Index

accessing cyberspace, 294
accessing systems for information warfare, 75–9
ActiveX, 242, 287
Acxiom, 202
Adams, James, 38
affinity cards, 196, 209
Afghanistan war
  al Qaeda's dependence on Internet and, 45–6
  coalitions and, 129, 172
  commercial satellite photos and, 177
  information overload and decision-making hierarchy, 109
  minimal role of cyberspace conquest in, 2
agoras. *See* castles and agoras
Ahmad, Fahim, 261
AI. *See* artificial intelligence
air bags, 197
air-gapped systems, 64, 106, 270
al Qaeda. *See also* specific operations, e.g, September 11, 2001, attacks
  command and control exercised online, 48
  dependence on Internet, 45–6
  relative dependence on information infrastructure, 272
Alexander, Yonah, 44
alliances. *See* coalitions
Alneda.com, 259
Amazon.com, 146
Amerindian language, Sapir-Whorf hypothesis based on, 235–6, 248
Andalusi, Ameer, 261
Anna Kournikova virus, 92, 241
Annan, Kofi, 98
ANSI X12 standard for electronic data interchange (EDI), 246
anticorruption uprisings in Southeast Asia, 148
architecture
  boundaries between systems, growing fuzziness of, 306
  defined, 142–3
  enterprise architecture and systems integration, 142–8
  form and function, relationship between, 240–1
  informational. *See* information architecture
  standards defining, 244
Arthur, Brian, 277
artificial intelligence (AI), 115, 248

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-87160-0 - Conquest in Cyberspace: National Security and Information Warfare
Martin C. Libicki
Index
More information

assessment as information warfare countermeasure, 87–90
asymmetric coalitions, 130–1, 166, 191
AT&T/DSC phone outage, 37
ATM machines, 24, 58

back doors installed by systems vendors, 77, 268
Back Orifice, 285
Baird, Zoe, 210
Bangkok, anticorruption uprising in, 148
bank cards, 195
battle damage assessment (BDA), 87–90, 215
Bayesian logic, 52, 55, 58–9
BDA. *See* battle damage assessment
Bekaa Valley campaign (1982), 91
Berners-Lee, Tim, 245, 248
Beta format, 277
betrayal of coalition partners, deliberate, 228–30
bin Laden, Osama, 44, 48. *See also* al Qaeda
biometrics
  national identity systems and, 184–6, 188–90
  public surveillance devices and, 197
blackmail and coercion, 208–11
Bluetooth, 36, 77, 103
Bosnia conflict, 69
boundaries
  between semantic and syntactic layers, problems maintaining
    friendly conquest, 242–4
    hostile conquest, 241–2
    layers in cyberspace, 240
  between systems, 297–9
BSD UNIX, 286

Canadian terrorism cases, 47, 260–1
castles and agoras, 62–71
  accessing closed systems, 76–9
  attacking castles through their agoras, 64–6
  complex networks housing both, 64
  defined, 62–4
  inducing enemy into castling itself, 70–1
  layers of cyberspace and, 65–6
  military vs. civilian approach to, 65–70
  redundancy and filtration, 63
cell phones
  alliances with individuals and, 151–4
  Microsoft and, 283
  surveillance via, 197–8
centralization of decision-making hierarchy and information overload, 107–11
CERT (Computer Emergency Response Team), 38
China
  EP-3 aircraft grounded in (2001), 175
  Fulangong, 148
  stratagem, preference for, 274
  successful constraints imposed on Internet by, 8
Churchill, Winston, 52, 128
Cisco Systems, 227
Citibank, 223
Clarke, Richard, 45
Clinton, Bill, 290
closed vs. open systems, 3, 9, 42, 141, 249
coalitions
  asymmetric, 130–1, 166, 191
  benefits of, 130–1
  corporate models of, 128–9
  costs of, 132–3, 136–42
  Department of Defense (DoD) Global Information Grid (GIG), 142, 159–64, 250
  dependence created by, 136–42
  enterprise architecture and systems integration, 142–8

© Cambridge University Press www.cambridge.org

Cambridge

Cambridge University Press
978-0-521-87160-0 - Conquest in Cyberspace: National Security and Information Warfare
Martin C. Libicki
Index
More information

geospatial database used to build, 178–82
individuals, alliances with, 148–54
information access, hidden advantages of providing, 191
information exchanges in, 131–6
logic of soft power in, 127
mechanisms of, 128–30, 167–8
military models of, 129–30
NATO, 69, 155, 164–6, 191
organizations, alliances of, 155–66
overt and covert binding mechanisms of, 167–8
standards issues, 137–8, 140–1
technological development, ecology of, 155–9
vulnerabilities of. *See* intimacy and vulnerability

Code Red worm, 18, 37, 91–2, 285
coercion and blackmail, 208–11
Cold War
counterintelligence/prediction, 91
intelligence systems during, 194
technological developments resulting from, 100
U.S. public readiness for, 214

collateral damage, 98–9, 258–9
command and control
control paradox of information warfare, 96
flood and sag, 81, 121–4
hostile conquest, best use of, 256–62
information overload, 102–3, *See also* information overload
information scarcity, 102
ping and echo, 121–2
redundancy in, 85
terrorists and terrorism, use of Internet by and for, 48–9

commons, Internet viewed as, 8
complexity and conquest, 240–4
boundaries between semantic and syntactic layers, problems maintaining, 240–2
friendly conquest, 242–4
hostile conquest, 241–2

Computer Emergency Response Team (CERT), 38
computer network exploitation. *See* spying or eavesdropping
conglomerates, information overload and rise of, 108
conquest in cyberspace, 1–14
defining, 4–10
layers in cyberspace, 8–10
persistence of certain rules in cyberspace, 7–8
recognition of actions required for existence in cyberspace, 6–7
replicable construct, cyberspace as, 5–6
friendly vs. hostile conquest, 3–4. *See also* friendly conquest; hostile conquest
growing importance of cyberspace and, 1–3
nonstate actors' potential role in, 2
policy regarding. *See* policy questions
types of hostile attacks, 1–2

construct, cyberspace as replicable, 5–6
control paradox of information warfare, 96
conversation, conquest in cyberspace as. *See* layers in cyberspace; linguistic analogies
cookies, 201–2, 204
corruption, 81–2
AI and
assessment as countermeasure against, 89–90
intimacy and vulnerability to, 230
learning as countermeasure against, 86
policy on use of hostile conquest and, 261–2

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-87160-0 - Conquest in Cyberspace: National Security and Information Warfare
Martin C. Libicki
Index
More information

counterintelligence/prediction, 90–101
  importance of, 90–3
  limitations of, 93–5
countermeasures
  against friendly conquest. *See* defending against friendly conquest
  against hostile conquest. *See* defending against hostile conquest
  against information warfare. *See* information warfare
credibility of information, undermining. *See* noise, information warfare as
cryptography. *See* encryption
culture, informational, 117
customer relationship management (CRM) software, 196
cyberspace
  access points, growing number of
  AI in, 115, 248
  boundaries between systems, increasing fuzziness of, 297–9
  conquest in. *See* conquest in cyberspace
  growing significance of, 1–3
  hardware and software advances
  privatization of security and trust in, 272–6
  public and private versions of, 301–3
  replicable construct, viewed as, 5–6
  standardized encryption for, 299–301

deception
  as type of information warfare, 29–30
  decision-making hierarchy, injecting information into, 118–21
  information overload, effects of, 106–7
  learning as countermeasure against, 85–6
decision-making hierarchy and information overload
  delegation and hierarchical decomposition as coping strategy, 112–13
  injecting information into, 118–21
  micromanagement, overload leading to, 107–11
defending against friendly conquest, 256, 281–9
  determining what is unwarranted or undesirable influence, 257
  difficulty in legislating for, 281–2
  Microsoft
    friendly conquest by, 282–5
    security issues related to market dominance of, 285–9
defending against hostile conquest, 256, 262–76
  determining existence and source of threat, 262–5
  determining what must be defended and why, 256
  escalation in offensive-defensive activities, 265–8
  insurance, 269
  laws, effectiveness of, 268–9
  level of threat from, 262
  privatization of security in cyberspace, 272–6
  restrictive, monitoring, and securitization tactics, 268–70
  transparency, 270–2
defending against information warfare. *See* under information warfare
Defense Department. *See* Department of Defense
defense systems, information warfare against. *See* information warfare

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-87160-0 - Conquest in Cyberspace: National Security and Information Warfare
Martin C. Libicki
Index
More information

denial or disruption of service, 80–1
  assessment as countermeasure against, 89
  intimacy and vulnerability to, 230
  learning as countermeasure against, 86–7
  policy on use of hostile conquest and, 259–60
Department of Defense (DoD)
  AI, interest in
  data dictionary terms, 246
  defense contractor privileges, 221
  Global Information Grid (GIG), 142, 159–64, 250
dependence
  coalitions creating, 136–42
  complexity and, 255
  friendly conquest, 167
  global systems, 191
  intimacy and vulnerability issues, 228
  policy questions regarding, 279–80, 281
deployability of information warfare, 99
Dertouzos, Michael, 304
Desert Storm. *See* Gulf War
developing vs. developed countries, 2, 77, 152
Digital Millennium Copyright Act, 268–9, 282
digital signatures, 33–4
  accessing systems for information warfare, 75
  deception, as means of defeating, 120
  defending against hostile conquest and, 271
  inability to obtain, 273
  registries, 273
  retail conquest and, 218
  standardized encryption and
DigitalGlobe, 175
digitization of information, 203
disinformation, 50–5
disruption of service. *See* denial or disruption of service
distraction as form of information warfare, 83–4
Djakarta, anticorruption uprising in, 148
DoD. *See* Department of Defense
DOS overtaken by Windows, 243–4

eavesdropping. *See* spying or eavesdropping
ebXML (electronic business XML), 254
E-commerce attack of February 2000, 80
Edwards, Edwin, 210
electromagnetic pulses (EMP), 29
electronic business XML. *See* ebXML
electronic warfare
  as information warfare, 29
  filtration as defense against noise, 57
e-mail, 198–2, 215, 242, 273
EMP. *See* electromagnetic pulses
encryption
  cell phone messages, 152
  corruption, defending against, 82
  information warfare and, 23, 32–3, 43
  national identity system, 186–7, 189
  radar-to-radar links, 79
  redundancy as defense against noise, 56
  standardized, 299–301
  wireless devices used to hack into closed systems, 78
enterprise architecture and systems integration, 142–8
Eros satellite, 175
E-services (Hewlett-Packard), 253–4
espionage. *See* spying or eavesdropping

© Cambridge University Press www.cambridge.org

Cambridge University Press
978-0-521-87160-0 - Conquest in Cyberspace: National Security and Information Warfare
Martin C. Libicki
Index
More information

ethics
  hostile conquest, best use of, 257–62
  information warfare and, 97–8
  national identity systems and, 189–90
EU Galileo satellite navigation constellation, 167, 279
Expedia, 284
exploitation of computer networks. *See* spying or eavesdropping

false alarms, 83
filtration
  as defense against noise, 57–9
  castles and agoras, 63
flood and sag, 81, 121–4
form and function, relationship between, 240–1
Fourier transforms, 56
free speech in cyberspace, supposed inevitability of, 7–8
French commercial satellites, 175
Friedman, Thomas, 128
friendly conquest, 3, 12–13, 125–68
  best use of, 256–7, 276–81
  coalitions and. *See* coalitions
  complexity facilitating, 242–4
  defending against. *See* defending against friendly conquest
  defined, 3–4, 126–7
  enterprise architecture and systems integration, 142–8
  information access, hidden advantages of providing, 191
  intertwining with hostile conquest, 13
    in retail endeavors, 193, 218–19
    intimacy and vulnerability, 230
  layers of cyberspace and, 10, 13–14
  Microsoft's attempts at, 282–5
  thought experiments in, 166–8, 192
    using geospatial data. *See* geospatial database
    using national identity systems. *See* national identity systems
  vulnerability resulting from intimacy. *See* intimacy and vulnerability
Fulangong, 148
function and form, relationship between, 240–1

Galileo satellite navigation constellation, 167, 279
Gates, Bill, 290
geospatial database, 170–82
  as general information, 170
  coalition building via, 178–82
  commercial satellites, problem of, 175–8
  compliance with U.S. rules, ensuring, 179–80
  control of international remote sensing capabilities via, 178–80
  internal structure of industry, influence on, 178–9
  international participation in, 171–2
  interpretation, role of, 191–2
  likelihood of, 169–70
  national sovereignty, geospatial definition of, 170–1
  pricing and market influence, 178
  ship tracking via, 181
  standards for, 174–5
  transparency, taking advantage of, 178–82
  U.S. agencies involved in tracking geospatial data, 171
  U.S. benefits derived from, 172–3, 182
  U.S. influence on world and, 169
  XML precursors, 246
Germany
  commercial satellites, 175–6
  Stasi in East Germany, 209
Gibson, William, 4

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-87160-0 - Conquest in Cyberspace: National Security and Information Warfare
Martin C. Libicki
Index
More information

GIG. *See* Global Information Grid
Global Crossing, 295
global geospatial database. *See* geospatial database
Global Information Grid (GIG), 142, 159–64, 250
globalization of information, 203–4
GlobalStar, 295
Google, 200, 213
Gould, Stephen J., 235
Grady, Scott, 66
Gresham's law, 206
Gulf War
- cleverness of enemies, anticipating, 101
- commercial satellite capabilities and, 175
- communications links, attack on, 102
- conspicuous nonmicromanagement of, 112
- counterintelligence/prediction, 94–8
- military personnel, coercion or blackmail of, 211
- minimal role of cyberspace conquest in, 2
- technological developments resulting from, 100

Hailstorm (Microsoft initiative), 199–200
Hammoud (Ameer Andalusi), 261
hard power vs. soft power, 3–4, 276
Harding, Warren, 230
hardware and software
- powerful hardware leading to complex software, 292–4
- redundancy, 84–5

Haski, Hassan el, 48
Health Insurance Portability and Accountability Act (HIPAA), 269
Henry, Ryan, 38
Herman Miller systems, 157
Hewlett-Packard E-services, 253–4
hierarchy of decision-making and information overload
- delegation and hierarchical decomposition as coping strategy, 112–13
- injecting information into, 118–21
- micromanagement, overload leading to, 107–11

HIPAA, *See* Health Insurance Portability and Accountability Act
Hitler, Adolph, 29, 53
Hoover, J. Edgar, 210
Hopfield net, 56
hostile conquest, 3, 10–12
- best use of, 256–62
- complexity facilitating, 241–2
- defending against. *See* defending against hostile conquest
- defined, 3–4
- information warfare, 15–16, *See also* information warfare
- intertwining with friendly conquest, 13
  - in retail endeavors, 193, 218–19
  - intimacy and vulnerability, 230
- layers of cyberspace and, 10, 13–14
- types of, 1–2

Hotmail, 48, 283
Hudson River tunnels plot, 261

IADs, 75, *See* integrated air defense systems, potential attacks on, *See also* information warfare
IBM's WebSphere program, *See* WebSphere program, IBM
ICANN, *See* Internet Corporation for Assigned Names and Numbers
IDC (consulting group), 45
identification of individuals
- in cyberspace, 200–02
- national systems for. *See* national identity systems

CAMBRIDGE

Cambridge University Press
978-0-521-87160-0 - Conquest in Cyberspace: National Security and Information Warfare
Martin C. Libicki
Index
More information

Ikonos satellite, 175–6
I-Love-You virus, 33, 37, 80, 92, 94, 285
IM. *See* Instant Messaging
Indian commercial satellites, 175
individuals, alliances with, 148–54
industrial revolution and noise tolerance, 60
information architecture
  culture of information and, 117
  injecting information into, 118–21
  nodal architecture, elements of, 118
  significance of, 116–21
information culture, 117
information exchanges in coalitions, 131–6
information overload
  conventional information warfare techniques and, 105–7
  coping strategies, 107, 111–16
  decision-making hierarchy
    delegation and hierarchical decomposition as coping strategy, 112–13
    injecting information into, 118–21
    micromanagement, overload leading to, 107–11
  diverse communication media, proliferation of, 103–4
  flood and sag, 81, 121–4
  geolocation methods, 104
  information architecture and effects of. *See* information architecture
  information culture and, 117
  nodal architecture, elements of, 118
  ping and echo, 121–2
  problem of, 102–3
  sources of, 103–5
information revolution
  overload created by. *See* information overload
  retail conquest and. *See* retail conquest
information scarcity, 102
information warfare, 7–14
  accessing systems, 75–9
  against command and control. *See* command and control; information overload
  as noise. *See* noise, information warfare as
  as terrorist attack, 43–6
  by information overload. *See* information overload
  control paradox, 96
  countermeasures, 79, 84–90
    assessment, 87–90
    learning, 85–7
    prediction/intelligence, 90–5
    redundancy, 84–5
  deployability, 99
  difficulty of, 37–43, 73–5, 95–6, 100–1
  direct destruction of information, 21–2
  effective management and weaponization, importance of, 95–6
  ethical issues, 97–8
  hostile conquest as, 15–16
  ideal-type definition of, 16–24
  increasing global importance of information systems and, 49
  information systems, attacks on, 22–4
  integrated logistics support for, 100
  integration into combined arms, problem of, 99
  layers in cyberspace and, 24–7
  means of, 79–84
    corruption, 81–2
    denial or disruption of service, 80–1
    distraction, 83–4
    spying or eavesdropping, 79–80

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-87160-0 - Conquest in Cyberspace: National Security and Information Warfare
Martin C. Libicki
Index
More information

nuclear warfare compared, 37–43
predictability of effects and collateral damage, 98–9
safe storage and use issues, 99–100
strategic, 73–101
training issues, 100
types of, 27–31
computer network attacks, 27–8, 37
deception, 29–30
electronic warfare, 29
physical attacks on information systems, 29
psychological warfare, 30
spying or eavesdropping (exploitation), 28–9
understanding of information system controls crucial to, vii
information warfare, 35
insiders, suborning or threatening, 76
Instant Messaging (IM), 202, 215
insurance against computer network attacks, 269
integrated air defense systems (IADS), potential attacks on, 75, *See also* information warfare
integrated logistics support for information warfare, 100
integration of information warfare into combined arms, problem of, 99
integration of systems and enterprise architecture, 142–8
intelligence used to predict attacks, 90–5
importance of, 90–3
limitations of, 93–5
interception. *See* spying or eavesdropping
Internet
cell phone access to, 151–4
growing importance of, 1–3
layers in cyberspace, 239
market or commons, viewed as, 8
retail conquest via, 198–202
telephony, increasing overlap with
terrorist use of. *See under* terrorists and terrorism
Internet Corporation for Assigned Names and Numbers (ICANN), 279–80
Internet Protocol version 6 (IPv6), 201, 218
intimacy and vulnerability, 220–30
deliberate betrayals, 228–30
maintenance of internal barriers, 220–2
reputations, ruining, 223
sundering relationships as aim of cyberspace conquest, 222–5, 230
susceptibility of coalition partners to attack, 225–8
invention, benefits of, 276
IPv6, 2, 201, 218. *See* Internet Protocol version
Iraq war
and video cameras, 152
NATO and, 166
U.K. vs. U.S. forces, relative openness of, 69
Iraqi assistance to Serbians during Kosovo campaign, 87
Iraqi war against Kuwait. *See* Gulf War
Iridium satellite system, 103, 295
Islamic terrorists. *See* terrorists and terrorism
Israel
Bekaa Valley campaign (1982), 91
Eros satellite, 175
stealth technology development and, 100
Ivanov, Igor, 98

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-87160-0 - Conquest in Cyberspace: National Security and Information Warfare
Martin C. Libicki
Index
More information

Jacquard, Roland, 44
Japan
keiretsu, 166–7
origins of organizational alliance in, 156–7
Toyota and Toguchi method, 60
Java, 241, 254, 287
Jihadist terrorists. *See* terrorists and terrorism
Johnson, Paul, 48

Kaplan, Robert, 44
keiretsu, 166–7
Kellogg-Briand Pact, 270
keystroke monitors, 203
knowledge and learning as information warfare countermeasure, 85–7
Kosovo conflict
coalitions and, 129, 172
hostile conquest, best use of, 258
information overload and decision-making hierarchy, 109
Iraqi assistance to Serbians in, 87
military personnel, coercion or blackmail of, 211
minimal role of cyberspace conquest in, 2
Kournikova virus, 92, 241

Lakoff, George, 234
Landsat 7 satellite imagery, pricing of, 178
language. *See* linguistic analogies
laws against hostile conquest, effectiveness of, 268–9
layers in cyberspace, 8–10, 231–55, *See also* physical layer/phonology, pragmatic layer, semantic layer, syntactic layer
boundaries between semantic and syntactic layers, problems maintaining, 240
friendly conquest, 242–4
hostile conquest, 241–2
castles and agoras, 65–6
complexity in. *See* complexity and conquest
form and function, relationship between, 240–1
information warfare and, 24–7
Internet, 239
interoperability between, 233–4, 237
OSI model, 237–9, 255
learning as information warfare countermeasure, 85–7
Lebanese role in foiling Hudson River tunnels plot, 261
Lessig, Lawrence, 7
Liberty Alliance, 285
Lindsay, Germaine, 47
linguistic analogies, 231–2
layers of cyberspace. *See* layers of cyberspace; physical layer/phonology; pragmatic layer; semantic layer; syntactic layer
narrative and vocabulary, retail interpretation of wholesale campaign via, 216–17
of coalition dependency, 138–9
redundancy as defense against noise, 55–6
Sapir-Whorf hypothesis, 235–6, 248
Linux, 32, 36, 172, 222, 286–7
London subway bombings, 47, 196

M2G, 44
Madrid bombings, 48
Manila, anticorruption uprising in, 148
market, Internet viewed as, 8
massive multiplayer online role-playing games (MMORPGs), 6
Mayaguez Rescue, 109
McLuhan, Marshall, 241

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-87160-0 - Conquest in Cyberspace: National Security and Information Warfare
Martin C. Libicki
Index
More information

McNealy, Scott, 204
M-commerce, 152
Meier, Sid, 293
Melissa virus, 18, 37, 285
micro-electromechanical (MEM) devices, 197
micromanagement and information overload, 107–11
Microsoft
  Code Red worm and, 94
  customer relationship model, 134
  DOS overtaken by Windows, 243–4
  friendly conquest by, 282–5
  growing complexity of software, 294
  Hotmail, 48, 283
  intimacy and vulnerability, 227
  market dominance of, 7
  P3P, 205
  Passport and Hailstorm initiatives, 199–200
  pragmatic layer and Web services offered by, 254
  security issues related to market dominance of, 285–9
  semantic and syntactic layers, permeability between, 242–4
microwave attacks, 29
military personnel, coercion or blackmail of, 210–11
Milosevic, Slobodan, 98, 258–9
Minihan, Lt. General Kenneth A., 38
misinformation, 50–5
MMORPGs. *See* massive multiplayer online role-playing games
mobile phones. *See* cell phones
MoneyCentral, 284
Moore's Law, 292
Morris worm, 37
Moussaoui, Zacarias, 189

narrative, role of, 216–17
national identity systems, 182–91
  biometric components, 184–6, 188–90
  casual access, preventing, 186, 189
  correlation of identified person with history, 186
  CRS (card reading system), 186–7
  encryption, 186–7, 189
  ethical objections to, 189–90
  foreign systems and, 187–91
  history on individuals built up by, 184
  interpretation, role of, 191–2
  likelihood of, 169–70
  rationales for, 183–4
  reliable association of individuals with their history via, 183–4
  standards for, 190–1
  terrorists and terrorism, control of, 169, 183, 189–90
  U.S. influence on world and, 169
National Institute of Standards and Technology (NIST) Advanced Encryption Standard, 299
national sovereignty, geospatial definition of, 170–1
NATO. *See* North American Treaty Organization
Netscape, 201
network attacks, 27–8, 37
network exploitation. *See* spying or eavesdropping
networking
  globalization of information via, 203–4
  of sensor devices, 197–8
Neumann, Peter, 286
Nimda worm, 285
NIPRnet, 64
NIST. *See* National Institute of Standards and Technology Advanced Encryption Standard
nodal architecture, elements of, 118

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-87160-0 - Conquest in Cyberspace: National Security and Information Warfare
Martin C. Libicki
Index
More information

noise, information warfare as, 50–72
  confusion rather than destruction induced by, 71–2
  disinformation, 50–5
  filtration as defense against, 57–9
  misinformation, 50–5
  redundancy as defense against, 55–7
  tolerance for noise, 59–60
    in cyberspace, 62–71. *See also* castles and agoras
    in real environments, 60–2
North American Treaty Organization (NATO), 69, 155, 164–6, 191
North Korea, 272
nuclear warfare
  effective weaponization of nuclear devices, 96
  ethics of information warfare compared to, 98
  information warfare compared, 37–43
Nye, Joseph, 3, 276

one-to-one services, 148–54
Open Systems Interconnection (OSI) reference model, 237–9, 255
open vs. closed systems, 3, 9, 42, 141, 249
operating systems, 32–3
  commercial systems, trends in and toward, 35–7
  filtration as defense against noise, 59
  intimacy and vulnerability, 222
organizations, alliances of, 155–66
  DoD's Global Information Grid (GIG), 142, 159–64, 250
  technological development, ecology of, 155–9
Orwell, George, 235
OSI. *See* Open Systems Interconnection
outsourcing service functions, 297–9

P3P. *See* Platform for Privacy Preferences
Passport (Microsoft initiative), 199
passwords
  accessing systems for information warfare, 75
  countermeasures against attacks on, 86
  filtration as defense against noise, 58
  information warfare and, 22, 33, 39
  layers of cyberspace and, 9
  Passport (Microsoft initiative), 199
Patriot missiles, 94
Peartree, Edward, 38
permanent vs. temporary damage from computer network attacks, 37
personal information, retail conquest via. *See* retail conquest
personalization of Web pages, 213
persuasion in retail conquest
  amalgamation of private information via, 207
  limitations on, 214–15
  use of private information for purposes of, 211–13
PGM. *See* precision guided munitions
phishing, 119, 213
physical layer/phonology, 8
  cyberspace, 236
  human language, 232
  information warfare and, 24
  OSI model, 238
ping and echo, 121–2, 217–19
Platform for Privacy Preferences (P3P), 205
plug-ins, 59
policy questions, 1–14, 256–90
  friendly conquest
    best use of, 256–7, 276–81
    defending against. *See* defending against friendly conquest

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-87160-0 - Conquest in Cyberspace: National Security and Information Warfare
Martin C. Libicki
Index
More information

hostile conquest
best use of, 256–62
defending against. *See* defending against hostile conquest
politicians and political appointees, coercion or blackmail of, 210
pragmatic layer, 249–54
cyberspace, 237
human language, 233
processing of, 239–40, 245
precision guided munitions (PGM), 91, 159
predictability of effects and collateral damage
information warfare, 98–9, 258–9
policy on use of hostile conquest and, 258–9
prediction/counterintelligence, 90–5
importance of, 90–3
limitations of, 93–5
prioritization, coping with information overload by, 113–14
privacy concerns
national identity system, ethical objections to, 189–90
Passport (Microsoft initiative), 199
retail conquest, 204–6
private information, collection and use of. *See* retail conquest
privatization of security and trust in cyberspace, 272–6
processor speed, 292–3
Proctor and Gamble, 157, 223
psychological warfare and propaganda
as information warfare, 30
at retail level, 195, 210–11
at wholesale level, 193
public and private versions of cyberspace, 273
public policy. *See* policy questions
push techniques, 213, 215

Quickbird satellite, 175

radar-to-radar links, 78–9
Radio Free Europe, 194
radio frequency identification devices (RFIDs), 187, 197–8
Ralston, Joseph, 210
RapidEye satellite, 175
redundancy
castles and agoras, 63
command and control, 85
communications, 84
defense against noise, 55–7
hardware, 85
information overload and
diverse communication media, proliferation of, 103–4
effects on conventional information warfare techniques, 105
information warfare countermeasure, 84–5
software, 84–5
Reid, Richard, 189
remote maintenance ports, hacking via, 76–7
rental car transponders, 197
replicable construct, cyberspace as, 5–6
reputations, exploiting intimacy to ruin, 223
retail conquest, 193–219
amalgamation of private information, 206–8
coercion and blackmail, 208–11
combination of friendly and hostile conquest in, 193, 218–19
globalization of information and, 203–4
limitations on, 214–15
low-value vs. high-value information, 194–5
narrative, monitoring, 216–17
persuasion
amalgamation of private information via, 207
limitations on, 214–15

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-87160-0 - Conquest in Cyberspace: National Security and Information Warfare
Martin C. Libicki
Index
More information

retail conquest *(cont.)*
    use of private information for purposes of, 211–13
  privacy concerns, 204–6
  psychological warfare and propaganda, 195, 210–11
  purchasing private information, 207–8
  sources of information used in
    cyberspace, 198–202
    real world devices, 195–8
  stealing private information, 208
  using private information, 208–13
  volume of information available for, 194–5
  vulnerability through intimacy. *See* intimacy and vulnerability
  wholesale campaigns
    limitation of retail conquest by, 215
    measured using retail channels, 215–17
    spying or eavesdropping at level of, 193
RFIDs. *See* radio frequency identification devices
Robertson, Nic, 44
Roosevelt Dam, supposed terrorist attack on, 45
Russia
  ethics of information warfare and, 98
  in Cold War. *See* Cold War

safe storage and use issues, 99–100
Saffo, Paul, 204
SAP enterprise management software, 133
Sapir-Whorf hypothesis, 235–6, 248
satellites. *See also* specific satellites and satellite systems, e.g, Galileo
  dependency, systems developed from fear of, 167, 279
  geospatial database and. *See* geospatial database
  growing access to cyberspace and
SCUD missiles, 94, 100
semantic layer, 9, 245–9
  boundaries with syntactic layer
    friendly conquest, 242–4
    hostile conquest, 241–2
    problems maintaining, 240
  categorical structuring provided by, 234–6
  concepts and language, relationship between, 235–6
  cyberspace, 237
  human language, 232–3
  information warfare, 25
  narrative and vocabulary, retail interpretation of wholesale campaign via, 216–7
  processing by humans, 239–40, 245
  real vs. abstract semantics in cyberspace, 245
  standards for, 245–9
Semantic Web, 248
sensors
  networking and retail conquest, 197–8
  pragmatic layer and, 250–1
September 11, 2001, attacks, 214–15
  command and control, use of Internet for, 48
  national identity systems and, 169, 183
  public surveillance devices installed in wake of, 196
SETI-at-home, 151
Shannon, Claude, 50
Shapiro, Carl, 140
ship tracking via global geospatial database, 181
shunting, 213
Sidewalk, 284
signatures, digital. *See* digital signatures

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-87160-0 - Conquest in Cyberspace: National Security and Information Warfare
Martin C. Libicki
Index
More information

Silicon Valley, 64, 128, 156
simple object access protocol (SOAP), 254
SIPRnet, 64
SOAP. *See* simple object access protocol
social norms operating in cyberspace, 8
soft power vs. hard power, 3–4, 276
software and hardware
- powerful hardware leading to complex software, 292–4
- redundancy, 84–5

Sony, 277
spam, 15, 48, 73, 112, 115, 213, 274
specialists, distillations of information from, 113
speed of processors, 292–3
Spot satellite, 175
spying or eavesdropping
- assessment as countermeasure against, 88–9
- information overload, effects of, 105–6
- intimacy and vulnerability to, 229
- policy on use of hostile conquest and, 260–1
- strategic means of information warfare, 79–80
- type of information warfare, 28–9
- wholesale level, operation at, 193

standards
- architecture of cyberspace defined by, 244
- coalition dependency and, 137–8, 140–1
- encryption, 299–301
- geospatial database, 174–5
- national identity systems, 190–1
- policy questions regarding friendly conquest and, 277–8, 281
- semantic layer, 245–9
- XML, 245–7, 254

Stasi, 209
stealth technology development, 100
Stephenson, Neil, 5
storage and use, safety issues relative to, 99–100
strategic information warfare, 73–101
Sun Microsystems, 254, 285
Sun Tzu, 38
Surrey Satellite Technology, 175
surveillance devices, proliferation of, 196–8
syntactic layer, 8–9
- boundaries with semantic layer
  - friendly conquest, 242–4
  - hostile conquest, 241–2
  - problems maintaining, 240
- cyberspace, 236–7
- human language, 232
- information warfare, 24–5
- interoperability of layers and, 237–8
- OSI model, 239
- XML, 245–7, 254

systems integration and enterprise architecture, 142–8

Tanweer, Shehzad, 47
Teapot Dome scandal, 230
technological development, ecology of, 155–9
telephony. *See* cell phones
temporary vs. permanent damage from computer network attacks, 37
TerraSAR-X satellite, 176
terrorists and terrorism
- hostile conquest used against, 259–62
- information warfare and, 43–6
- layers of cyberspace used by Islamic terrorists, 10
- narrative, role of, 216
- national identity systems and, 169, 183, 189–90

© Cambridge University Press www.cambridge.org

terrorists and terrorism *(cont.)*
  use of Internet by and for, 46–9
    command and control, 48–9
    hostile conquest used against, 259–2
    instructional materials, gathering and distributing, 47–8
    recruitment tool, 46–7
thought experiments in friendly conquest, 166–8, 192
  using geospatial data. *See* geospatial data
  using national identity system. *See* national identity system
TiVo, 199
Toguchi method, 60
tokens for accessing systems, 75
toll collection surveillance devices, 196–7
Toronto bombing case, 47, 260–1
Toyota, 60
training issues in information warfare, 100
transparency
  defending against hostile conquest, 270–2
  geospatial database taking advantage of, 178–82
trellis encoding, 50
Trinity, 96
TRUSTe, 205
Tsouli, Younis, 47, 260
Tucker, David, 45
Turing test, 202

UAVs. *See* unmanned aerial vehicles
UDDI. *See* Universal Description, Discovery, and Integration
Uniform Computer Information Transactions Act (UCITA), 269
United Kingdom
  Canadians warned of Toronto bombing plot by, 260
  Iraq war, relative openness of forces in, 69
  Jihadist presence on Internet, British intelligence attacks on, 259
  London subway bombings, 47, 196
  public surveillance devices, 196
United States
  DoD. *See* Department of Defense
  geospatial database thought experiment and. *See* geospatial database
  in Cold War. *See* Cold War
  Iraq war, relative openness of forces in, 69
  national identity system, thought experiment on. *See* national identity system
Universal Description, Discovery, and Integration (UDDI), 254
UNIX, 286–92
unmanned aerial vehicles (UAVs), 103–4, 162, 181, 250
updating and maintaining services online, 36, 104, 134, 242
use and storage, safety issues relative to, 99–100

Van Creveld, Martin, 112
Varian, Hal, 140
very small aperture terminals (VSATs), 103, 296
VHS, 278
videotape standards, 277–8
Vietnam War, 152
viruses and worms. *See also* specific viruses, e.g, Melissa virus
  evolution of, 18–19
  Microsoft security issues related to market dominance, 285–9
visualization technologies, 115
VSATs. *See* very small aperture terminals
vulnerability through intimacy. *See* intimacy and vulnerability

CAMBRIDGE

Cambridge University Press
978-0-521-87160-0 - Conquest in Cyberspace: National Security and Information Warfare
Martin C. Libicki
Index
More information

W3C (Worldwide Web Consortium), 204–5, 245
Wal-Mart, 157, 195, 223
warning systems, attacking, 83
Web. *See* Internet
Web Services Description Language (WSDL), 254
Webcams, 196
WebSphere program, IBM, 254
Well, The, 9
Whitney, Eli, 60
wholesale campaigns. *See also* retail conquest
  limitation of retail conquest by, 215
  measured using retail channels, 215–17
  spying or eavesdropping at level of, 193
Wi Fi, 36
Wi Max, 36
Windows operating system. *See* Microsoft; operating systems
wireless devices used to hack into closed systems, 77–8
wiretapping, 78
World Radio Conference, 5
World Trade Center attacks. *See* September 11, 2001, attacks
World War I, 214
World War II
  battleship silhouettes, proposed use of, 52
  D-Day invasions, deceptions regarding, 29, 53, 106
  effective weaponization of nuclear devices in, 96
  propaganda aimed at fielded forces, 210–11
  war plans planted on corpses, 88
World Wide Web. *See* Internet
Worldwide Web Consortium (W3C), 204–5, 245
worms and viruses. *See also* specific worms, e.g, Morris worm
  evolution of, 18–19
  Microsoft security issues related to market dominance, 285–9
WSDL (Web Services Description Language), 254

XML, 245–7, 254

Yahoo, 48, 205

Zarqawi, Abu Musab al, 216
Zawahiri, Ayman, 48

© Cambridge University Press www.cambridge.org