

# Index

- Abbott, Andrew, 14
- Abraham, Kavi Joseph, 16
- accountability theories and mechanisms  
for Advanced Persistent Threat Groups,  
241–242
- for cyber peace, 220
- Acquaviva, Guido, 134–135
- Advanced Persistent Threat Groups (APTs)  
critical infrastructure attacks, 238
- Stuxnet attack, 95, 132, 238
- cyber hybrid warfare by, 240–242
- accountability mechanisms for, 241–242
- effective control strategies, 241
- as grey-zone tactic, 240
- under international law, 241
- state responsibilities in, role of, 241–242
- Cyber Tech Accord and, 242
- electoral processes manipulation, 239
- by Russia, 239
- in U.S., 239
- espionage by, 237–238
- ICT4Peace, 236, 242
- information system attacks, 239
- ransomware attacks, 121, 239–240
- WannaCry cyber attack, 227, 239–240
- theoretical approach to, 236–237
- in U.S.  
electoral processes in, manipulation of, 239
- Solarwinds attack, 237
- adversarial artificial intelligence, 122
- aggression. *See* cyber aggression
- AGI. *See* artificial general intelligence
- AI. *See* artificial intelligence
- Alker, Hayward, 5
- Alliance for Peacebuilding, 98
- ambiguous signals, in cyber off-ramps, 67
- Ankersen, Christopher, 195–204
- APTs. *See* Advanced Persistent Threat Groups
- Arab Spring, 94
- Argentina, feminist movements in, 94
- ARPANET, 31
- artificial general intelligence (AGI), 117
- artificial intelligence advanced towards, 124
- cybersingularity and, implications  
for, 123–124
- defensive capabilities of, 123
- definition of, 123
- development of, 123
- offensive capabilities of, 123
- artificial intelligence (AI)
- adversarial, 122
- artificial general intelligence and, 124
- background of, 118–123
- cyber attack methods, 121
- definition of, 118
- global service corps, shared governance of,  
124–125
- information anonymity and, 118–119
- in information attacks, 118–119
- information attribution and, 118–119
- information security measures and, 119–123
- defensive, 120
- as deterrence, 120
- linkages to artificial intelligence, 121–123
- offensive, 120–121
- as proactive, 120
- theoretical approach to, 117–118
- ASIAS System. *See* Aviation Safety Information  
Analysis and Sharing System
- ASRS. *See* Aviation Safety Reporting System
- aviation model, for cyber peace, 156–157
- under Convention on International Civil  
Aviation, 156
- under International Civil Aviation  
Organization, 156
- threat intelligence in, 157

- Aviation Safety Information Analysis and Sharing (ASIAS) System, 163–164
- Aviation Safety Reporting System (ASRS), 163–165
- Federal Aviation Administration, 165
  - National Aeronautics and Space Administration and, 165
- Barlow, John Perry, 39
- Black Lives Matter movement, 94
- Bolton, John, 84
- botnets, 121
- boundaries, of cyber peace, 14–17
- with cyber aggression and, 14–15
    - defend forward approach to, 15
    - in Estonia, 14–15
  - with cyber crime, 15–16
  - with cyber lawlessness, 15–16
  - in multistakeholder collaborations, 16–17
    - under polycentric governance, 16
    - under polycentric governance, 16–17
    - multistakeholder forms of, 16
- Cavelty, Myriam Dunn, 12
- CBMs. *See* confidence-building measures
- CDL. *See* Defence League Cyber Unit
- Chesney, Bobby, 85
- China
- Communist Party of China, 22
  - cyber attacks by
    - Mustang Panda, 225–226
    - against U.S. Office of Personnel Management, 224
  - detention of Muslims in, 22
  - digital repression in, 26
    - tactical expertise in, 28–29
    - threat identification in, 25–28
- CISCP. *See* Cyber Information Sharing and Collaboration Program
- civil liberties, digital repression and, 26
- civilians, information sharing with military, 45–46
- climate change policies. *See also* Paris Call for Trust and Security
- Paris Climate Accord, xx
- Clinton, Hillary, 225
- coercive habituation, digital repression and, 28
- coercive potential, in wargames, 80
- Colombia
- cyber peacebuilding processes in, 99–100
    - digital spoilers in, 105
    - in Inter-American Human Rights System, 100
  - Internet access in, 107–108
  - multistakeholder governance in, 103–104
  - policy implications for, 108–110
  - promotion of human rights, 99–101
  - stability in, 104
- Digital Security policy in, 107
- Comey, James, 135
- Communist Party of China, 22
- Comoros case, ICC, 139
- Computers at Risk* (National Research Council), 160
- confidence-building measures (CBMs)
- advantages of, 55
  - definition of, 55
  - through information sharing, 54–56
  - non-military, 54
  - origins of, 54
- Convention on International Civil Aviation, 156
- Council of Advisers on the Application of the Rome Statute to Cyberwarfare, 135–136
- Covid-19 pandemic
- cyberspace access during, 217
  - “infodemic” as result of, 217–218
- Craig, Amanda, 10
- crime. *See* cyber crime
- crimes against humanity, 136
- crimes of aggression, cyber attacks as, 145–147
- crises escalation, in cyber war, 66
- conflict processes, 66
  - cyber operations and, 69–70
  - over territorial disputes, 66
- critical infrastructure attacks, by ATPs, 238
- Stuxnet attack, 95, 132, 238
- crowdsourcing
- for cyber peace, as theoretical concept, 230
- CyberPeace Corps, 232
- research by, 233–234
  - societal value of, 234
- for cybersecurity, 231–235
- through bounty programs, 233
  - calls to action, 234–235
  - through collaboration, 233
- CyberPeace Corps, 232
- Defence League Cyber Unit, 231
- in Estonia, 231
  - through intelligence sharing, 233
  - as theoretical concept, 230
  - volunteer journey, phases of, 234
- definitions and scope of, 230–231
- CSRS. *See* Cyber Security Reporting System
- cyber, 11–12
- martial quality of, 13
  - military applications, 12, 13
  - peace as element of, 12–14
  - cyber 9/11, 132–133, 143–144

- cyber aggression, cyber peace and, 14–15  
 defend forward approach to, 15  
 in Estonia, 14–15
- cyber attacks, 132–133. *See also* International Criminal Court  
 with artificial intelligence, 121  
 by China  
 Mustang Panda, 225–226  
 against U.S. Office of Personnel Management, 224  
 as crime of aggression, 145–147  
 cyber 9/11 scenario, 132–133, 143–144  
 for data-theft, 132  
 deterrence measures against, 133–137  
 Domain Name System as resource, 225–226  
 Domain-based Message Authentication, Reporting, and Conformance resource, 225–226  
 for election manipulation, 132, 144, 147  
 against essential services, 218–219  
 extortion and, 132  
 as genocide, 144–145  
 of information technology systems, 132  
 under international human rights law, 133–134  
 under international humanitarian law, 133–134  
 multi-factor authentication against, 226  
 phishing, 224  
 scope of, 132  
 Stuxnet attack, 95, 132, 238  
 for theft of state secrets, 132  
 in Ukraine, on power grid, 95, 158  
 NotPetya attacks, 132, 158, 227–228  
 under UN Charter, 133–134  
 in U.S.  
 against Democratic National Committee, 225  
 against Office of Personnel Management, 224  
 prosecution of, 135  
 WannaCry, 227, 239–240  
 as war crimes, 141–143
- cyber conflict, 12
- cyber crime, 15–16, 54
- cyber hybrid warfare, by APTs, 241–242  
 accountability mechanisms for, 241–242  
 effective control strategies, 241  
 as grey-zone tactic, 240  
 under international law, 241  
 state responsibilities in, role of, 241–242
- cyber hygiene. *See also* cyber attacks; cybersecurity  
 Global Cyber Alliance and, 223–224  
 Cyber Information Sharing and Collaboration Program (CISCP), 46–47  
 cyber threat information in, 47  
 as non-polycentric, 57  
 real-time information in, 47  
 scope of platform, 46–47  
 STIX language, 50, 53  
 TAXII language, 50, 53  
 Traffic Light Protocol, 51, 53
- cyber lawlessness, 15–16
- cyber off-ramps, 67–70, 87–88  
 ambiguous signals in, 67  
 in de-escalation strategies, 65–66  
 elasticity of demand, 68, 69  
 information costs of, 69  
 public response to, 67  
 substitutability dynamics, 67–69
- cyber peace. *See also* boundaries; cyber war; cybersecurity; digital peace; peacebuilding processes; *specific topics*  
 accountability theories for, 220  
 as concept, 11–14  
 linguistic elements in, 11–14  
 conditions of, 5–6  
 goals and purposes in, 5  
 practices and, 9–10  
 crowdsourcing for, as theoretical concept, 230  
 definitions of, xx–xxi, xxiii–xxiv, 4–5, 39, 213–215  
 information and communication technologies and, 7–8  
 ontology and, 4  
 Erice Declaration on Principle for Cyber Stability and Cyber Peace, xxi  
 information and communication technologies and, 8  
 four pillars of, xxv–xxvi, 3–4  
 in International Relations and Global Studies theories, 3–4  
 under International Telecommunication Union, xxi  
 as multidimensional concept, 219–220  
 origins of, xx–xxi  
 in polycentric governance systems, xxi–xxii, xxiv, 9–10  
 positive, xxiv, xxv–xxvi  
 definition of, 3  
 elements of, xxv–xxvi  
 four pillars of, 3  
 positive peace perspective for, xxiii  
 as practices, 7–9  
 best practices model, 10  
 conditions and, 9–10  
 practice turn, 7  
 stakeholders in, xxv–xxvi  
 theoretical approach to, xx–xxvi  
 word cloud for, xxiii

- Cyber Security Reporting System (CSRS), 163–164, 166
- tactics, techniques, and procedures in, 166
- cyber sovereignty, xxv, xxvi
- Cyber Tech Accord, 242
- cyber war, 12. *See also* cyber hybrid warfare; wargames
- crises escalation and, 66
- conflict processes, 66
- cyber operations and, 69–70
- over territorial disputes, 66
- cyber off-ramps, 67–70, 87–88
- ambiguous signals in, 67
- in de-escalation strategies, 65–66
- elasticity of demand, 68, 69
- information costs of, 69
- public response to, 67
- substitutability dynamics, 67–69
- cyber operations
- as complements, in crisis escalation, 70
- as escalation-prone, 69–70
- as substitutes for other power measures, 70
- de-escalation strategies, cyber off-ramps and, 65–66
- evidence for, 70–81
- through case studies, 71
- through experimental studies, 71
- research design, 70–71
- through wargames, 71–81
- as negative peace, 65
- stability strategies, 65–66
- theoretical approach to, 64–65
- between U.S. and Iran, 81–87
- assessment of, 86–87
- covert operations in, 83
- cyber operations in, 83
- escalation of, 84–85
- origins of, 81–83, 85
- sanctions as result of, 86
- Summer 2019 crisis, 84–86
- cybernetics, 11–12
- Cyber-NTSB. *See* National Cybersecurity Board
- CyberPeace Corps, 167, 232
- research by, 233–234
- societal value of, 234
- CyberPeace Institute, 8–9, 175, 212
- cybersecurity. *See also* crowdsourcing; cyber war; information security measures
- access to, 216–218
- ecosystem of international law and norms, 218–219
- information sharing and, 42
- best practices for, 50–51
- cross-sector cooperation for, 42
- under Cybersecurity Information Sharing Act, 44–45
- definition and scope of, 43
- in peacebuilding processes, through
- cybersecurity governance, 102–103
- as human-centered, 106–108
- phishing attacks, 224
- in South Africa, with National Cybersecurity Policy Framework, 107–108
- Cybersecurity Information Sharing Act, U.S. (2016), 44–45
- cybersingularity, AGI and, 123–124
- cyberspace. *See also* cybersecurity; *specific topics*
- access issues in, 216–218
- during Covid-19 pandemic, 217
- Global Commission on Stability in Cyberspace, xx, 190
- infrastructure issues, 216
- layered deterrence in, xxii
- origins of, 11–12
- in polycentric governance systems, xx
- stability of, xxiv–xxv
- Cyberspace Solarium Commission, xxii
- Daniel, Michael, 135
- data destruction, 138–139
- data-theft, 132
- Declaration of Independence of Cyberspace, 39
- Defence League Cyber Unit (CDL), 231
- defend forward approach, to cyber aggression, 15
- defensive information security, 120
- denial of service, 121
- Diehl, Paul, 13–14
- Digital Blue Helmets initiative, xxv, 97–98
- digital divide, 3–4
- in cyber peacebuilding processes, 106, 107
- digital peace, xxiv
- digital repression, 23–25
- in China, 26
- tactical expertise in, 28–29
- threat identification in, 25–28
- as civil liberties violation, 28
- coercive habituation and, 28
- cost–benefit analysis of, 25–26, 32
- information and communication technologies
- involved in, 24, 25–32
- autonomous structures, 31–32
- Internet networks, 31–32
- kill switches, 29
- state control over, 30
- tactical expertise of and, 28–29
- threat identification through, 25–28
- infrastructure of, 30–32
- in Islamic Republic of Iran, 31, 32

- in literature, 33
- origins of, 26
- as physical integrity violation, 26
- in Poland, 29–30
- repressive agents, 29–30
- with smartphones, 24
- targets of, 28
- Digital Security policy, in Colombia, 107
- digital spoilers, in cyber peacebuilding processes, 104–106
  - in Colombia, 105
  - in South Africa, 105
- DMARC resource. *See* Domain-based Message Authentication, Reporting, and Conformance resource
- Domain Name System (DNS), 225–226
- Domain-based Message Authentication, Reporting, and Conformance (DMARC) resource, 225
- drive-by exploits, 121
  
- Eichensehr, Kristen, 135
- election manipulation
  - Advanced Persistent Threat Groups and, 239
  - from Russia, 239
  - in U.S., 239
- cyber attacks for, 132, 144, 147
- empirical studies, for cyber research
  - barriers to, 205–208
  - data collection issues, 205–207
  - expertise from multiple domains, limitations on, 207
  - narrow range of contexts, 207–208
  - cyber-related data publishing, 209–210
  - incentives for interdisciplinary research teams, 208
  - research partnerships, 208–209
    - with private stakeholders, 209
    - with public stakeholders, 209
  - theoretical approach to, 205
- Erice Declaration on Principle for Cyber Stability and Cyber Peace, 241
  - information and communication technologies and, 8
- Estonia
  - crowdsourcing for cybersecurity in, 231
  - Defence League Cyber Unit, 231
  - cyber aggression in, 14
- exploit kits, 121
- extortion, cyber attacks and, 132
  
- Federal Aviation Administration (FAA), 165
- feminist movements, in Argentina, 94
  
- Financial Services Information Sharing and Analysis Center (FS-ISAC), 43, 47–49
  - financial sector role in, 49
  - as non-polycentric, 57
  - operational elements of, 48
  - private sector role in, 48–49
- France, Paris Call for Trust and Security, xix–xx, xxv–xxvi, xxix, 176, 242
- François, Camille, xxii–xxiii, 195–204
- FS-ISAC. *See* Financial Services Information Sharing and Analysis Center
  
- Galtung, Johan, xxiv, 12–13
- GCA. *See* Global Cyber Alliance
- genocide, 136
  - cyber attacks as, 144–145
  - in Rwanda, 145
- GGE. *See* Group of Governmental Experts
- Gibson, William, 11–12
- Global Commission on Stability in Cyberspace, xx, 190
- Global Commission on the Stability of Cyberspace, 175–176
- Global Cyber Alliance (GCA), 223–224
- global public goods, 3
- Global South, peacebuilding processes in, 96
- gravity threshold, in Rome Statute, 137–139
- Greenberg, William, 5
- Group of Governmental Experts (Sixth Group) (GGE), 171, 177–182, 190, 219
  - goals and purpose of, 179–180
  - mandates for, 179–182
  - multilateral negotiations by, 172–174
  - norm implementation by, 181–182
  - Open-Ended Working Group compared to, 179–182
  - political context for, 177–179
- Guide to Cyber Threat Information Sharing* (National Institute of Standards and Technology) (NIST), 40, 43–44
- Guterres, António, 242
  
- hacktivism, 54
- Healey, Jason, xxi–xxii, 15
- Hofweber, Thomas, 4
- human rights. *See also* international human rights law
  - in Colombia, 100–101
  - in cyber peacebuilding processes, 99–102
  - in South Africa, 101
- human rights law, peacebuilding processes under, 100
- human-centered approach, to peacebuilding processes, 98

- human-centered cybersecurity governance, 106–108
- humanitarian law. *See* international humanitarian law
- Hurwitz, Roger, 155–156
- IAEA. *See* International Atomic Energy Agency
- ICAO. *See* International Civil Aviation Organization
- ICC. *See* International Criminal Court
- ICT. *See* information and communication technologies
- ICT4Peace, 236, 242
- ICTR. *See* International Criminal Tribunal for Rwanda
- ICTY. *See* International Criminal Tribunal for the Former Yugoslavia
- identity theft, 121
- I.L.C. *See* International Law Commission
- “infodemic,” cyberspace access and, 217–218
- information and communication technologies (ICT)
- cyber peace and, 7–8
  - CyberPeace Institute and, 7–8
  - development changes in, 22
  - digital repression and, 24, 69
    - autonomous structures, 31–32
    - Internet network infrastructure, 31–32
    - kill switches, 29
    - state control over, 30
  - tactical expertise of and, 28
  - threat identification through, 25–28
  - Ericc Declaration on Principle for Cyber Stability and Cyber Peace and, 8
  - peacebuilding processes with, 95–98
    - in South Africa, 107–110
  - World Federation of Scientists and, 8
  - youth empowerment through, 7
- information anonymity, 118–119
- information attribution, 118–119
- information costs, of cyber off-ramps, 69
- information security measures, with artificial intelligence, 119–123
- defensive information security, 120
    - as deterrence measure, 120
  - linkages within, 121–122
  - offensive measures, 120–121
  - as proactive measure, 120
- information sharing. *See also* Cyber Information Sharing and Collaboration Program
- best practices for, 40–41
  - between civilians and military, 45–46
  - clarification of “rules of the road,” 40
  - as confidence-building measure, 40
  - through crowdsourcing, for cybersecurity, 233
  - cyber peace through, 53
    - as best practice, 53–54
    - as confidence-building measure, 54–56
    - informational symmetries for, 53
    - risk assessment for, 53
    - thresholds of non-permissible online behavior, 53
  - cybersecurity and, 42
    - best practices for, 50–51
    - cross-sector cooperation for, 42
    - under Cybersecurity Information Sharing Act, 44
    - definition and scope of, 43
  - definition of, 43–46
  - Financial Services Information Sharing and Analysis Center and, 46–49
    - financial sector role in, 49
    - as non-polycentric, 57
    - operational elements of, 48
    - private sector role in, 48–49
  - Guide to Cyber Threat Information Sharing*, 40, 43–44
  - between military and civilians, 45
  - mitigation of cyberthreats through, 51–53
  - national platforms for, 50
  - non-polycentric, 57–58
  - open-source sharing communities, 45
  - operational aspects of, 43–51
    - agreed rules for thresholds
      - of shared threats, 44
    - as best practice for cybersecurity, 50–51
    - normative-substantive disincentives, 53
    - operative disincentives, 52
    - regulatory issues, 44
    - sharing entities, 45
  - overview of, 58–59
  - under polycentric governance, 41–42, 56–58
    - parameters of, 56
  - purpose of, 43
  - in regulatory contexts, 52
  - risk assessment and, 40
  - by stakeholders, 41
  - tactics, techniques, and procedures (TTPs)
    - in, 41
  - theoretical approach to, 39–43
  - trans-national platforms for, 50
  - trust building through, 40
  - types of information shared, 44
  - for vulnerabilities to cyber threats, reduction strategies for, 40
- information system attacks, 239
- information technology (IT). *See also* information and communication technologies

- cyber attacks of, 132
  - informational symmetries, for information sharing, 53
  - instrument of power responses, in wargames, 78
  - Inter-American Human Rights System, 100
  - International Atomic Energy Agency (IAEA), 156
  - International Civil Aviation Organization (ICAO), 156
  - International Criminal Court (ICC)
    - ad hoc* tribunals, 134
    - Comoros* case, 139
    - crimes against humanity and, 136
    - criminalization and prosecution of cyber attacks and, 147–148
    - considerations for, 137
    - as crime of aggression, 145–147
    - for data destruction, 138–139
    - as genocide, 144–145
    - Prosecutor v. Al Hassan*, 138
    - under Rome Statute, 136–137
    - Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 138
    - as war crimes, 141–143
    - genocide and, 136
      - cyber attacks as, 144
      - in Rwanda, 145
  - International Law Commission and, 147
  - in Iraq, 132
  - Islamic State, 132
  - Lubanga* appeal judgment, 137
  - in Myanmar, 132–133, 145
  - Rome Statute, 131–133
    - attribution through admissible evidence under, 139–140
    - Council of Advisers on the Application of the Rome Statute to Cyberwarfare, 135
    - criminalization of cyber attacks under, 136, 147
    - cyber attacks as crime of aggression, 145–147
    - cyber attacks as genocide under, 145
    - cyber attacks as war crimes under, 143
    - gravity threshold in, 141
    - principle of distinction in, 142
    - substantive crimes under, 140–141
    - UN Charter and, 146
    - weapons use under, 142
  - in Rwanda, 145
  - in Syria, 133
  - theoretical approach to, 131–132
  - war crimes in, 136
    - cyber attacks as, 141–143
- International Criminal Tribunal for Rwanda (ICTR), 134
- International Criminal Tribunal for the Former Yugoslavia (ICTY), 134
- international human rights law
  - cyber attacks under, 133–134
  - ecosystem of norms for, 218–219
- international humanitarian law, 100
  - cyber attacks under, 133
  - ecosystem of norms for, 218–219
- international law. *See also* international human rights law
  - cyber hybrid warfare under, 241
- International Law Commission (ILC), 147
- International Organization*, Special Issue of, 5, 18
- International Relations and Global Studies, 3
- International Telecommunication Union (ITU), xxi, 5–7
- Internet. *See also* digital divide
  - access to, 216–218
    - in Colombia, 107–108
    - in peacebuilding processes, 106–108
    - in South Africa, 106–107
- ARPANET, 31
- Iran. *See also* Islamic Republic of Iran
  - cyber war with U.S., 81–87
    - assessment of, 86–87
    - covert operations in, 83
    - cyber operations in, 83
    - escalation of, 84–85
    - origins of, 81–83, 85
    - sanctions against Iran, 86
    - Summer 2019 crisis, 84–86
  - Iran–Iraq War, 82
  - nuclear weapons development by, 82–83
    - under Joint Comprehensive Plan of Action, 82–83
  - Operational Nimble Archer, 82
  - Operational Praying Mantis, 82
  - Saudi Arabia as cyber target of, 83
- Iranian Revolution, 82
- Iran–Iraq War, 82
- Iraq, International Criminal Court in, 133
- ISIL. *See* Islamic State
- Islamic Republic of Iran, digital repression in, 31, 132
- Islamic State (ISIL), 132–133
- IT. *See* information technology
- ITU. *See* International Telecommunication Union
- JCPOA. *See* Joint Comprehensive Plan of Action
- Jensen, Benjamin, 15
- Joint Comprehensive Plan of Action (JCPOA), 82

- Khomeini, Ayatollah Ruhollah, 82  
 Kim Jong-Un, 239  
 Krasner, Stephen, 5  
 Kreps, Sarah, 67
- lawlessness. *See* cyber lawlessness  
*Lubanga* appeal judgment, 137  
 Lyon, David, 12
- Macron, Emmanuel, xix–xx  
 malware, 121  
 Marlin-Bennett, Renée, xi–xx  
 metaphors, 17–18  
   inadvertent complicity in, 17–18  
 MFA. *See* multi-factor authentication  
 Microsoft Corporation, peacebuilding processes  
   and, 175
- military  
   cyber elements in, 12–14  
   information sharing with civilians, 45–46
- money laundering, 54  
 Mubarak, Suzanne, 7  
 multi-factor authentication (MFA), 226  
 multistakeholder collaborations, 16–17  
   in peacebuilding processes, 102–104  
   in Colombia, 103  
   history of, 174–176  
   in South Africa, 103  
   under polycentric governance, 16
- Muslims, in China, detention of, 2  
 Mustang Panda cyber attack, 225–226  
 Myanmar, 132–133, 145
- National Aeronautics and Space Administration  
 (NASA), 165  
 National Cybersecurity Board (Cyber-NTSB),  
   159–163  
   applications of, 162–163  
   *Computers at Risk*, 160  
   development of, 161–162  
   goals and purpose of, 159–161
- National Cybersecurity Policy Framework, in  
   South Africa, 107
- National Institute of Standards and Technology  
 (NIST), 40, 43–44  
 National Research Council, 160  
 National Transportation Safety Board (NTSB),  
   163–166
- near-miss reporting systems, 165–166  
 negative peace, cyber war as, 65  
 Net Mundial conference, 174  
*Neuromancer* (Gibson), 11  
 Nguyen Xuan Phuc, 225  
 NIST. *See* National Institute of Standards and  
   Technology
- non-military confidence-building measures, 54  
 non-polycentric information sharing, 57  
 normative-substantive disincentives, for  
   information sharing, 53
- North Korea, WannaCry cyber attack by, 227,  
   239–240  
 NotPetya attacks, 132, 158  
 NTSB. *See* National Transportation Safety  
   Board
- OEWG. *See* Open-Ended Working Group  
 offensive information security measures, 120–121  
 Office of Personnel Management (OPM), in  
   U.S., 157–158  
   cyber attacks against, by China, 224
- Open-Ended Working Group (OEWG), 171,  
   177–182, 190  
   China and, 177–178  
   cyber stability strategies by, 182–184  
   goals and purpose of, 180  
   Group of Governmental Experts compared  
   to, 179–182  
   mandates for, 179–182  
   norm implementation by, 181–182  
   origins of, 177–178  
   political context for, 177–179  
   Russia and, 177–178, 183–184  
   UN Member States in, 178–179
- open-source sharing communities, 45  
 Operation Earnest Will, 82  
 Operation Praying Mantis, 82  
 operative disincentives, of information  
   sharing, 52
- OPM. *See* Office of Personnel Management  
 Ostrom, Elinor, 156  
 Ostrom, Vincent, xxv–xxvi
- Pact of Paris, xx–xxvi  
 Paris Call for Trust and Security, xix–xx,  
   xxv–xxvi, xxix, 176, 242  
 Paris Climate Accord, xx
- peace  
   as element of cyber, 12–14  
   negative, 65  
   universal definitions of, xxiv
- Peace Studies, xxiv, 12–13
- peacebuilding processes, through cyber  
   applications. *See also* Colombia; Open-  
   Ended Working Group; South Africa  
 Alliance for Peacebuilding, 98  
 comprehensive approach to, 96–99  
   potential applications in, 97  
 cybersecurity governance, 102–103  
   human-centered, 106–108  
 definition of, 97–98



- Digital Blue Helmets initiative, 97
- digital divide and, 106–107
- digital spoilers in, 105–106
- four pillars of, 99–108
- Internet access, inclusivity for, 106–108
  - multistakeholder governance, 102–104
  - promotion of human rights, 99–102
  - stability in cyberspace, 104–106
- in Global South, 96
- Group of Governmental Experts (Sixth Group) and, 171, 177–182, 190
- goals and purpose of, 179–180
  - mandates for, 179–182
  - multilateral negotiations by, 172–174
  - norm implementation by, 181–182
- Open-Ended Working Group compared to, 179–182
- political context for, 177–179
- history of, 171–176
- CyberPeace Institute, 175
  - Global Commission on the Stability of Cyberspace, 175–176
  - through multilateral negotiations, 172–174
  - multistakeholder roles in, 174–176
  - Net Mundial conference, 174
  - Paris Call for Trust and Security, xix–xx, xxv–xxvi, xxix, 176
- under human rights law, 100
- human-centered approach to, 98
- with information and communication technologies, 95–98
- in South Africa, 108–110
- under international humanitarian law, 100
- intrastate armed processes and, de-escalation of, 96
- Microsoft Corporation and, 175
- origins of, 96–97
- Program of Action and, 182–184
- through social media, 97
- state-centric approach to, 104–105
- theoretical approach to, 94–95, 170–171
- UN Draft Resolutions, 184–189
- Russia sponsored resolution, 188
  - State Sponsorship resolution, 185–186
  - U.S. sponsored resolution, 185–187
- by UN General Assembly, 172–174
- UN Draft Resolution votes, 187–190
- phishing attacks, 224
- physical integrity, violations of, 26
- PoA. *See* Program of Action
- Podesta, John, 225
- Poland, 29–30
- polycentric governance, xxv–xxvi, xx
- cyber peace and, xxi–xxii, xxiv, 9–10
  - boundaries of, 16–17
  - information sharing under, 41–42, 56–58
    - parameters of, 57  - monocentric governance and, 10
  - multistakeholder forms of, 16
- positive cyber peace, xxiv, xxv–xxvi
- definition of, 3
  - elements of, xxv–xxvi
  - four pillars of, 3
- positive peace perspective
- for cyber peace, xxiii
  - social elements, 13–14
- principle of distinction, in Rome Statute, 142
- proactive information security measures, 120
- Program of Action (PoA), 182–184
- Prosecutor v. Al Hassan*, 138–139
- Putin, Vladimir, 239
- The Quest for Cyber Peace*, 5–6
- ransomware
- by Advanced Persistent Threat Groups, 121, 239–240
  - WannaCry cyber attack, 227, 239–240
- Reagan, Ronald, 154
- Reid, Herbert, 13
- repression. *See also* digital repression
- by states
    - benefits of, 24–26
    - through city planning, 30
    - political costs of, 238
    - traditional modes of, 23–26, 238
- repressive agents, 29–30
- Reynolds, Linda, 240
- risk assessment, with information sharing, 40
- Robinson, Michael, xxii
- Roff, Heather, 132–133, 219–220
- Rome Statute. *See* International Criminal Court
- Russia
- electoral manipulation by, through APTs, 239
  - NotPetya attacks by, 132, 138, 227–228
  - UN Draft Resolutions by, for cyber peace, 188
- Ruzicka, Jan, 12
- Rwanda, 145
- International Criminal Tribunal for Rwanda, 134
- SAHRC. *See* South African Human Rights Commission
- Sánchez, Óscar Arias, 5
- Saudi Arabia, as cyber target of Iran, 83
- Schaake, Marietje, 15–16
- Schneider, Jacqueline, 67
- Scott, James, 30
- Searle, John, 5

- Security Service. *See* Sluzba Bezpieczenstwa
- Shackelford, Scott, 9–10
- side channel attacks, 121
- simulation diagrams, in wargames, 73
- Sluzba Bezpieczenstwa (Poland), 29–30
- smartphones, digital repression with, 239
- Smith, Brad, 175
- social engineering, 121
- social media
- Arab Spring and, 94
  - peacebuilding processes through, 97
- social movements, 94
- Solarwinds attack, 237
- Solemani, Qasem, 86
- South Africa
- cyber peacebuilding processes in, 94, 99
  - cyberspace stability in, 105–106
  - digital spoilers in, 104–106
  - information and communication technologies in, 108–110
  - Internet access in, 107
  - multistakeholder governance in, 102–103
  - policy implications for, 108–110
  - promotion of human rights, 101
  - South African Human Rights Commission, 101
  - through transitional justice, 108
  - National Cybersecurity Policy Framework, 107
- South African Human Rights Commission (SAHRC), 101
- sovereignty. *See* cyber sovereignty
- spam, 121
- Special Tribunal for Lebanon, 134
- stakeholders
- in cyber peace, xxv–xxvi
  - in empirical research, private/public partnerships in, 209
  - information sharing by, 41
  - multistakeholder collaborations, 16–17
  - in peacebuilding processes, 102–104
  - under polycentric governance, 16
- state repression. *See* repression
- state-centric approach, to peacebuilding processes, 104
- STIX language, in CISCSP, 50, 53
- Strange, Susan, 18
- Stuxnet attack, 95, 132, 238
- substitutability dynamics, with cyber off-ramps, 67–69
- Syria, 133
- tactical expertise, in digital repression, 28–29
- tactics, techniques, and procedures (TTPs)
- in Cyber Security Reporting System, 166
  - in information sharing, 41
- TAXII language, in CISCSP, 50, 53
- terrorism, 54
- Thornton, E. Nicole, 17–18
- threat identification, in digital repression, in China, 25–28
- threat intelligence, in aviation model, 157
- TLP. *See* Traffic Light Protocol
- Touré, Hamadoun, 5
- Traffic Light Protocol (TLP), 51, 53
- transitional justice, in South Africa, 108
- treatment groups, in wargames, 74–76, 78
- Trump, Donald, 81–87
- trusted verifiers. *See* verifiers
- TTPs. *See* tactics, techniques, and procedures
- Ukraine, digital attacks on power grid in, 95, 158
- NotPetya attacks, 132, 158, 227–228
- UN. *See* United Nations
- UN Charter
- cyber attacks under, 133–134
  - Rome Statute and, 146
- United Nations (UN). *See also* Open-Ended Working Group
- Draft Resolutions, for cyber peace, 184–189
  - Russia sponsored resolution, 188–189
  - State Sponsorship resolution, 185
  - U.S. sponsored resolution, 185–187
- General Assembly, 172–174
- UN Draft Resolution votes, on cyber peace resolutions, 187–190
- Group of Governmental Experts (Sixth Group), 171, 177–182, 190, 219
- goals and purpose of, 179–180
  - mandates for, 179–182
  - multilateral negotiations by, 172–174
  - norm implementation by, 181–182
  - Open-Ended Working Group compared to, 179–185
  - political context for, 177–179
- United States (U.S.). *See also* verifiers; *specific topics*
- Advanced Persistent Threat Groups in electoral processes manipulated by, 239
  - Solarwinds attack, 237
- cyber attacks in
- against Democratic National Committee, 225
  - against Office of Personnel Management, 224
  - prosecution of, 135

- cyber war with Iran, 85, 81–87
    - assessment of, 86–87
    - covert operations in, 83
    - cyber operations in, 83
    - escalation of, 84–85
    - origins of, 81–83, 85
    - sanctions as result of, 86
    - Summer 2019 crisis, 84–86
  - election manipulation in, Advanced Persistent Threat Groups and, 239
  - Federal Aviation Administration, 165
  - Joint Comprehensive Plan of Action and, 82–83
  - National Aeronautics and Space Administration, 165
  - National Transportation Safety Board, 163–166
  - Office of Personnel Management in, 157–158
    - cyber attacks against, by China, 224
  - Operation Earnest Will, 82
  - Operation Nimble Archer, 82
  - Operation Praying Mantis, 82
  - UN Draft Resolutions by, for cyber peace, 185–187
  - World Health Organization and, withdrawal from, 155–156
- Valeriano, Brandon, 15
- verifiers, of cyber peace
- aviation model for, 156
    - under Convention on International Civil Aviation, 156
    - under International Civil Aviation Organization, 156
  - threat intelligence in, 157
- Aviation Safety Information Analysis and Sharing System, 163–164
- Aviation Safety Reporting System, 163–165
- Federal Aviation Administration, 165
  - National Aeronautics and Space Administration and, 165
- Cyber Security Reporting System, 165, 166
- tactics, techniques, and procedures in, 166
- in domestic incident investigations, 159–163
- in historical incident investigations, 157–159
- NotPetya attacks, 158
  - Office of Personnel Management, 157–158
- International Atomic Energy Agency and, 156
- international investigation mechanisms, 166–167
- CyberPeace Corps, 167
  - National Cybersecurity Board (Cyber-NTSB), 159–163
    - applications of, 162–163
    - Computers at Risk*, 160
    - development of, 161–162
    - goals and purpose of, 159–161
  - National Transportation Safety Board, 163–166
  - near-miss reporting systems, 165–166
  - purpose of, 154–156
- violence, universal definitions of, xxiv
- WannaCry cyber attack, 227, 239–240
- war crimes, 136
- cyber attacks as, 141–143
- wargames
- coercive potential in, 80
  - conventional escalation in, 79
  - cyber escalation in, 79
  - cyber substitution in, 80
  - evidence through, 71–81
  - instrument of power responses, 79
  - participant behaviors, 72–74
  - response preferences in, 77
  - scenarios in, 78
  - simulation diagrams, 73
  - treatment groups, 74–76, 79
- WeChat, 22
- Wegener, Henning, xxiii–xxiv, 6
- WHO. *See* World Health Organization
- Wiener, Norbert, 11
- WikiLeaks, 225
- Woman's International Peace Movement, 162–163
- word cloud, for cyber peace, xxiii
- World Federation of Scientists, 5–6
- Ericc Declaration on Principle for Cyber Stability and Cyber Peace, xxi
  - information and communication technologies and, 8
  - information and communication technologies and, 8
- World Health Organization (WHO), 155–156
- Yanarella, Ernest, 13

