

# Index

## A

Academia section, 239–240  
Active Cyber Defence, 157  
Advanced analyst (LEA-AA), 147  
Advanced Persistent Threats (APTs), 130, 172  
*A History of Warfare*, 10  
Albanian government, 119, 120  
Alberts, D.S., 176  
Alliance for Cybersecurity, 127  
*Anarchical Society*, 3  
Antolin-Jenkins, V., 89  
ARCO rights (access, rectification, cancellation and objection), 146  
Armed conflict, 13  
Arquilla, J., 160  
Article 49(1) of Additional Protocol I, 102  
Article 52 of Additional Protocol, 107  
Article 52(2) of Additional Protocol I, 111  
Artificial socio-cognitive systems, 144  
Attacks, 100–102  
Attributes of attack, 177–179  
Attribution and transparency, 238  
Australian government, 133  
Automated exploit tools, 221  
AVOIDIT methodology, 173

## B

Bank of England, 200  
Barkham, J., 89  
Barrett, E.T., 7, 77  
Baylon, C., 213–229  
Begby, E., 11  
Bellamy, A.J., 11  
Bishop, M., 173  
Boundary problem

CNE/CNA, 27  
computer network's structure, 26, 27  
consequential harm, 27  
hacking back, 26  
hostile system, 26  
legitimate target, 25  
malicious software, 26  
military commanders, 27  
preparatory exploitation, 26  
self-propagating software, 26  
Bradbury, S.G., 89  
Brenner, S., 89  
Brown, D., 95  
Bundesamt für Sicherheit in der Informationstechnik (BSI) standards, 127, 130, 133  
Budapest Convention, 117, 118  
Bull, H., 3  
Burdon, M., 153

## C

Cabinet Office, 197  
Cameron, K., 148  
CAPER, 146–152, 154, 156  
CAPER crawling system, 148  
CAPER regulatory model (CRM), 142, 149, 152–162  
Card, S., 176  
Casanovas, P., 139–162  
Cath, C.N.J., 231–241  
Caveats, 123–124  
Cavoukian, A., 148  
Centre for Protection of National Infrastructure (CPNI), 174, 197, 199, 202

- China, 128–130
- China General Nuclear Power Corporation (CGN), 226
- China Internet Network Information Centre (CNNIC), 109
- Chinese deal, 226
- CIA, 142
- Civilians
  - attacks, 37–38
  - cybercriminals, 40
  - cyberspace, 35
  - desirable targets, 36
  - dual-use resources, 36
  - dual-use targets, 37
  - easy targets, 35–36
  - ethical justification, 37
  - hardware, 35
  - intermediate steps, 38–39
  - military activities, 35
  - military operations, 35
  - side effects, 37, 39–40
  - spoofing, 41–42
  - unreliability of cyberwarfare, 39
- Clarke, R., 218
- Classical antiquity, 11
- Classical legal theory, 154
- Coates, A.J., 8
- Cohen, F., 173
- Collateral damage, 43
- Collier, J., 187–211
- Committee on the Protection of Critical Infrastructure, 194
- Common Law, 141
- Companies selling vulnerabilities
  - cyber attacks, 219
  - industrial control systems, 219
  - penetration testing tool, 219
  - SCADA zero-days, 219
  - security, 220
  - TechTarget, 220
  - vendors, 220
  - zero days, 219
- Computer network attacks (CNA)
  - bricking, 23
  - CNE, 23
  - cyber Pearl Harbors, 23
  - international humanitarian law, 23
  - national jurisdictions, 24
  - physical damage, 24
  - violent attacks, 23
- Computer network exploitation (CNE)
  - and CNA, 23, 28
  - electronic attacks, 23
  - illegitimate access, 25
  - interpretation/distinction, 25
  - legitimate target, 26
  - non-human agency, 20
  - software tools, 20
  - system malfunctioning, 27
  - targeted network, 20
- Cooperative Cyber Defence Centre of Excellence (CCDCOE), 91
- Corfu Channel, 119–121, 123
- Corfu Channel* case, 116
- Cornish, P., 1–16
- Corporate Insider Threat Detection (CITD), 175
- Council of European Convention on Cybercrime, 117
- Critical infrastructure (CI), 126–130
- Customary International Cybersecurity Law, 117–118, 121, 124, 133
- Customary International Humanitarian Law, 106
- Cyber attacks, 122, 132, 133, 142, 156, 157, 161, 170–172, 177–183, 189, 191, 192, 196–198, 200–203, 205, 210
  - attack methods, 34
  - Australian sewage, 38
  - automated exploit tools, 221
  - automatic propagation, 40–41
  - catastrophic destruction, 29
  - computer networks, 22
  - computer system, 19
  - core model
    - attributes of attack, 177–179
    - impact, 180
    - mitigation, 180–181
    - values, 179
  - cybercrime, 35
  - cyber-operations, 63
  - DDoS's attempt, 64
  - definition, 20, 170
  - ethics, 30
  - human interests, 64
  - intentional disruption, 19
  - international armed conflicts, 21
  - international humanitarian law, 20
  - LOGIC BOMB, 64
  - mail system, 37
  - Metasploit Framework, 221
  - military target, 35
  - physical harm and damage, 19
  - physical operation, 22
  - political conflict, 30
  - public policy requirements, 64
  - reformations, 23
  - related work, 172–175

- search engines, 221, 222
- sequential manner, 24
- service attacks, 19, 64
- side effects, 37
- Stuxnet, 34
- Tallinn Manual, 19
- technical restrictions, 222
- violence, 28
- vulnerabilities, 36
- Cyber coercion, 46
- Cyber commands, 227, 228
- Cyber conflict
  - aggression, 6
  - attribution problem, 7
  - conflict-focused ethical constraints, 5
  - and coercion, 6
  - double effect principle, 6
  - ethical debate, 2
  - ethical governance, 8
  - ethically-guided judgement, 3
  - international humanitarian law, 2
  - political leaders, 7
  - pre-emption debate, 8
  - public debate, 2
  - relationship, 3
  - sensational attacks, 2
  - technological challenges, 6
- Cybercrimes, 145, 160, 161
- Cybercriminals, 39, 216
- Cyber crisis management, 188–192, 194, 196–201
  - comparison between Estonia and United Kingdom, 201–203
  - explanatory variables
    - digital dependence, 206–207
    - history, 205
    - political philosophy, 206
    - size, 203–204
    - threat landscape, 205–206
  - lessons, strategy and policy, 207–209
- Cyber defence, 173, 174, 181, 182
- Cyber Defence League (CDL), 193–195, 202
- Cyberharm
  - ability and opportunity, 56
  - bilateral and dynamic, 56
  - computer-information systems, 51
  - cyberattacks, 55, 57
  - cyber-ethics, 49
  - cyberwarfare, 50
  - economic damage, 50
  - economic injury, 55
  - economic loss/physical injury, 54
  - environmental and informational systems, 54
  - hacker's experimentations, 54
  - human agents, 53
  - human interests, 50, 55–57
  - human values, 57
  - information systems, 52
  - initial plausibility, 52
  - instrumental view, 50, 51, 54
  - intentional disruption, 51
  - interests and entitlements, 54
  - intrinsic view, 53, 54
  - legal entitlements, 55
  - legitimate moral entitlements, 50
  - manumission, 51
  - mediators, 56
  - metaethical and metaphysical theses, 54
  - moralized conception, 50
  - non-living systems, 52
  - non-sentient entities, 53
  - ontological commonalities, 52
  - psychological consequences, 52
  - psychological discomfort, 55
  - public elements, 55
  - public honor, 53
  - sentient animals, 52
  - social equilibrium, 52
  - theoretical judgments, 56
- Cyber operations
  - active defense, 92
  - amendment, 96
  - armed attack, 92
  - biases and blindspots, 97
  - categories, 89
  - civilian and military targets, 94
  - cyberspace, 94
  - cyber-specific arrangement, 95
  - cyber weapons, 94
  - human experience, 97
  - human rights, 88
  - international law, 88, 89, 96
  - international legal rules, 94
  - international legal system, 95
  - international peace and security, 90
  - international regulation, 97
  - international relations, 90
  - international rules and structures, 90
  - jus in bello*, 93, 94
  - law-making role, 89
  - military objective, 93
  - proportionality, 93
  - revision and amendment, 98
  - revolution, 88
  - self-defense, 92
  - software corporations, 95
  - stakeholders and resistance, 89

- Cyber operations (*cont.*)  
 Tallinn Manual, 91  
 technological advancement, 88  
 technology corporations, 89  
 vulnerabilities, 92  
 warfare, 93  
 weapons and capabilities, 97
- Cyber-security, 116–133, 159, 172,  
 174–176, 181–183, 188,  
 190–203, 205–210, 225–228
- Cyber-security due diligence  
 nation regulations  
 China, 128–130  
 Germany, 127–128  
 United States, 125–126  
 polycentric approach, 132
- Cyber Security Information Sharing  
 Partnership (CISP), 198
- Cyber-security policy, 181
- Cyber security strategy, 196
- Cyber situational awareness and understanding  
 models, 174, 175
- Cyberspace, 152, 157, 158, 160, 170, 172,  
 174–177, 180, 187–189, 210  
 communication and information transfer, 5  
 cyber debate, 15  
 human invention, 4  
 innovation and progressive  
 development, 88  
 moral framework, 4  
 nuclear proliferation, 14  
 nuclear threat, 15  
 partitioning, 45  
 political organisation, 5  
 reverse-engineering, 15  
 technologically skilled, 4  
 vulnerabilities, 4
- Cybersphere, 233
- Cyber warfare, 142, 156–162  
 Article 52, 34  
 collateral damage, 34  
 confidential information, 226  
 cyberattack, 60  
 cyberspace, 34  
 definition, 232  
 deflationary feature, 61  
 human interest, 61  
 information systems, 60  
 international community, 232  
 international legal norms, 232  
 military and civilian targets, 34  
 participants, 227  
 principles, 44  
 Stuxnet, 34  
 technical issues, 231  
 universal principles, 233
- Cyber weapon, 7, 214  
 during peacetime, 218  
 ethical problems with Stuxnet, 215–217  
 Stuxnet, 215
- D**
- Danks, D., 2
- Danks, J.H., 2
- Data, 151  
 collection and storage, 151  
 reuse and transfer, 151
- Decision-making process, 171, 172, 177, 183
- Definite military advantage, 107, 108
- de Maizière, T., 127
- Democratic Control of Armed Forces (DCAF),  
 158
- Department of Health, 196
- Department of Transport, 196
- Deterrence, 233, 236, 237
- Digital by Default, 195
- Digital dependence, 206, 207
- Digital systems, 188–190, 200, 206, 207, 210
- Dinstein, Y., 89
- Dipert, R., 2, 49, 73
- Dipert, R.R., 2
- Distinction  
 cyberspace, 35  
 ethical problems, 46  
 military and civilian, 34
- Distributed denial of service (DDoS), 102,  
 191, 192
- Domain Name System (DNS), 108
- Domestic institutional organisation, 191–192
- Donohue, L., 159
- Dual-use  
 civilian entities, 37  
 civilians and militaries, 36  
 command-and-control, 37  
 government's actions, 37  
 military and civilian users, 45  
 military parts, 37
- Duffield, M., 7
- E**
- Eberle, C.J., 5
- Electricite de France (EDF), 226
- Electronic attacks  
 CNE, 20  
 computer networks, 20, 30  
 computer system's function, 19

- Electronic attacks (*cont.*)  
 criminal act, 24  
 cyber attacks, 20  
 damage/destruction to objects, 19  
 hostile act, 25  
 hostile exploitation, 30  
 human decision making, 20  
 humanitarian law, 21  
 industrial systems, 24  
 international lawyers, 18  
 internet and global communications networks, 19  
 IP address, 24  
 just war tradition, 21  
 kinetic/physical effect, 19  
 law  
   armed conflict, 18  
   and ethics, 18  
   and morality, 18  
 legal judgement, 18  
 military and non-military targets, 24  
 moral and legal judgement, 18  
 physical action, 24  
 physical infrastructure, 30  
 political conflict, 30  
 positive identification, 24  
 remote computer networks, 25  
 service attacks, 19  
 system's characteristics, 20  
 technical issues, 30  
 transgressor, 19  
 virtuous consequentialism, 29  
 Emergency Act, 191  
 Entropy  
   environment, 83  
   infosphere, 79  
   moral evil, 82  
   occurrence, 80  
 e-residency, 206  
 Eritrea-Ethiopia Claims Commission (EECC), 111  
 e-services, 192  
 Estonia, 127, 188, 189, 204–211  
   domestic institutional organisation, 191–192  
   international engagement, 194–195, 203  
   stakeholder mobilisation, 192–194  
   vs. United Kingdom, 201–203  
 Estonian Computer Emergency Response Team (CERT-EE), 192, 193, 195  
 Estonian Cyber Defence League, 208  
 EU Data Protection Rules, 140  
 European Conferences on Data Protection, 159  
 European LEAs Interoperability (ELIO), 148  
 European Union (EU), 195  
 European Union Agency for Network and Information Security (ENISA), 214  
 Europol, 161  
 Exodus Intelligence, 220
- F**  
 Fairclough, G., 169–183  
 Federal Office for Information Security, 127  
 Fisher, D., 2, 29  
 Floridi, L., 80  
 Flowers, A., 157  
 Foreign and Commonwealth Office, 200
- G**  
 G2 cybersecurity code, 128  
 General Agreement on Tariffs and Trade (GATT), 124  
 General Data Protection Reform package (GDPR), 140, 141, 146, 151, 159  
 General prosecution of the war, 106  
 Generic analyst (GA), 147  
 Geneva Additional Protocol I, 237  
 Germany, 127–128, 130  
 Gifford, D.J., 88  
 Glassman, M., 144  
 Global Positioning System (GPS), 37  
 Glorioso, L., 231–241  
 Golden Rule, 9  
 Gottschalck, P., 158  
 Governmental Group of Experts (GGE), 218  
 Greitzer, F.L., 174
- H**  
 Hacking-for-hire companies, 217  
 Hague Rules on Air Warfare, 103  
 Happa, J., 169–183  
 Healey, J., 170  
 Heating, ventilation and air conditioning (HVAC), 131  
 Her Majesty's Revenue and Customs (HMRC), 197  
 Highwayman, 62  
 Hoepman, J.H., 148, 149  
 Holistic Management of Employee Risk (HoMER), 174  
*Homo sapiens*, 10  
**Hoisington, M.**, 87–98  
 Howard, J.D., 173

Human agency  
 complexity/disaggregation, 27  
 computer networks, 27, 28  
 cyber attacks, 28  
 cyber security, 29  
 dumb software, 29  
 knowledge and moral requirements, 27  
 malicious code, 28  
 moral requirement, 28  
 network exploitation, 27  
 non-human agents, 28  
 responsibility, 28  
 violation, 29

Human intelligence (HUMINT), 143

Hutton, R., 176

Hybrid model, 151

## I

Imagery intelligence (IMINT), 143

Impact of Attack, 180

Information and communication technologies (ICTs), 4, 213  
 enemy's informational infrastructure, 67  
 ethical conundrums, 68  
 proposed analysis, 68  
 revolution, 67  
 theoretical vacuum, 68

Information Ethics, 78–80

Information revolution, 240

Information-security community, 40

Information warfare (IW)  
 artificial agents, 81  
 civil society and military organisations, 76  
 civilian informational infrastructure, 77  
 combatants vs. non-combatants, 76  
 computer virus, 71  
 conceptual investigation, 68  
 context, 76  
 declaring and waging, 72  
 dgression, 70  
 equilibrium, 76  
 ethical analysis, 68  
 ethical guidelines, 68, 75  
 ethical regulations, 68  
 Information Ethics, 81  
 kinetic warfare, 77  
 laws and regulation, 77  
 moral accountability, 81  
 moral agents, 80  
 morality of artificial agents, 80  
 non-violent cases, 75  
 ontological hiatus, 74, 82  
 police forces, 82

principles, 68, 81–83  
 qualifiable effects, 80  
 spectrum definition, 69  
 transversality, 72  
 unethical actions, 76  
 universal goods, 75

Infosphere, 81

Institutional strengthening, 154, 155

Institutional-Semantic Web Regulatory Model (i-SWRM), 149, 155, 156

Intermediate institutional models, 149

Intermediate institutions, 154

International Atomic Energy Agency (IAEA), 214

International Committee of the Red Cross (ICRC), 11, 100

International Court of Justice (ICJ), 99, 116–124  
 caveats, 123–124  
 Corfu Channel, 119–121  
 cybersecurity due diligence, 122–123  
 Nicaragua, 121–122  
 Trail Smelter, 121

International Criminal Tribunal for the former Yugoslavia (ICTY), 100

International engagement  
 Estonia, 194–195, 203  
 United Kingdom, 200–201

International humanitarian law (IHL), 5, 102, 238

International law, 117

Internet  
 communication network, 109  
 cyber operations, 109, 111  
 economic targets, 111  
 ICTY Final Report, 109  
 international criminal law, 110  
 military action, 110  
 military manuals, 109  
 military objective, 111  
 NATO aircraft, 109  
 neutralization, 110  
 resilience, 110

Internet-connected industrial control systems, 221, 222

Iranian Revolutionary Guards, 220

Islamic State in Iraq and Syria (ISIS), 217

IT Security Act, 128

## J

Jaouën, F., 158

Jenkins, R., 2, 58

- Jensen, E.T., 106  
 Jinping, Xi., 129  
 Joint Cyber Unit (JCU), 200  
 Judaeo-Christian just war, 5  
*jus ad bellum*  
   armed conflict, 89  
   armed hostilities, 95  
   cyber operations, 90  
   epochal shift, 96  
   and *jus in bello*, 90  
   power dynamics, 94  
*jus in bello*  
   armed conflict, 89, 93  
   hostilities, 93  
 Just war theory (JWT), 233  
   attacked computer system, 74  
   categorization, 21  
   CNE, 23  
   combatants and non-combatants, 9  
   communications networks, 10  
   computer systems, 22  
   cruising computer virus, 73  
   cyber attacks, 22  
   cyber conflict, 9  
   domain, 77  
   ethical analysis, 73  
   ethical discussion, 21  
   ethical no-go zone, 10  
   existing apparatus of laws, 77  
   hostile action, 22  
   human behaviour, 9  
   human life and liberty, 9  
   intelligence collection, 22  
   international contexts, 73  
   jurisprudence and practice, 9  
   *jus in bello*, 72  
   knowledge formation, 22  
   knowledge generation, 23  
   legitimate targets, 21  
   military activity, 22  
   moral analysis, 73  
   moral discourse, 74  
   ontological hiatus, 74  
   ontology, 73  
   pacifism/realism, 72  
   personal and political  
     responsibility, 21  
   sanguinary war, 75  
   storage devices, 22  
   surveillance, 22  
   targeted killings, 22  
   tense relations, 75  
   universal nature, 77  
   war as last resort, 74
- K**  
 Kang, M.J., 144  
 Keegan, J., 10  
 Kennedy, D., 90  
 Kerry, J., 195  
 Killchain, C., 173  
 Kilovaty, I., 157  
 Kirgis, F.L., 118  
 Knopf, J.W., 14  
 Koops, B.-J., 148, 149  
 Kornmaier, A., 158  
 Kuehn, A., 115–133
- L**  
 Lauristin, M., 141  
 Law of armed conflict, 11, 99, 100  
 Law section, 235, 236  
 Leahy, S.P., 88  
 LEA's External User (LEU), 147  
 Leenes, P., 148  
 Legal Enforcement Agents (LEAs), 140,  
   144–149, 151, 152, 156, 160  
 Legg, P., 175  
 Lessig, L., 153  
*lex feranda*, 123  
 Lin, H., 89  
 Lin, P., 159  
 Lough, D.L., 173
- M**  
*Mahabharata*, 11  
 Margaret Thatcher, 206  
 McDonald, J., 17–30  
 Measurement and signatures intelligence  
   (MASINT), 143  
 Mental models, 170, 171, 175, 176, 178, 182  
 Meta-rule of law, 142, 144–146, 152–154,  
   156, 158, 160–162  
 Metasploit Framework, 221  
 Microsoft, 133  
 Military objectives  
   Article 52(2) of Additional Protocol I, 104  
   carbon filaments, 102  
   circumstances, 104  
   cloud computing, 106  
   cyber attacks, 104  
   cyber context, 104  
   cyber operations, 102, 103  
   dual-use cyber infrastructure, 106  
   Geneva Conventions, 103  
   internet, 109  
   military manuals, 103

- Military objectives (*cont.*)  
 partial destruction, 103  
 pro-Russian propaganda, 102  
 Protocol I, 101, 106  
 software components, 109  
 transmission of orders, 105  
 transportation-related networks, 107  
 uranium enrichment, 104  
 US definition, 106  
 US government communications, 105
- Ministry of Defence (MoD), 197
- Mirror model, 173
- Mirroring effect, 181
- Mission integration framework, 174
- Mitigation of Attack, 180–181
- Mobile technology, 144
- Moral reflection, 11, 13
- Moral vocabulary, 12
- Morality and war, 29
- Multi-level protection scheme (MLPS), 129
- Multi-lingual Crime Ontology (MCO), 148
- Murkens, J.E.M., 152
- N**
- National Cyber Security and Communications Center, 195
- National Defence Authorization Act, 143
- National grid, 199
- National Institute of Standards and Technology (NIST) Framework, 116, 118, 125–128, 130–133
- National Security Agency (NSA), 220
- NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE), 190, 191, 201  
 cyber attacks, 233  
 cyber warfare, 232  
 cyber weapon, 232  
 cyberspace, 232, 233  
 ethical principles, 232  
 legal mechanisms, 232  
 Oxford, 231  
 perfidy, 233  
 policy-makers, 232  
 stakeholders, 233
- NATO cyber security framework manual, 174
- Networks  
 command-and-control, 37  
 cyberattack, 35  
 military operations, 35  
 protocols, 41  
 web browsers, 35
- Nicaragua, 117, 121–122
- Nicaragua v. United States*, 117
- Non-tangible terms, 180, 183
- Nordic-Baltic, 195, 205, 207
- Norman, D.A., 170
- Normative-SWRM, 155, 156
- North American Treaty Organization (NATO), 11, 91, 143, 188, 190, 195, 201, 203–205, 208
- Nuclear facilities  
 commercial off-the-shelf systems, 223  
 cyber security, 224  
 foreign components, 224  
 IAEA, 223  
 public internet, 223
- Nuclear security, 214
- Nussbaum, M., 56
- O**
- Obama, B., 125, 126, 128
- Oceanian flagship, 64
- O'Connor, T.R., 145
- One-size-fits-all policy, 209
- Ontological design patterns (ODP), 155
- Open social intelligence (OSI), 145
- Open source (OS), 140
- Open Source Intelligence (OSINT), 139, 140, 142–146, 148, 149, 152–157, 161
- Open Social Intelligence (OSI), 140, 143–145
- Opinio juris*, 118
- Organization of American States, 118
- OSINT cybercrime crawling, 161
- Ostrom, E., 132, 152, 156
- Ostrom, V., 132
- P**
- Paet, U., 195
- Palombella, G., 152
- Perfidy, 41, 237
- Pirolli, P., 176
- Political philosophy, 206
- Political section, 233–235
- Politics  
 armed conflict, 12  
 cyberspace, 3  
 ethical project, 13  
 moral consciousness, 12  
 moral language, 13  
 strategy and ethics, 3  
 technological challenges, 12  
 and war, 13



- Prikk, K., 192  
 Primary privacy law, 159  
 Principles of Fair Information Practices (FIPs), 148  
 Privacy by Default (PbD), 140  
 Privacy by Design (PbD), 140, 142, 147–152, 159  
 Privacy Impact Assessment (PIA), 147, 149, 151, 152  
 Product tampering, 42  
 Propagation  
   cyberattacks, 40–41  
   worm-based, 34  
 Psychological damage, 42  
 Pudong New Area of Shanghai, 105  
 Pythian, M., 142
- R**
- Radio Television of Serbia (RTS), 109  
 RAND paper, 160  
 Regulations on Classified Protection of Information Security, 129  
 Reichberg, G.M., 11  
 Reparations, 45  
 ReVuln customers, 219  
 Rid, T., 23  
 Right of data access, 151  
 Rights Expression Languages (REL), 155  
 Ritsch, M., 152  
 Roig, A., 149  
 Ronfeldt, D., 160  
 Roscini, M., 99–111  
 Rosenzweig, P., 89  
 Rowe, N.C., 33–46  
 Russell, S., 115–133  
 Russia, 207, 208
- S**
- Sanders, J.W., 80  
 SCADA systems, 24  
 Schmitt, M., 89  
 Schmitt, M.N., 157  
 Schneier, B., 23  
 Schreier, F., 158  
 Secondary privacy law, 159, 160  
 Self-defense, 91  
   Amy Pascal's privacy, 58  
   annexation, 59  
   beneficial features, 58  
   cyberattacks, 57, 58, 60  
   cyberharm, 57  
   damaging effects, 59  
   eastasian occupation, 59  
   instrumentalist view, 58  
   interpersonal relationships, 58  
   invasion, 58  
   rare earth minerals, 60  
   state action, 59  
   Stuxnet, 58  
   target nation, 59  
   temporal proximity, 60  
 Self-determination  
   computer programs, 61  
   cyberharm, 60  
   cyberwarfare, 62  
   epistemic factor, 62  
   goals, 62  
   highwayman, 62  
   human interests, 61, 63  
   individual's entitlement, 61  
   interests and entitlements, 61  
   magnitude, 62  
   military action, 60–61, 63  
   political action, 62  
   resistance, 63  
   self-defense, 62  
 Semantic Web Regulatory Models (SWRM), 155  
 Sensemaking model, 175, 176, 181  
 Shackelford, S.J., 115–133  
 Shanghai Cooperation Organization, 128  
 Shaw, M.N., 8  
 Signals intelligence (SIGINT), 143  
 Smith, P.T., 49–64  
 Social and people-centric models, 174  
 Social engineering, 174  
 Social intelligence, 144  
 Social media, 146  
 Steinhauer, J., 88  
 Strachan, H., 13  
 Strategic intelligence, 145  
 Stuxnet, 28, 101, 122  
   collateral damage, 216  
   cyber arms race, 216  
   cyber domain, 216  
   cyber weapon, 213  
   high-profile cyber weapon, 217  
   Iranian nuclear facilities, 215  
   nuclear weapons, 215  
   sovereign state, 215  
 Supervisory Control and Data Acquisition (SCADA) systems, 105, 157, 179, 218  
 Swarming, 161  
 Syse, H., 11

**T**

Taddeo, M., 10, 67–84, 231–241  
 Tallinn Manual, 116, 118  
 Tallinn Manual on International Law applied  
 to Cyber Warfare, 157  
 Tallinn Manual on the International Law  
 Applicable to Cyber Warfare, 101  
 Tangible terms, 179, 180, 183  
 Technology-centric models, 173  
 Tene, O., 159  
 Terrorists, 217  
 Total Defence model, 202, 204  
 Trachtman, J., 88  
 Trail Smelter, 121, 123  
 Transnational rule of law, 152  
 Tranter, K., 88

**U**

UN General Assembly, 6  
 UN General Assembly Resolution, 118  
 UN Security Council, 6  
 United Kingdom (UK), 188–190, 195–211  
 COBRA, 196  
 Cyber Security Strategy, 196  
 domestic institutional organisation,  
 196–198  
 DSTL, 174  
 vs. Estonia, 201–203  
 GCHQ, 196, 197, 199  
 international engagement, 200–201  
 JCU, 208  
 stakeholder mobilisation, 198–200  
 United Kingdom Computer Emergency  
 Response Team (CERT-UK),  
 197, 198, 201, 202, 208  
 United Nations (UN), 195  
 United Nations Group of Governmental  
 Experts (UNGGE), 232, 235  
 United States (U.S.), 117, 121, 125–126, 128,  
 130, 195, 204  
 USAF Intelligence Targeting Guide, 111

US Air Force Pamphlet, 107  
 U.S. Computer Emergency Readiness  
 Team (US-CERT), 195  
 US CYBERCOM former, 107  
 US Department for Homeland  
 Security, 217  
 US National Security Agency (NSA), 228  
 Usmani, Z-ul-H., 145

**V**

Validation exposure randomness de-allocation  
 improper conditions taxonomy  
 (VERDICT), 173  
 Values of Attack, 179  
 Vendors, 224  
 Visual analytics module (VA), 148  
 von Clausewitz, C., 13  
 Vulnerabilities, 222

**W**

Walzer, M., 10  
 Waxman, M., 89  
 Web 2.0, 142, 153  
 Weick, K.E., 181  
 Weinstein, J., 131  
 Westin, A., 148  
 Whole of nation approach, 192  
 Windsor, P., 13  
 Wireless network standard (WAPI), 129  
 World Trade Organization (WTO), 124

**X**

Xiao, L., 176, 177  
 X-road, 191

**Z**

Zeadally, S., 157  
 Zittrain, J.L., 153