, ICJ) 26
- corporations, determination of nationality of 23
- correspondence, of detained persons in armed conflict, protection of 216–17
- countermeasures 36–7
 - cyber 38
 - permissibility of 17, 29
 - for States injured by wrongful acts 36–41

Cambridge University Press

978-1-107-02443-4 - Tallinn Manual on the International Law Applicable to Cyber Warfare:
Prepared by the International Group of Experts at the Invitation of the NATO Cooperative
Cyber Defence Centre of Excellence

Michael N. Schmitt

Index

[More information](#)

- criminal responsibility
 - of commanders and superiors 91–4
 - overall control test for 32–3
- criteria
 - for armed attacks 55
 - for cyber operations qualifying as use of force 48–52
 - for direct participation in hostilities 119–20
 - for existence of international armed conflict 79–84
 - for military objectives 127–9
- cross-border activities
 - in non-international armed conflict 86
 - in self-defence 60–1
- cultural property, targeting rules
 - applicable to 152, 228–30
- customary international law
 - on combatant immunity 96
 - on intervention 44
 - on State responsibility 29
 - and *Tallinn Manual* Rules 6–9
 - on use of force 43–4
- cyber attacks 17, 76, 106–10
 - espionage acts amounting to 195
 - indiscriminate 156–8
 - originators of
 - identification of 110
 - legitimacy of concealment of 183, 189–90
 - precautions in 164–5, 176–80, 224
 - cancellations/suspensions of attacks 172–3
 - choice of targets duty 170–2
 - constant care duty 165–7, 173
 - means and methods of warfare choice 168–70
 - and proportionality 170
 - verification of targets duty 167–8
 - warnings duty 173–6
 - proportionality in 136, 159–64, 170
 - spill-over effects in neutral territory of 250
 - targeting rules applicable to 105
 - civilian objects 110, 124–5
 - civilians 113–14
 - cultural property 228–30
 - dams, dykes and nuclear electrical generating stations 223–5
 - distinction principle 110–12
 - dual-use objects 135–6
 - lawful objects of attack 115–18
 - medical computers, networks and data 206–10
 - medical and religious personnel, medical units and transports 204–5, 208–10
 - military objectives 128
 - natural environment 231–3
 - objects indispensable to survival of civilian population 225–7
 - UN personnel, installations, materiel, units and vehicles 210–13
 - with terror purposes 122–4
 - see also* cyber operations, as armed attacks; cyber warfare
- cyber blockades 195–8, 201
- cyber booby traps 146–8
- cyber capability 53
- cyber countermeasures 38
- cyber defences
 - active 257
 - passive 261
- cyber espionage 50, 192–5
- cyber infrastructure 15, 142, 258
 - camouflage of 185
 - control by States/parties to a conflict over 26–9, 178
 - as immovable or movable State property 245–6
 - and jurisdiction of States 18–21
 - flag States and States of registration 21–3
 - as military objective 133–4
 - neutral 248–9, 252–3
 - protection of 250
 - as object indispensable to survival of civilian population 227
 - obligations of Occupying Powers to restore and maintain 242–3
 - and State sovereignty 15–18
 - use of
 - for cyber attacks 183

Cambridge University Press

978-1-107-02443-4 - Tallinn Manual on the International Law Applicable to Cyber Warfare:

Prepared by the International Group of Experts at the Invitation of the NATO Cooperative

Cyber Defence Centre of Excellence

Michael N. Schmitt

Index

[More information](#)

INDEX

267

- from another State, and State responsibility 36
- governmental, and State responsibility 34–5
- and territorial jurisdiction 19
- cyber operations 1–2, 15, 76, 258
 - as armed attacks 17
 - and self-defence rights 54–62
 - anticipatory 63–6
 - collective 67–8
 - see also* cyber attacks
- combatant status for persons
 - engaged in 98
- criminal 101–2
- diplomatic, protection of 234
- harmful, prevention of 27–9
- jurisdiction of States over 18–26
- and *jus ad bellum* 42
 - threat or use of force 17, 42–5
- law of armed conflict applicable to 3, 75–8
 - blockades 195–8, 200–1
 - civilian status presumption 115
 - collective punishments 234–6
 - combatant immunity/unprivileged belligerency 101–3
 - conscription/enlistment of children 218–20
 - constant care duty 165–7, 173
 - criminal responsibility of commanders and superiors 91–4
 - detained persons 214–18
 - espionage 50, 192–5
 - journalists 220–2
 - levée en masse* 103
 - mercenaries 103–4
 - non-interference with humanitarian assistance 236–8
 - non-international armed conflicts 85–8
 - participation in hostilities 95, 120–2
 - perfidy 180–4
 - precautions in attack *see* cyber attacks, precautions in
 - protective emblems, prohibition on improper use of 185–92
 - ruses 184–5
 - see also* cyber attacks, targeting rules applicable to
- law of neutrality applicable to 78, 248–9
 - and compliance with UN Security Council resolutions 255–6
 - obligations of neutral States 252–4
 - operations in neutral territory 251–2
 - protection of neutral cyber infrastructure 250
 - remedies against enemy's unlawful activities on neutral territory 254–5
- law of occupation applicable to 239–40
 - confiscation/requisition of property 245–7
 - Occupying Powers allowed to ensure its security 244–5
 - protection of civilians 240–2
 - public order and safety ensured in 242–4
- non-forceful measures against threats to peace 70
- by non-State actors 18, 54
 - and attribution of wrongful acts to States 32–3, 35
- and operational zones 202
- remedial 28
- and responsibility of States 15, 29–34
 - countermeasure permissible 36–41
 - governmental infrastructure use 34–5
 - infrastructure used of another State 36
- as self-defence acts 68
- and sovereignty of States 15–18
- and use/threats of force 43, 45–53
 - prohibited use/threats 17, 42–5
- cyber security 2, 4, 13
- cyber warfare
 - international law applicable to 3, 13
 - US policies on 2–3
 - means and methods of 140–2

Cambridge University Press

978-1-107-02443-4 - Tallinn Manual on the International Law Applicable to Cyber Warfare:
Prepared by the International Group of Experts at the Invitation of the NATO Cooperative
Cyber Defence Centre of Excellence

Michael N. Schmitt

Index

[More information](#)

268

INDEX

- cyber warfare (cont.)
 - booby traps 146–8
 - indiscriminate 144–6, 156–9
 - precautions in choice of 168–70
 - reprisals 149–53
 - starvation of civilians 148–9, 226
 - to enforce naval/aerial blockades 200–1
 - unnecessary suffering 143–4
 - weapons reviews 153–6
 - see also* cyber attacks
- cyber weapons 100, 141–2
 - transmission across neutral territory of 252
 - uncontrollable chains of events created by 145–6
- cyber zones 199–200
- cyberspace 258
 - armed conflicts in 84
 - hostile use of 13
 - jurisdiction in 19
 - neutrality in 249
 - sovereignty over 18
- damage
 - causation of, and wrongful acts 30
 - caused by cyber attacks 108–9
 - collateral 109, 159–61
 - excessive 161, 223–4
 - obligation to minimize 168–70
 - uncertainty about 163
 - see also* harm
- dams, cyber attacks on, duty of care for 223–5
- data 258
 - attacks on
 - harm caused by 107–9
 - as military objective 127
 - determination of residence of 19
 - dual-use of, targetability of 136–7, 206
 - medical
 - identification of 207–8
 - protection in armed conflict of 206–8
 - loss of 208–10
 - as property 245
 - transit of, in armed conflict 78
- definitions
 - blockades 195
 - booby traps 146–7
 - botnets 257
 - civilian objects 125–34
 - civilians 104, 113
 - cloud computing 257
 - computers, computer networks and computer systems 258
 - countermeasures 36–7
 - cultural property 228
 - cyber attacks 106–10
 - cyber espionage 193
 - cyber infrastructure 258
 - cyber operations 258
 - cyberspace 258
 - data 258
 - high seas 21
 - humanitarian assistance 237
 - international airspace 21
 - Internet 260
 - malware/malicious logic 260
 - mercenaries 104
 - military objectives 125–34
 - natural environment 231–2
 - occupation 239
 - outer space 21
 - perfidy 180–1
 - social networks 261
 - software 261
 - spoofing 261
 - State jurisdiction 18
 - State sovereignty 16
- delayed effects, and direct participation in hostilities 121
- Denial of Service (DoS) 259
- destruction
 - of property, and perfidy 182–3
 - wanton 232
- detained persons in armed conflict, law of armed conflict applicable to 213–14, 216–18
- digital cultural property 229–30
- diplomatic archives and communications, protection in armed conflict of 25–6, 233–4

Cambridge University Press

978-1-107-02443-4 - Tallinn Manual on the International Law Applicable to Cyber Warfare:
Prepared by the International Group of Experts at the Invitation of the NATO Cooperative
Cyber Defence Centre of Excellence

Michael N. Schmitt

Index

[More information](#)

INDEX

269

- direct participation in hostilities 95–6, 104–6, 118–22
 - by journalists 222
 - and presumption of civilian status 115
- directness criterion for determination of use of force 49
- distinction principle 110–12
- distinctive sign/emblem requirements
 - for combatant status 99–100
 - for cultural property 230
 - for medical transports and units 206–8
- domestic law
 - criminal cyber operations in 101–2
 - obligations of Occupying Powers for maintaining of 243
- doubt, threshold of, for presumption of civilian status 114–15
- drafting of *Tallinn Manual* 10–11
- dual-use objects
 - segregation of military and civilian use in 177–8
 - targetability of 134–7, 206
- due care threshold 28
- duration, of direct participation in hostilities 121
- dykes, cyber attacks on, duty of care for 223–5
- economic coercion 46
- economic objects, war-sustaining, targetability of 130–1
- effective contribution to military action 130, 137–40
- effectiveness
 - of control
 - over cyber operations by commanders/superiors 93–4
 - tests 32, 92–3
 - of cyber blockades 197–8
 - of warnings 174–5
- effects *see* consequences
- emblems
 - distinctive
 - for cultural property 230
 - for medical transports and units 206–8
 - prohibition on improper use of 185–92
- enemies
 - acts harmful to 208–9
 - indicators of, prohibition on improper use of 188–91
- enforcement
 - actions by international organizations 69–72
 - of blockades 200–1
 - of law, agencies in armed forces 100–1
- equipment
 - diplomatic, protection of 234
 - journalistic, protection of 222
 - medical
 - identification of 206–8
 - protection of 204–6, 208–10
 - military
 - rules on use when gaining control of 190–1
 - State responsibility for use of 35
 - of UN, protection of 210–13
- espionage
 - cyber 50, 192–5
 - and perfidy 183
 - State responsibility for 30
- essential interests, necessity defences based on 40
- Estonia, cyber operations directed against (2007) 40–1, 57–8, 82
 - Estonian jurisdiction over 20
 - law of armed conflict not applicable to 75
- exceptions, to State sovereignty 16
- excessiveness, of collateral damage 161, 223–4
- expression, freedoms of, Occupying Powers imposing limitations on 243
- extraterritorial jurisdiction 20
 - over cyber operations 20
- flag States, jurisdiction over cyber infrastructure by 21–3
- flags, warships carrying neutral or enemy 191

Cambridge University Press

978-1-107-02443-4 - Tallinn Manual on the International Law Applicable to Cyber Warfare:
Prepared by the International Group of Experts at the Invitation of the NATO Cooperative
Cyber Defence Centre of Excellence

Michael N. Schmitt

Index

[More information](#)

- force
 - prohibited use of 42
 - for countermeasures 37–8
 - cyber operations as 17, 42–5
 - use/threats of
 - and armed attacks 45–7, 52, 55
 - cyber operations as 43, 45–53
 - UN Security Council
 - authorizations for 69–71
 - see also jus ad bellum*
- foreseeable consequences of attacks/
 - cyber attacks 181, 250
- freedoms of expression, Occupying
 - Powers imposing limitations
 - on 243
- functionality, interference with, as
 - damage caused by cyber
 - attacks 108–9
- Gabčíkovo-Nagymoros case*
 - (*Hungary v. Slovakia*, ICJ)
 - 38–9
- Galić case* (ICTY) 163
- Geneva Conventions (1949) 8–9
 - on criteria for existence of
 - international/
 - non-international armed
 - conflict 79, 84–6
 - on obligations to prosecute war
 - crimes 91–2
- Genocide case (Bosnia and Herzegovina v. Serbia and Montenegro, ICJ)* 32–3, 80
- geo-coordinates, tracking of, and
 - territorial jurisdiction 19
- geographical limitations
 - on blockades 197
 - on cyber operations in armed
 - conflict 78–9
 - on non-international armed
 - conflicts 78–9, 85–6
- Georgia, cyber operations directed
 - against (2008 conflict with
 - Russia) 20, 75–6
- government employees, civilian,
 - targetability of 118
- government purposes, sovereign
 - immunity for cyber
 - infrastructure devoted
 - exclusively to 24
- governmental authority, and organs of
 - State 31
- governmental cyber infrastructure,
 - State responsibility for
 - operations launched from
 - 34–5
- Hague Conventions on the Laws and
 - Customs of War on Land
 - (1907)
 - Convention IV 77
 - Regulations 8–9, 242–3, 246–7
 - Convention V 251–2
- Hague Cultural Property Convention
 - (1954) 228–30
- harm
 - caused by attacks on data 107–9
 - thresholds of 56, 107, 113
 - see also* damage
- harmful cyber operations/attacks,
 - prevention of 27–9
- high seas 21
 - cyber infrastructure on 21–2
- hors de combat* status 116
- hostile acts *see* belligerent rights
- hostilities
 - armed conflict in absence of 84
 - participation in 95
 - see also* direct participation in
 - hostilities
 - requirement for existence of armed
 - conflict 82–3
- human rights law
 - and limitations on freedoms
 - of expression in occupation
 - 243
 - and restricted access to Internet 17
- humanitarian assistance operations
 - non-interference with 236–8
 - protection of those involved in
 - 210–13
- ICC (International Criminal Court)
 - Statute, on criminal
 - responsibility of commanders
 - and superiors 93, 94

Cambridge University Press

978-1-107-02443-4 - Tallinn Manual on the International Law Applicable to Cyber Warfare:
Prepared by the International Group of Experts at the Invitation of the NATO Cooperative
Cyber Defence Centre of Excellence

Michael N. Schmitt

Index

[More information](#)

INDEX

271

- ICJ (International Court of Justice)
 Advisory Opinions, *Nuclear Weapons (Legality of the Threat or Use of Nuclear Weapons)* 54, 111, 140–1
 on armed attacks 45–7, 54, 56
 Cases
 Corfu Channel (United Kingdom v. Albania) 26
 Gabčíkovo-Nagymoros (Hungary v. Slovakia) 38–9
 Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) 32–3, 80
 Nicaragua (Military and Paramilitary Activities in and against Nicaragua) 26, 44–7, 55–6, 58, 61, 68
 Oil Platforms (Iran v. United States) 38, 56, 61
 Tehran Hostages (United States v. Iran) 234
 on countermeasures 38–9
 on effective/overall control 32, 80
 on law of armed conflict 3
 on means and methods of warfare 143
 on prohibited interventions 44
 on protection of diplomatic premises 234
 on self-defence rights 68
 on sovereign equality 26
 ICRC (International Committee of the Red Cross)
 on belligerent reprisals 151
 on collective punishments 235
 Customary International Humanitarian Law Study of 7
 on improper use of enemy/neutral indicators 190, 192
 Interpretive Guidance 97–8
 on *levées en masse* 102–3
 on military advantage 132
 observer status at drafting of *Tallinn Manual* 10
 on perfidy 182
 on precautions in attack 164–5, 177
 on protection of natural environment 232
 on threshold of violence for existence armed conflict 82–3
 ICT use *see* cyber infrastructure
 ICTY (International Criminal Tribunal for the Former Yugoslavia)
 Cases
 Galić 163
 Limaj 89
 Tadić 32–3, 80–1, 87–8
 on organized armed groups 89
 overall control test of 32–3, 80–2
 on proportionality in attack 163
 on thresholds for non-international armed conflicts 87–8
 identification
 of medical computers, networks and data 206–8
 of originators of cyber attacks 110
 immediacy
 of consequences 49
 requirement for self-defence acts 66–7
 imminent attacks, and self-defence rights 63–6
 immovable State property, obligations of Occupying Powers to safeguard capital value of 245–6
 immunity
 combatant 95–102
 for cyber operations participants 98
 for *levées en masse* participants 102–3
 for spies 195
 sovereign, and international armed conflicts 25
 incidents, amounting to armed attacks 56
 indirect effects of cyber attacks 160–1
 indiscriminate attacks/means and methods of warfare 125, 144–6, 156–9
 individuals
 criminal responsibility of 32–3, 91–4
 overall control test not applicable to 81–2

Cambridge University Press

978-1-107-02443-4 - Tallinn Manual on the International Law Applicable to Cyber Warfare:
Prepared by the International Group of Experts at the Invitation of the NATO Cooperative
Cyber Defence Centre of Excellence

Michael N. Schmitt

Index

[More information](#)

- individuals (cont.)
 - prohibition to direct
 - countermeasures at 39
- informal groups, collective activities of 90
- injury
 - prohibition to cause superfluous 143–4
 - see also* collateral damage, excessive
- intensity criterion for non-international armed conflicts 87
- and cyber operations 88
- intentions
 - of armed attacks, and self-defence rights 59–60
 - of cyber operations, relevance of 57
 - to attack objects indispensable to survival of civilian population 226
 - to carry out threats of force 53–4
 - to spread terror 123–4
 - to use a civilian object for military ends 129
- interception of cyber attacks 110
- interference 217
 - with functionality, as damage caused by cyber attacks 108–9
 - with humanitarian assistance operations 236–8
 - with sovereign immunity 24
- international airspace 21
- cyber infrastructure in 21–2
- international armed conflicts
 - categorizations of, and State control over non-State actors 79–82
 - criteria for existence of 79–84
 - law of neutrality in, and cyber operations/infrastructure 15
 - and sovereign immunity 25
 - see also* law of armed conflicts non-international armed conflicts
- international cyber security law 13
- international humanitarian law *see* law of armed conflict
- international law
 - applicable to cyber warfare *see* law of armed conflict, applicable to cyber operations
 - applicable to cyberspace 3, 13
 - compliance with, and sovereign immunity 24–5
 - customary
 - on combatant immunity 96
 - on intervention 44
 - on State responsibility 29
 - and *Tallinn Manual* Rules 6–9
 - on use of force 43–4
 - legality presumption in 51
 - obligations
 - to comply with UN Security Council resolutions 255–6
 - to prevent acts contrary to international law 27–8
 - to prosecute war crimes 91–2
 - State jurisdiction limited by 21
 - peremptory norms of 39
 - on sovereign immunity 23–4
 - violations/breaches of
 - interference with sovereign immunity 24
 - involvement of States with non-State actors as 33–4
 - and State responsibility for cyber operations 29–34
- international telecommunications law, and restricted access to Internet 17
- internationally wrongful acts
 - see* wrongful acts
- Internet 260
 - cyber attacks against 136
 - military use of, and neutrality 251
 - and objects indispensable to survival of civilian population 227
 - restricting access to 17
- interventions, UN Charter prohibition on 44
 - cyber operations as violations of 17, 44–5
- invasiveness criterion for
 - determination of use of force 49–50
- Iran, cyber operations directed against nuclear capabilities of (Stuxnet, 2010) 58, 83–4, 170, 262

Cambridge University Press

978-1-107-02443-4 - Tallinn Manual on the International Law Applicable to Cyber Warfare:
Prepared by the International Group of Experts at the Invitation of the NATO Cooperative
Cyber Defence Centre of Excellence

Michael N. Schmitt

Index

[More information](#)

INDEX

273

- irregular armed forces 97
- Island of Palmas* Arbitral Award
(*Netherlands v. US*) 16
- journalists in armed conflict, protection
of 220–2
- jurisdiction of States over cyber
infrastructure/operations
18–26
- jus ad bellum*
and cyber operations 42
threat or use of force 17, 42–5
and law of armed conflict 77
- knowledge, constructive, of cyber
operations 28, 253
- Kosovo Liberation Army (KLA) 89
- last feasible window of opportunity
standard 64–5
- law of armed conflict
applicable to cyber operations 3,
75–8
blockades 195–8, 200–1
collective punishments 234–6
combatant immunity/
participation in hostilities 95,
101–3
see also direct participation in
hostilities
constant care duty 165–7, 173
criminal responsibility of
commanders and superiors
91–4
distinction principle 110–12
espionage 50, 192–5
improper use of protective
emblems prohibition 185–92
indiscriminate attacks, means and
methods prohibition 125,
144–6, 156–9
non-interference with humanitarian
assistance 236–8
non-international armed conflicts,
existence of 84–91
participation in hostilities
see direct participation in
hostilities
- perfidy 180–4
- precautions in attack *see* cyber
attacks, precautions in
- presumption of civilian status 115
- ruses 184–5
see also cyber attacks means and
methods of cyber warfare
protections in armed conflict
targeting rules of law of
armed conflict
- customary 7, 29
- and sovereign immunity 25
see also targeting rules of law of
armed conflict
- law enforcement *see* enforcement
- law of neutrality 15, 78, 248–9
and compliance with UN Security
Council resolutions 255–6
cyber operations in neutral territory
251–2
inviolability of neutral territory in
250
obligations of neutral States in 252–4
protection of neutral cyber
infrastructure in 250
remedies against enemy's unlawful
activities on neutral territory
254–5
- law of occupation 240
and collective punishments 235–6
confiscation/requisition of property
245–7
protection of civilians in 240–2
public order and safety assurances
242–4
and security of Occupying Powers
244–5
- law of the sea, and rights over
submarine cables 17–18
- legality presumption in international
law 51
- levées en masse participants
combatant immunity for 102–3
targetability of 116, 118
- Limaj* case (ICTY) 89
- limitations
on freedoms of expression, imposed
by Occupying Powers 243

Cambridge University Press

978-1-107-02443-4 - Tallinn Manual on the International Law Applicable to Cyber Warfare:
Prepared by the International Group of Experts at the Invitation of the NATO Cooperative
Cyber Defence Centre of Excellence

Michael N. Schmitt

Index

[More information](#)

- limitations (cont.)
 - geographical
 - on blockades 197
 - on cyber operations in armed conflict 78–9
 - on non-international armed conflicts 85–6
 - on State jurisdiction, by international law obligations 21
 - on State sovereignty 17
- locations
 - criterion for military objectives 128
 - of cyber operations, and State responsibility 33
 - of ICT users, and territorial jurisdiction 19
- malware 260, 262
 - assessment of damage caused by 16
 - introduction of, as cyber attack 109–10
- manuals
 - on cyber warfare *see Tallinn Manual*
 - military
 - used as source for *Tallinn Manual* 8–9
 - on war-sustaining activities 130–1
- Martens Clause 77–8
- means and methods of cyber warfare 140–2
 - booby traps 146–8
 - indiscriminate 144–6, 156–9
 - precautions in choice of 168–70
 - reprisals 149–53
 - to enforce naval/aerial blockades 200–1
 - unnecessary suffering 143–4
 - weapons reviews 153–6
- measurability of consequences 50
- medical personnel, units and transport, computers, computer networks and data
 - identification of 206–8
 - protection in armed conflict of 204–6
 - loss of 208–10
- membership, of organized armed groups 97–8, 116–17
- mercenaries, unprivileged belligerent status of 103–4
- methods of warfare *see* means and methods of warfare
- military activities, prohibition of compulsory participation in
 - detained persons 217–18
 - enemy nationals in occupation 242
- military advantage 130–3, 161–2
 - and precautions in attack 171–2
- military character criterion for determination of use of force 50–1
- military commanders/superiors, criminal responsibility of 91–4
- military equipment
 - of enemy, rules on use when gaining control of 190–1
 - State responsibility for use of 35
- military manuals
 - used as source for *Tallinn Manual* 8–9
 - on war-sustaining activities 130–1
- military objectives 7
 - attacks on/targetability of 114, 125–34
 - dual-use objects 134–7
 - segregation of military and civilian use 177–8
 - proximity of civilians and civilian objects to 179
- motives *see* intentions
- nationality, of aircrafts and satellites 23
- NATO (North Atlantic Treaty Organization)
 - Allied Command Transformation 9–10
 - as collective security organization 72
 - Cooperative Cyber Defence Centre of Excellence (Tallinn, Estonia) 1
 - Strategic Concept (2010), cyber warfare included in 2–3
- natural environment, protection in armed conflict of 231–3
- nature criterion, for military objectives 127

Cambridge University Press

978-1-107-02443-4 - Tallinn Manual on the International Law Applicable to Cyber Warfare:
Prepared by the International Group of Experts at the Invitation of the NATO Cooperative
Cyber Defence Centre of Excellence

Michael N. Schmitt

Index

[More information](#)

INDEX

275

- Naulilaa Arbitral Award (Portugal v. Germany)* 38
- naval blockades, cyber warfare used for enforcement of 200–1
- necessity
- defences, actions/countermeasures based on 39–40
 - determination of 245
 - principle, in exercise of self-defence rights 61–3
- neutral indicators, prohibition on improper use of 191–2
- neutrality
- and blockades 198, 200–1
 - law of 15, 78, 248–9
 - and compliance with UN Security Council resolutions 255–6
 - and cyber operations in neutral territory 251–2
 - inviolability of neutral territory in 250
 - obligations of neutral States in 252–4
 - protection of neutral cyber infrastructure 250
 - remedies against enemy's unlawful activities on neutral territory 254–5
- neutralization, of military objectives 132–3
- NIAC Manual (non-international armed conflicts) 7–8
- Nicaragua case (Military and Paramilitary Activities in and against Nicaragua, ICJ)* 26, 44–7, 55–6, 58, 61, 68
- non-commercial use 35
- non-forceful measures against threats to peace 69–70
- non-international armed conflicts 84–91
- civilians in 105
 - geographic limitations of 78–9, 85–6
 - law of armed conflict applicable to
 - attacks on objects indispensable to survival of civilian population 226
 - blockades 198
 - combatant immunity absent from 101–2
 - and cyber operations 76–7
 - distinction principle 111
 - humanitarian assistance operations 236
 - improper use of neutral indicators 192
 - precautions in attack 176
 - manuals on 7–8
 - presumption of civilian status in 115
- non-intervention principle 44
- cyber operations as violations of 17, 44–5
- non-kinetic armed attacks 54–5
- non-State actors
- armed attacks by, and self-defence rights 58–9
 - in armed conflict
 - as armed attack 54
 - State control over 79–82
 - as violations of State sovereignty 18
 - cyber operations by, and attribution of wrongful acts to States 32–3, 35
 - State involvement with, as violation of international law 33–4
 - UN Charter prohibition on use of force not applicable to 43–4
- norms, peremptory, of international law 39
- nuclear capabilities, of Iran, cyber operations directed against (Stuxnet, 2010) 58, 83–4, 170, 262
- nuclear electrical generating stations, cyber attacks on, duty of care for 223–5
- Nuclear Weapons Advisory Opinion (Legality of the Threat or Use of Nuclear Weapons, ICJ)* 54, 111, 140–1
- objective territorial jurisdiction 20
- over cyber operations 20
- objects 126–7
- of attack 113–18, 125

Cambridge University Press

978-1-107-02443-4 - Tallinn Manual on the International Law Applicable to Cyber Warfare:
Prepared by the International Group of Experts at the Invitation of the NATO Cooperative
Cyber Defence Centre of Excellence

Michael N. Schmitt

Index

[More information](#)

- objects (cont.)
 - see also* targeting rules of law of armed conflict
- obligations
 - of international law
 - breaches of, and State responsibility for cyber operations 29–34
 - State jurisdiction limited by 21
 - to comply with UN Security Council resolutions 255–6
 - to prevent acts contrary to international law 27–8
 - to prosecute war crimes 91–2
 - of neutral States 252–4
 - of Occupying Powers 241–3
 - of parties to armed conflicts
 - to care for dams, dykes and nuclear electrical generating stations 223–5
 - to respect and protect
 - journalists 220–1
 - medical and religious personnel, medical units and transports 205–6
 - UN personnel 211–12
 - to take precautions in attack 164–5, 167–80
 - of States
 - to respect the sovereignty of other States 26
 - to review weapons 153–6
- occupation law 239–40
 - and collective punishments 235–6
 - confiscation/requisition of property in 245–7
 - protection of civilians in 240–2
 - public order and safety assurances 242–4
 - and security of Occupying Powers 244–5
- Oil Platforms* case (*Iran v. United States*, ICJ) 38, 56, 61
- operational zones 199–200
 - cyber operations in support of 202
- organized armed groups 88–90
 - criteria for combatant status of members of 97
 - prohibition to conscript/enlist children in 218–20
 - targetability/combatant status of members of 97–8, 116–17
 - virtual organizations qualifying as 98–9
- organs of State 30–1
 - constructive knowledge of 253
 - governmental authority equated with 31
 - and State responsibility 31
- originators
 - of armed attacks 58
 - of cyber attacks
 - identification of 110
 - legitimacy of concealing of 183, 189–90
- outer space 21
 - cyber infrastructure in 21–2
 - inclusion in natural environment of 231–2
- overall control test 32–3, 79–82
- paramilitary groups, incorporated into armed forces 100–1
- passive cyber defences 261
- passive precautions 176–7
 - failure to take 180
- peace
 - threats to 69
 - non-forceful measures against 69–70
- peacekeeping operations, protection of persons involved in 210–13
- peremptory norms of international law 39
- perfidy, prohibition of 180–4
- Permanent Court of Arbitration, *Island of Palmas* Arbitral Award (*Netherlands v. US*) 16
- Permanent Court of International Justice, on international law 3
- platforms, jurisdiction over cyber infrastructure on
 - enjoying sovereign immunity 23–6
 - in high seas/international airspace/outer space 21–3
- policing, of cyber operations 28

Cambridge University Press

978-1-107-02443-4 - Tallinn Manual on the International Law Applicable to Cyber Warfare:
Prepared by the International Group of Experts at the Invitation of the NATO Cooperative
Cyber Defence Centre of Excellence

Michael N. Schmitt

Index

[More information](#)

INDEX

277

- political coercion 46
- precautions in attack 164–5, 176–80, 224
 - cancellations/suspensions of attacks 172–3
 - choice of targets duty 170–2
 - constant care duty 165–7, 173
 - means and methods of warfare
 - choice 168–70
 - and proportionality 170
 - verification of targets duty 167–8
 - warnings duty 173–6
- preparations, for attacks 65
- presumptions
 - of civilian status 114–15
 - of civilian use of objects 137–40
 - against direct participation in hostilities 122
 - of legality in international law 51
 - of public ownership, for confiscation and requisition of property in occupation 246
- prevention
 - of acts contrary to international law 27–8
 - of exercise of belligerent rights 253–4
 - of harmful cyber operations/attacks 27–9
- preventive strikes 65–6
- private contractors, targetability of 117–18
- private property, rules on confiscation/requisition of 246–7
 - in occupation 246–7
- propaganda, spread of, as direct participation in hostilities 222
- property
 - confiscation/requisition of, in occupation 245–7
 - cultural, protection of 152, 228–30
 - destruction of, and perfidy 182–3
 - see also* civilian objects dual-use
 - objects military objectives
- proportionality principle
 - in countermeasures 38–9
 - in cyber attacks 159–64, 170
 - against Internet 136
 - in exercise of self-defence rights 61–3
- prosecution, of war crimes, obligations of 91–2
- prospective acts 27
- protections in armed conflict
 - of children 218–20
 - of civilians/civilian objects 113–14
 - distinction principle 110–12
 - in occupation 240–2
 - see also* direct civilian participation in hostilities
 - precautions in attack
 - of cultural property 228–30
 - of detained persons 213–18
 - of diplomatic archives and communications 25–6, 233–4
 - of journalists 220–2
 - of medical personnel, units and transport, computers, systems and networks 204–8
 - loss of 208–10
 - of natural environment 231–3
 - of neutral cyber infrastructure 250
 - of objects indispensable to survival of civilian population 225–7
 - religious personnel 204–5
 - specific 203–4
 - of UN personnel, installations, materiel, units and vehicles 210–13
- protective emblems, prohibition on improper use of 185–92
- protracted violence 88
- proximate causes of death or injury 181–2
- punishments, collective, prohibition of 234–6
- purposes
 - of countermeasures 37
 - criterion for military objectives 129
- reasonableness tests 27
- Red Cross/Crescent/Crystal
 - prohibition on improper use of 185–7
 - see also* ICRC
- regional organizations, self-defence rights exercised by 71–2

Cambridge University Press

978-1-107-02443-4 - Tallinn Manual on the International Law Applicable to Cyber Warfare:
Prepared by the International Group of Experts at the Invitation of the NATO Cooperative
Cyber Defence Centre of Excellence

Michael N. Schmitt

Index

[More information](#)

278

INDEX

- registration, States of, jurisdiction over
 - cyber infrastructure by 21–3
- religious personnel
 - protection in armed conflict of
 - 204–5
 - loss of 208–10
- remedial cyber operations 28
- remote control over cyber operations,
 - and State jurisdiction 22
- repeated actions, qualifying as direct
 - participation in hostilities
 - 121–2
- reprisals
 - Additional Protocol I on 152–3
 - belligerent 41, 149–52
- requisition of property 137
 - in occupation 245–7
- respect, duties to 26, 165–7, 205,
 - 211–12, 220–1, 228–30, 241
- responsibility
 - criminal 32–3, 91–4
 - of States
 - for cyber operations 15, 29–34
 - countermeasures permissible
 - 36–41
 - from governmental
 - infrastructure 34–5
 - routed through another State 36
 - invocation by another State 39
- retorsion, acts of 40
- retroactive attribution of wrongful
 - acts 34
- Rome Statute *see* ICC (International Criminal Court) Statute
- ruses
 - legitimacy of use of 131, 184–5,
 - 189–90
 - and perfidy 184
 - warnings as 176
- Russian Federation, cyber operations in
 - international armed conflict
 - with Georgia (2008) by 20,
 - 75–6
- St Petersburg Declaration (1868)
 - 124–5
- sanctuary, provision of, and use of force
 - criteria 46–7
- satellites
 - nationality of 23
 - sovereign immunity of 24
- seas
 - high 21
 - cyber infrastructure in 21–2
 - law of 17–18
- security
 - collective 72
 - cyber 2, 4, 13
 - of Occupying Powers, measures
 - allowed for assurance of 244–5
- threats
 - cyber warfare as 2
 - laws/freedoms suspended because
 - of 243
 - violations of law of neutrality
 - qualifying as 255
- self-defence rights
 - armed (cyber) attacks triggering of
 - 17, 54–61
 - anticipatory 63–6
 - collective 67–8
- exercise of
 - necessity and proportionality
 - principle in 61–3
 - by regional organizations 71–2
 - reporting requirement to UN
 - Security Council 68
 - by United Nations Security
 - Council 69–71
 - use of force in 42
- invocation of 29
 - of UN personnel 212–13
- self-determination rights 82
- severity criterion for determination of
 - use of force 48
- Simma, Judge 38
- social networks 261
 - legitimacy of cyber attacks against
 - 135–6
- software 261
 - qualifying as weapons 100
- sovereign equality principle 26
- sovereign immunity, cyber
 - infrastructure on platforms
 - subject to, jurisdiction over
 - 23–6

Cambridge University Press

978-1-107-02443-4 - Tallinn Manual on the International Law Applicable to Cyber Warfare:
Prepared by the International Group of Experts at the Invitation of the NATO Cooperative
Cyber Defence Centre of Excellence

Michael N. Schmitt

Index

[More information](#)

INDEX

279

- sovereignty of States
 - and control over cyber
 - infrastructure/operations 15–18
 - and cross-border actions in self-defence 60–1
 - obligations of States to respect 26
- space *see* cyberspace outer space
- speculative advantage 132
- spill-over effects in neutral territory, of cyber attacks 250
- spoofing 261
 - of locations, and territorial jurisdiction 19
 - by non-State actors, and State responsibility 35
- spying *see* espionage
- starvation of civilians, prohibited as method of warfare 148–9, 226
- States
 - attribution of wrongful acts to 29–31
 - and governmental authority 31
 - and non-State actor cyber operations 32–3, 35
 - and organs of State concept 31
 - retroactive 34
 - control of
 - over cyber infrastructure/operations 15–18, 26–9, 178
 - over non-State actors 79–82
 - immovable property of, obligations of Occupying Powers to safeguard capital value of 245–6
 - immunity of 25
 - involvement of, as criterion for determination of use of force 51
 - jurisdiction over cyber
 - infrastructure/operations 18–26
 - neutral 248, 252–4
 - obligations of
 - to respect sovereignty of other States 26
 - to review weapons 153–6
 - recognition of cyber warfare as security threat by 2
 - responsibility of
 - for cyber operations 15, 29–34
 - countermeasures permissible in cases of 36–41
 - from governmental infrastructure 34–5
 - routed through a State 36
 - invocation by another State 39
 - sovereignty of, and cross-border actions in self-defence 60–1
- Stuxnet operations (2010) 58, 83–4, 170, 262
- subjective territorial jurisdiction 19–20
- submarine cables
 - and neutrality 250–1
 - ownership of 23
 - rights of coastal States over 17–18
 - rules on seizure or destruction of, in occupation 247
- suffering, unnecessary 143–4
- superiors, criminal responsibility of 91–4
- survival of civilian population
 - assurances of continued computer operations essential to 242
 - prohibition of attack on objects indispensable to 225–7
- suspension of attacks 172–3
- Tadić* case (ICTY) 32–3, 80–1, 87–8
- Tallinn Manual* 1, 3–4
 - authority of 11
 - commentary 6–7
 - drafting process 10–11
 - international group of experts 9–10
 - Rules 5–6
 - consensus on 6
 - scope of 4–5
 - sources 9
 - of customary international law 7–9
 - military manuals 8–9
 - secondary 9
 - targeting rules of law of armed conflict 106, 115–18
 - choice of targets duty 170–2

Cambridge University Press

978-1-107-02443-4 - Tallinn Manual on the International Law Applicable to Cyber Warfare:
Prepared by the International Group of Experts at the Invitation of the NATO Cooperative
Cyber Defence Centre of Excellence

Michael N. Schmitt

Index

[More information](#)

- targeting rules of law of armed conflict (cont.)
 - civilian objects 110, 124–5
 - civilians 110, 113–14
 - and direct participation in hostilities 95–6, 118–22
 - government employees 118
 - proportionality principle 159–64
 - cultural property 152, 228–30
 - dams, dykes and nuclear electrical generating stations 223–5
 - distinction principle in 110–12
 - dual-use objects 134–7, 206
 - medical personnel, units and transports, computers, networks and data 204–10
 - military objectives 125–34
 - natural environment 231–3
 - objects indispensable to survival of civilian population 225–7
 - organized armed group members 97–8, 116–17
 - religious personnel 204–5, 208–10
 - UN personnel, installations, materiel, units and vehicles 188, 210–13
 - verification of targets duty 167–8
 - see also* combatant immunity
 - protections
 - Tehran Hostages case (United States v. Iran, ICJ)* 234
 - telecommunications law, international, and restricted access to Internet 17
 - terminology problems 7
 - regarding countermeasures 40–1
 - territorial jurisdiction 18
 - and ICT use 19
 - objective 20
 - subjective 19–20
 - see also* extraterritorial jurisdiction
 - territorial sea, rights over submarine cables in 17–18
 - territories
 - neutral 248
 - belligerent nexus not present in activities on 254
 - cyber operations on 251–2
 - inviolability of 250
 - remedies against enemy's unlawful activities on 254–5
 - physical control of, and Additional Protocol II type conflicts 90–1
 - terror, prohibition of spreading of 122–4
 - threats
 - of cyber attacks 123
 - to peace 69
 - non-forceful measures against 69–70
 - to security
 - cyber warfare as 2
 - laws/freedoms suspended because of 243
 - violations of law of neutrality qualifying as 255
 - of use of force, cyber operations constituting 52–3
 - thresholds
 - of control, tests for 32–3
 - of danger for civilians 174, 178
 - of doubt, for presumption of civilian status 114–15
 - of due care 28
 - of harm 56, 107, 113
 - of use of force 45–6
 - of violence
 - for existence of armed conflict 82–3
 - for existence of non-international armed conflict 84–91
 - transit
 - of data, in armed conflict 78
 - States of, and obligations/responsibilities of States 28–9, 36
 - treachery *see* perfidy
 - UN Charter
 - on military actions 50–1
 - on powers of UN Security Council to authorize use of force 69
 - prohibition on intervention in 44
 - cyber operations as violations of 17, 44–5

Cambridge University Press

978-1-107-02443-4 - Tallinn Manual on the International Law Applicable to Cyber Warfare:
Prepared by the International Group of Experts at the Invitation of the NATO Cooperative
Cyber Defence Centre of Excellence

Michael N. Schmitt

Index

[More information](#)

INDEX

281

- prohibition on threat or use of force
 - in 43–4
- on regional systems of collective security 72
- on self-defence rights 54
- on UN Security Council compliance obligations 256
- UN Emblem, prohibition on improper use of 187–8
- UN personnel, installations, materiel, units and vehicles, protection in armed conflict of 188, 210–13
- UN Safety Convention 211
- UN Security Council
 - authorizations for use of force by 69–71
 - compliance with resolutions of, and law of neutrality 255–6
 - mandating/authorizing regional organizations to exercise self-defence rights 71–2
 - on protection of diplomatic premises 233
 - self-defence actions reporting requirement to 68
- uncertainty, about collateral damage 163
- United Kingdom, cyber warfare
 - included in national security strategy of 2
- United States
 - Cyber Command 10
 - cyber warfare policies of 2–3
 - military manuals, Commander's Handbook 8–9, 130–1
- unlawful acts/activities 27, 254–5
- unprivileged belligerency 98, 101
 - by mercenaries 103–4
 - see also* combatant immunity
- urgent countermeasures 37
- use criterion for military objectives 128–9
- verification of targets duty 167–8
- Vienna Convention on Diplomatic Relations, on protection of diplomatic archives 233
- violations
 - of international law
 - interference with sovereign immunity 24
 - involvement of States with non-State actors as 33–4
 - and State responsibility for cyber operations 29–34
 - of law of neutrality, remedies available 254–5
 - of non-intervention principle, cyber operations as 17, 44–5
 - of State sovereignty
 - by cyber operations 16
 - by non-State actors 18
- violence 106–7
 - protracted 88
 - thresholds of
 - for existence of armed conflict 82–3
 - for existence of non-international 88
- virtual armed groups 89–90
 - qualifying as organized armed group 98–9
- virtual confiscation/requisition 247
- wanton destruction 232
- war correspondents 221
- war crimes
 - criminal responsibility of
 - commanders and superiors for 91–4
 - cyber operations qualifying as 92
 - obligations to prosecute 91–2
- war-sustaining activities, targetability of 130–1
- warfare
 - air and missile, manuals on 7, 9
 - see also* cyber warfare
- warnings, duty of issuing of 173–6, 209–10, 230
- warships, carrying neutral or enemy flags 191
- weapons
 - cyber 100, 141–2
 - transmission across neutral territory of 252

Cambridge University Press
978-1-107-02443-4 - Tallinn Manual on the International Law Applicable to Cyber Warfare:
Prepared by the International Group of Experts at the Invitation of the NATO Cooperative
Cyber Defence Centre of Excellence
Michael N. Schmitt
Index
[More information](#)

- weapons (cont.)
 - uncontrollable chains of events
 - created by 145–6
 - obligations of review of 153–6
- Webster, Daniel 63–4
- worship, protection of places of 205
- wrongful acts
 - attribution to States of 29–31
 - and governmental authority 31
 - and non-State actor cyber operations 32–3, 35
 - and organs of State concept 31
 - retroactive 34
 - and causation of damage 30
- countermeasures permissible for States injured by 36–41
- cyber operations qualifying as 29–30
- zones, operational 199–200
 - cyber operations in support of 202