

## INDEX

- Ababil (2012), Operation, 428–431  
*Affaire relative à la concession des phares de l'Empire ottoman*  
 arbitration, 152  
 Agence Nationale de la Sécurité des Systèmes d'Information (France), 116, 251–252  
 anonymous operation against North Korea (2013), 31  
 ANSSI. *See* Agence Nationale de la Sécurité des Systèmes d'Information (France)  
 APT 1, 96–98  
 APT 28, 78–80, 252–253  
 APT 29, 78–80  
*Armed Activities* case, 119, 123, 140–143, 237–238, 279, 464, 479  
 armed conflicts, law of, 5, 14–21, 39–44, 134, 136, 151, 219, 271, 320, 435, 490, 494  
 ARPANET, 33–34  
 artificial intelligence, 157–165  
 Ashkenazi, Gabi, 83  
 attribution, 51–53, 354, 356, 385, 474  
   to a machine, 55–72, 85  
   to a State, 111–188, 304–306  
     acts of non-state actors, 128–157  
     acts of State organs, 114–128  
     State practice, 165–184, 252, 416, 429, 432, 488, 495  
   to an individual, 55, 72–85  
   to an international organisation, 186–188  
 judicialisation of attribution, 182–184  
 attributions (collective and semi-collective) of 4 October 2018, 74, 166, 178–181  
 autonomous cyber operations. *See* artificial intelligence  
 Babar, 81–82  
 BadRabbit (2017), 77, 174, 180, 221, 230–232  
 Bangladesh, Central Bank cybertheft in, 182  
 BlackEnergy 3 malware, 76–77, 176  
 BlackEnergy group, 75, 77, 176  
*Bosnian genocide* case, 119, 123, 129, 140–143, 417  
 Bundesnachrichtendienst (BND)  
   espionage scandal (2008), 212  
 Bundestag (2015), cyber operations against, 66, 79  
 Chosun Expo Joint Venture, 183  
 circumstances precluding wrongfulness, 343–351  
   consent, 101–102, 215, 217, 221, 262, 345–346, 497  
   countermeasures. *See* countermeasures  
   distress, 348  
   *force majeure*, 229, 346–347, 497  
   necessity, 70, 348–350  
   self-defence. *See* *jus contra bellum*  
 Communications Security Establishment Canada, 81  
 composite act, 36–37, 222–241, 249, 253–254, 258

- Corfu Channel* case, 101, 106, 215, 237, 279, 292, 313, 353, 356, 359, 364, 368, 373, 406, 413
- Cosmos 954* case, 212–213, 229, 410
- countermeasures, 5, 14–21, 45, 49, 51, 56, 70, 87, 182, 196, 232, 282, 319, 330, 344, 382, 423–424, 433–460, 490
- armed countermeasures, 349, 442–443, 483–487
- collective countermeasures, 182, 232, 454–460
- urgent countermeasures, 445–448
- Cozy Bear. *See* APT 29
- critical infrastructure, 272, 288, 298–304, 341–342, 350, 396, 407–408, 414
- CrowdStrike, 78–79, 104
- CSEC. *See* Communications Security Establishment Canada
- Cyclades, 34
- damage, 36, 49, 96, 98, 150, 164, 176–177, 213, 215–222, 226–227, 229, 231–232, 247, 259, 268–270, 294–304, 309, 322–324, 331–334, 342, 350, 365, 370, 372, 379, 430, 441–442, 448, 450, 468–472, 475, 478, 481, 491
- DDoS attack, 36, 68, 71, 84, 146–149, 226–228, 241, 290–298, 303, 320–322, 331, 349, 363, 368–369, 385, 391, 404, 411, 426, 429, 439, 441, 446, 453, 489
- Democratic National Committee (DNC), hack of. *See* US presidential elections (2016)
- DOTA, 81
- DoublePulsar, 167–168, 373
- due diligence, 353–375
- distinction between State of transit and State of launch, 362–363, 368–369
- duty to prevent, 358–363
- human rights due diligence, 355–356
- threshold of harm, 363–366
- transboundary harm, 364–365, 369–371
- Duqu malware, 83
- elections, cyber operations against, 254–257. *See* French presidential elections (2017), US presidential elections (2016)
- Elghanian, Habib, 82
- ‘En Marche!’, hack of the French political party. *See* French presidential elections (2017)
- Equation Group, 168
- ESET, 77, 176
- Espionage, 35–36, 65, 96, 102, 193, 197–200, 211–212, 214, 218, 220, 258–260, 264, 267, 270
- Estonia (2007), DDoS attacks against, 46, 68–69, 84–85, 127, 146, 155–156, 227, 241, 259, 303, 305, 307, 309–310, 318, 320–322, 331, 335, 385, 412, 427–428, 456, 474, 495
- EternalBlue, 108, 167–168, 173–174, 373
- EternalBromance, 74, 174
- European Union Cyberdiplomacy Toolbox, 181
- evidence, 87–109
- unlawfully collected, 100–103
- EvilBunny, 82
- Fancy Bear. *See* APT 28
- Federal Security Service (Russian Federation), 66, 78–80, 89–91, 222–250
- FireEye, 77
- Flame malware, 83
- FloodNet, 145, 227
- French presidential elections (2017), 241, 250–254, 259, 495
- FSB. *See* Federal Security Service (Russian Federation)
- Fujitsu, autonomous cyberdefence software developed by, 161, 454
- Gabčíkovo-Nagymaros Project* case, 243, 395, 444, 449
- Galuskevits’ Dmitri* case, 84, 146–147

- GCHQ. *See* Government Communications Headquarters (United Kingdom)
- GCSB. *See* Government Communications Security Bureau (New Zealand)
- GCSC. *See* Global Commission on the Stability of Cyberspace
- Georgia (2008), cyber operations against, 42, 91, 122, 126, 227, 306, 318, 320–322, 346, 385, 411–412, 427–428, 456, 474
- German steel facility (2014), cyber operation causing physical damage to, 302, 407
- Gibson William, 10, 29
- Global Commission on the Stability of Cyberspace, 21–24, 356–357
- Government Communications Headquarters (United Kingdom), 264, 404
- Government Communications Security Bureau (New Zealand), 172, 180
- gravity, threshold of. *See* harm or gravity, threshold of
- Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of the United Nations, 2, 5, 14–21, 25, 27, 160, 165, 206, 357, 490
- GRU. *See* Main Intelligence Agency (Russian Federation)
- Guava, 98–99
- Guccifer 2.0, 79–80, 247
- harm or gravity, threshold of, 215–222, 232, 250, 289–298, 308, 329, 332, 336, 340, 363–366, 368, 371, 449, 483, 485
- human rights, 158, 197, 200, 260–271, 355, 360–361, 377, 406, 448, 451, 495
- ILC. *See* International Law Commission (United Nations)
- injury, 216, 218, 230–231, 268–269, 296, 303, 331–334, 342, 363–366, 370, 379, 436, 442, 449, 497
- International Law Commission (United Nations), 28, 112–113, 124, 139–140, 143–144, 148, 150, 185, 187, 190, 242, 282, 343, 345, 370, 383, 392, 405, 435, 444, 446, 455, 457–458, 462, 478, 485–486
- Articles on ‘Responsibility of States for Internationally Wrongful Acts’, 112–113, 118, 121–141, 143–144, 150–156, 218, 230, 343–350, 381, 383–384, 392, 405–407, 412, 437–460, 478, 485–486
- Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, 369–371
- Draft Articles on the Responsibility of International Organizations, 186–188
- Draft Principles on the Allocation of Loss in the Case of Transboundary Harm Arising out of Hazardous Activities, 369–371
- international organisations’ responsibility for cyber operations, 186–188
- intervention, unlawful. *See* non-intervention
- IP address, 57, 61–69, 79–80, 95, 97, 147
- ITU, 38, 186
- Japanese autonomous cyberdefence software. *See* Fujitsu, autonomous cyberdefence software developed by
- jurisdiction, 85, 100, 102, 111, 205–209, 214, 219–220, 237, 247–248, 261–264, 271, 350, 356
- jus ad bellum*. *See* *jus contra bellum*
- jus contra bellum*, 39–41, 273–342
- aggression, 276, 282, 291, 327–331, 459–460

- jus contra bellum* (cont.)  
 armed attack, 327–342  
 self-defence, 5, 14–21, 45, 49, 56, 196,  
 344, 423–424, 460–487, 490  
 threat of force, 311–327  
 use of force, 273–311  
*jus in bello*. *See* armed conflicts, law of
- Kaspersky, 74, 98, 167  
 KillDisk malware, 77, 176  
 kilo-byte, 82  
 kilo-octet, 82  
 ‘Kwangmyong’, 31
- Lazarus Group, 171, 183
- M.E.Doc software, 175  
 ‘Macron Leaks’. *See* French presidential  
 elections (2017)
- Main Intelligence Agency (Russian  
 Federation), 66, 78, 80, 90,  
 178–179, 181, 245, 247, 252
- Main Intelligence Service (Russian  
 Federation), 78–80, 89–91,  
 222–250
- Malaysia Airlines flight MH17, 91
- Mark I, 34
- Markov, Sergei, 84
- Microsoft, 3, 21–24, 27, 93, 108,  
 167–168, 170, 256, 331, 372,  
 397–398, 420
- Mimikatz, 74, 174
- Myrtus, 82, 99
- National Cyber Security Centre of  
 the GSBC (New Zealand),  
 172
- NATO. *See* North Atlantic Treaty  
 Organization
- NCSC. *See* National Cyber Security  
 Centre of the GSBC (New  
 Zealand)
- Nicaragua case, 18, 52, 118–120,  
 130–134, 136–139, 141–143,  
 149, 195, 233–238, 249, 259,  
 276, 279–281, 313, 326, 328,  
 330, 334, 390, 455, 477, 483
- non-interference. *See* non-intervention  
 non-intervention, 44, 102, 232–260,  
 271–272, 280–281, 286, 377,  
 385, 428, 498
- North Atlantic Treaty Organization, 38,  
 179, 186, 257–258, 324
- NotPetya, 74–75, 77, 173–177, 184, 222,  
 230–232, 370, 372–373, 398,  
 414–416
- Nuclear Weapons* Advisory Opinion,  
 279, 285, 314–315, 325, 328
- Office of Tailored Access Operations  
 of the NSA (United States),  
 167
- Oil Platforms* case, 479, 484, 486
- OPCW (Organisation for the  
 Prohibition of Chemical  
 Weapons), attempted hack  
 against, 178
- Orchard (2007), Operation, 243–244,  
 473–474
- Organization for Security and  
 Cooperation in Europe, 25, 92
- OSCE. *See* Organization for Security  
 and Cooperation in Europe
- ‘Paris Call for Trust and Security in  
 Cyberspace’, 3
- Park Jin Hyok, 182
- PLA Unit 61398. *See* APT 1
- Rainbow Warrior* case, 213, 413
- RBN. *See* Russian Business Network  
 retorsion, 423–433
- RQ-170 Sentinel, 72
- Russian Business Network, 122, 306
- Sandworm group. *See* BlackEnergy  
 group
- SBU. *See* Ukraine, Security Service of
- SCO. *See* Shanghai Cooperation  
 Organization
- Shadow Brokers, 108, 167–168, 174,  
 373
- Shanghai Cooperation Organization,  
 26, 186
- Slammer, 31, 331, 397
- Snowglobe. *See* Babar

- Sony Pictures Entertainment (2014),  
 hack of, 46, 89, 102–103, 166,  
 182, 239–240, 259, 431,  
 488–489, 495
- sovereignty, violation of, 44, 200–232,  
 241, 244, 250, 254, 258–259,  
 271, 346, 348, 351, 365, 370,  
 385–387, 413, 418, 442, 447,  
 450, 454, 470–471, 497–498
- threshold of harm, 215–219
- State responsibility, 381–421
- assurances and guarantees of  
 non-repetition, 388–392
  - obligation of cessation, 382–388
  - obligation of making reparation,  
 392–416
  - compensation, 405–412
  - restitutio in integrum*, 402–405
  - satisfaction, 412–414
  - shared responsibility, 416–420
- Stuxnet, 32, 36, 46, 52, 72, 82–84,  
 98–100, 154–155, 161, 211,  
 222–241, 244, 259, 268, 297,  
 302, 309–310, 322–323, 333,  
 341, 368, 403, 407, 418, 420,  
 428, 470–471, 482, 495
- SuperHard, 81
- surveillance, 261–268, 360–362
- Symantec, 82, 98–99
- Tadić* case, 120, 134–142, 144, 150
- Tallinn Manual*, 44–45, 113–114, 194,  
 198–200, 215–220, 294–296,  
 317, 330, 332–333, 338,  
 348–349, 357–359, 363–368,  
 409, 443–444, 465, 472,  
 485–486
- TAO. *See* Office of Tailored Access  
 Operations of the NSA (United  
 States)
- TeleBots group. *See* BlackEnergy group
- territorial sovereignty. *See* sovereignty,  
 violation of
- Tilde-d platform, 83
- Titi, 81. *See* Babar
- Trail Smelter* case, 364, 370
- TV5 Monde, hack of, 79
- Ugly Gorilla, 81
- Ukraine
- cyber operations against the energy  
 sector, 76–77, 173, 176
  - security service of, 77, 176
- UMBAGE, 75
- UNGGE. *See* Groups of Governmental  
 Experts on Developments in the  
 Field of Information and  
 Telecommunications in the  
 Context of International  
 Security of the United Nations
- unfriendly act, 193–200, 222, 424
- US military's Central Command  
 (2008), hack of its network, 223
- US presidential elections (2016), 66,  
 78–80, 89–91, 166, 180,  
 244–250, 254, 431–432, 488
- vulnerability, 108, 168–170, 174, 323,  
 331, 371–373, 387, 396, 398,  
 419–420, 434
- disclosure, 371–373
- Wall* Advisory Opinion, 279, 337, 387,  
 464
- WannaCry (2017), 73, 166–173,  
 182–183, 221, 230–232,  
 370–373, 398, 420, 431
- WikiLeaks, 75, 89, 247, 251
- Zapatista Army of National Liberation  
 (1997–1998), DoS attacks in  
 support of, 145, 227–228