

# Index

- Access Control Server (ACS) 128
- Aerospace Surveillance and Battlespace Management (ASBM) (*see under* battlespace)
- Afghanistan 6, 66
- Aircraft 6, 20, 25, 41, 76, 109, 111, 119, 127, 134–35;
- Airborne Early Warning and Control (AEW&C) aircraft (including *Wedgetail*) 17, 25, 28, 124, 126;
- AP-3C *Orion* 23, 25;
- F/A-18 E/F *Super Hornet* 28;
- F/A-18 *Hornet* 21, 24, 28;
- F-35 Joint Strike Fighter (JSF) 28;
- Multi-role tanker transport (MRTT) 25, 28;
- Unmanned Aerial Vehicle (UAV) (including *Global Hawk*) 3, 6, 21, 25, 28, 41–42, 119, 121, 127, 132–36;
- Air Defence Ground Environment Simulator (ADGESIM) 124
- Air defence system (including *Vigilare*) 20, 27, 127, 136
- Air Warfare Destroyer (AWD) (*see under* Naval vessels)
- al-Qaeda 83(*n*16), 132, 135
- Alberts, David 38
- Arquilla, John 34
- Asia-Pacific Economic Cooperation (APEC) 104
- Association of South East Asian Nations (ASEAN) 123
- Australian Communications and Media Authority (ACMA) 108
- Australian Computer Emergency Response Team (*see under* Computer Emergency Response Team)
- Australian Defence Force (ADF) 1–3, 5–16, 18–21, 23–28, 34, 38–40, 53, 61–62, 81, 85–86, 90, 94, 103, 109, 112–13, 119–22, 124, 126, 131–33, 135, 137–38, 143–44
- Australian Defence Organisation (ADO) 33
- Australian Defence Satellite Communications Capability (ADSCC) (*see under* Satellite)
- Australian Federal Police (AFP) 104, 106–107, 122, 125
- Australian Government Computer Emergency Readiness Team (GovCERT.au) (*see under* Computer Emergency Response Team)
- Australian Government Information Management Office (AGIMO) 108
- Australian High Tech Crime Centre (AHTCC) 104, 125
- Australian Secret Intelligence Service (ASIS) 78, 125, 129 (*see also* intelligence agencies *under* Intelligence)
- Australian Security Intelligence Organisation (ASIO) 106, 122, 125, 166 (*see also* intelligence agencies *under* Intelligence)
- Battle Management System–Dismounted (BMS–D) 24
- Battle Management System–Mounted (BMS–M) 24
- battlespace 21–22, 26, 39, 111, 123–24;
- Aerospace Surveillance and Battlespace Management (ASBM) 22, 126;
- awareness in 5, 12–13, 16, 19, 25, 86, 119–20, 130, 133;
- Battlespace Communications System (Land) 25, 27;
- transparency in 14
- Boyd, John 82(*n*2), 83(*n*22)
- Canada 21, 82(*n*9)
- Capability Development Group 21–22, 27, 166
- Cartwright, James F. 42
- Central Intelligence Agency (CIA) 36, 132, 135, 138 (*see also* intelligence agencies *under* Intelligence)
- Chief Information Officer Group (CIOG) 17, 123
- Chief of Joint Operations (CJOPS) 138
- China (*see* People’s Republic of China)
- Coalition:
- networks 7, 9, 22–24, 26–27, 33, 109–110, 112–13;
- operations 2, 7–9, 15, 17, 26, 85;
- partners 9, 12, 83(*n*23), 87
- Combat Control System (CCS) 127
- Combat Information System (CIS) 127, 135–36
- command and control (C2) 3, 7–8, 18, 20, 119, 121, 133;
- capability 25–27, 75, 88–89;
- command, control, communications and intelligence (C3I) 41, 133–34;
- command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) 24, 39–40;
- Project *Redfin* 24, 28;

## Australia and Cyber-warfare

- command, control, communications, computers, intelligence, surveillance, reconnaissance and electronic warfare (C4ISREW) 22–23, 25–26, 59–60, 63, 65, 75, 81;
- grid 6, 16, 23, 124, 131;
- systems 1, 3, 11, 16–17, 21, 24, 26, 37, 44, 97, 111, 119, 121, 126, 132, 134, 139; (see also under Warfare)
- commercial off-the-shelf (COTS) 13, 64, 97, 110
- Common Relevant Operating Picture* (CROP) 12
- communications intelligence (COMINT) (see under Intelligence)
- Communications Sector Infrastructure
  - Assurance Advisory Group (CSIAAG) 106, 116(n100)
- Computer Emergency Response Team (CERT) 102–104, 126–27;
  - Australian Computer Emergency Response Team (AusCERT) 92, 103, 114(n18), 126;
  - Australian Government Computer Emergency Readiness Team (GovCERT.au) 103, 107
- Computer Networks 4, 39–46, 48–50, 54(n19), 57(n60), 57(n72), 61–62, 71, 73, 82(n14), 91, 93, 97, 99–101, 103, 106, 109, 123, 125–28, 132–35, 139–43;
  - Blackberry* blackout 82(n9);
  - Computer Network Attack (CNA) 43, 67, 82(n14), 109, 135, 138;
  - Computer Network Defence (CND) 21, 99, 138;
  - Computer Network Exploitation (CNE) 68, 82(n14);
  - Computer Network Operations (CNO) 43, 77–78, 80, 82(n14);
  - Computer Network Vulnerability Assessment Program 106–107
- Computers 19, 21, 35, 37, 39–40, 43–44, 47–50, 54(n19), 57(n60), 58(n80), 63, 70–72, 86, 93–94, 97, 100–101, 103, 107–108, 124, 139–42;
- 'botnets' 40, 48;
- Common Gateway Interface (CGI) 45, 56(n52);
- file types 39;
- Personal Computer (PC):
  - growth of 34, 101, 142;
  - security of 107, 111;
  - viruses affecting 93, 101, 142;
- pro forma* data codes 40–41, 127, 129, 143 (see also Computer Networks; cyber-crime; Internet)
- Connectivity 5, 7, 13, 16, 20–21, 23, 26, 36, 39, 47, 61, 63, 65, 67, 86–87, 95–99, 109, 113, 120, 133–36, 143
- Cosgrove, Peter 6, 17–18
- Council of Australian Governments (COAG) 116(n96)
- Critical Information Infrastructure (CII) (see under Infrastructure)
- critical infrastructure (see under Infrastructure)
- cyber-attack capability (see under Warfare)
- cyber-crime 3, 33, 47–49, 51–53, 57(n60), 72, 83(n19), 92–93, 103, 125, 140–41
- cyber-forensics 47, 57(n64)
- cyber-warfare (see under Warfare)
- Cyber-warfare Centre (see under Warfare)
- decision-to-act cycle 5, 14 (see also OODA loop)
- Defence Imagery and Geospatial Organisation (DIGO) 36
- Defence Information Infrastructure (DII) (see under Infrastructure)
- Defence Information Systems Communications Element (DISCE) 138
- Defence Intelligence Organisation (DIO) 77–78 (see also intelligence agencies under Intelligence)
- Defence Network Operations Centre (DNOC) 21, 138
- Defence Planning Guidance 10
- Defence Science and Technology Organisation (DSTO) 78, 124, 127, 133
- Defence Signals Directorate (DSD) 4, 61, 77–78, 108, 120, 122–23, 125–26, 137;
  - Information Security Group of 123 (see also information security)
- Delon, François 42
- Denial of Service (DS) 4, 44–45, 48, 73, 99–101, 103, 128, 132, 139, 142;
- Distributed Denial of Service (DDoS) 40, 45, 48–49, 107, 142 (see also malicious software)
- Department of Communications, Information Technology and the Arts (DCITA) 107–108
- Department of Foreign Affairs and Trade (DFAT) 77
- Department of Prime Minister and Cabinet (DPM&C) 4, 77, 137
- Director General Capability Plans (DGCP) 122
- Director General Integrated Capability Development (DGICD) 122

- doctrine 1, 3–4, 11–12, 14–16, 18, 20, 27–28, 40, 61, 119, 121, 124, 133–35, 142
- Domains 13, 23, 25, 27–28, 45–46;  
cognitive domain 13, 54(*n*19);  
information domain 13, 37, 63;  
Networked Coalition Domain 26;  
physical domain 8, 13
- E-Security Coordination Group (ESCG) 122
- E-Security Policy and Coordination (ESPaC) 107
- electro-magnetic spectrum 122–24 (*see also* electro-magnetic pulse weapon *under* Weapons)
- electronic countermeasures (ECM) 41, 124, 127, 134;  
electronic counter-countermeasures (ECCM) 124, 127  
(*see also* Electronic Warfare *under* Warfare)
- electronic order of battle (EOB) data 131, 134
- electronic support measures (ESM) 124, 134
- Electronic Warfare (EW) (*see under* Warfare)
- Electronic Warfare Operational Support Unit (EWOSU) (*see under* Warfare)
- Environmental Impact Statement (EIS) 52
- Erbium [Er]-Doped Fibre Amplifier (EDFA) 129
- Evans, Jonathan 42
- Federal Bureau of Investigation (FBI) 47, 138
- fibre-optics 50, 96, 99, 125;  
fibre-optic cables 20, 41, 62, 79–80, 94–95, 127, 129–30, 138
- Force 2020* 5–7, 15, 119–20, 130
- Future Joint Operating Concept (FJOC)* 7, 15
- Global Information Infrastructure (GII) (*see under* Infrastructure)
- Global Network Operations (GNO) 139
- Global Positioning System (GPS) 34
- Global System for Mobile Communications (GSMC) 123
- Google search engine (*see under* Internet)
- hackers, electronic warfare by (*see* hackers *under* Warfare)
- Headquarters Joint Operations Command (HQJOC) 28, 137–38
- high-frequency (HF):  
high-frequency interception 124;  
ultra high-frequency (UHF) 126, 138;  
very high-frequency (VHF) interception 124  
(*see also* radio frequency)
- high-power microwave (HPM) penetration techniques 134 (*see also under* Weapons)
- Hornet* aircraft (*see under* Aircraft)
- Houston, Angus 7
- human intelligence (HUMINT) (*see under* Intelligence)
- Hypertext Transfer Protocol (HTTP), flaw in 127–28
- imagery intelligence (IMINT) (*see under* Intelligence)
- Information Age 5, 38, 59, 95, 120, 122
- Information and Communication Technology (ICT) 5, 50–51
- Information Assurance (IA) 46, 64–66, 79, 86, 98–99, 110, 113
- information infrastructure (*see under* Infrastructure)
- information (open source) 9, 34–36 (*see also* Open Source Intelligence *under* Intelligence)
- Information Operations (IO) 1–4, 9–10, 60–61, 67, 76–77, 82(*n*3), 86, 120–21, 125, 128, 131–36, 139, 142–43
- information security (infosec) 17, 46–47, 52, 56(*n*56), 88–89, 96, 98, 113, 122–23
- Information Superiority and Support (IS&S) Concept 10, 13, 18–19, 113, 142;  
collect-connect-use-protect framework as basis of 13;  
decision support as key component of 19, 44, 124;  
persistent awareness as key component of 19;  
pervasive security as key component of 19;  
ubiquitous network as key component of 19
- Information Technology (IT) 17, 33, 36–41, 43, 46, 49, 51, 59–60, 77–78, 90, 92–93, 96, 98, 100, 104, 106–109, 125, 133, 135, 140–42;  
Information Technology Security Experts Advisory Group 106
- Information Warfare (IW) (*see under* Warfare)
- Infrastructure 2–3, 9–10, 15–16, 19, 21–23, 26, 28, 33, 38–39, 41, 43, 46–47, 50–53, 59–76, 78–81, 85–86, 88–89, 93–94, 99–100, 103–106, 108–110, 121, 124;

- Critical Information Infrastructure (CII) 3, 33, 47, 49–50, 53, 85, 113;  
critical infrastructure 47, 50–52, 66, 88–89, 94, 99, 104–108, 116(*n*96);  
    Critical Infrastructure Advisory Council (CIAC) 105–106, 116(*n*101);  
    Critical Infrastructure Protection (CIP) 50, 88, 104–106, 116(*n*96, *n*101);  
    Critical Infrastructure Protection Group (CIPG) 122;  
    definition of critical infrastructure 104;  
Defence Information Infrastructure (DII) 2, 27, 38, 61–65, 67–69, 77, 80–81;  
    definition of DII 62;  
Global Information Infrastructure (GII) 37, 51, 59, 61–65, 67–69, 77, 80–81;  
    definition of GII 62;  
information infrastructure 3, 10, 15–16, 33, 38–39, 43, 46, 50, 53, 59–73, 75–76, 78, 80–81, 82(*n*5), 85, 103, 113, 122, 128, 131;  
National Information Infrastructure (NII) 3, 38, 53, 61–65, 67–69, 77, 80–81, 103, 122, 125–26, 137;  
    definition of NII 61;  
Network Centric Warfare infrastructure 136;  
Trusted Information Infrastructure 85, 110–11, 113  
Integration 6, 9, 15, 17, 22, 26–27, 86, 89, 109–110, 119, 122, 124, 135;  
    sensor integration 12, 15–16, 37, 41–42  
(*see also* NCW Integration *under* Network Centric Warfare; *see* Office of Warfighting Integration *under* Warfighting)  
Intelligence 11–13, 21, 25, 27, 33–35, 64, 73–74, 77, 80–81, 87–88, 90, 97, 108, 111, 119, 121, 126, 130–31, 133–34, 137;  
communications intelligence (COMINT) 124, 136;  
human intelligence (HUMINT) 68, 78, 80;  
imagery intelligence (IMINT) 125, 131;  
intelligence agencies 42–43, 49, 51, 121–23, 125, 130–32, 138;  
Intelligence and Security Group (I&SG) 123;  
Intelligence, surveillance and reconnaissance (ISR) 76, 26, 124, 136;  
Open Source Intelligence (OSINT) 35, 124, 136;  
signals intelligence (SIGINT) 80, 123, 131, 136  
(*see also* intelligence-based warfare *under* Warfare)  
Intelligence and Security Group (I&SG) (*see under* Intelligence)  
Intelligence, surveillance and reconnaissance (ISR) (*see under* Intelligence)  
International Force East Timor (INTERFET) 124  
International Organization for Standardization (ISO) 46–47, 56(*n*56)  
International Telecommunications Union (ITU) 82(*n*1)  
Internet 34–36, 42–43, 45–50, 53, 58(*n*80), 60–62, 70, 72, 75, 77, 79, 83(*n*15, *n*20), 86–87, 91–99, 101–105, 112–13, 120, 124, 126, 128–30, 136, 138, 140;  
Google search engine 91, 128;  
Internet Exchange Point (IXP) 130;  
Internet Protocol (IP) 24, 49, 96, 126;  
    Non-classified Internet Protocol Router Network (NIPRN*e*T) 43;  
Internet Security System (ISS) 128;  
Internet Service Provider (ISP) 106, 108, 125;  
Internetwork Operating System (IOS) 128;  
Voice Over Internet Protocol (VOIP) 99, 129  
Intrusion Detection Systems (IDS) 44, 46, 49, 57(*n*72), 96, 102, 110  
Iraq conflict (2003–) 6, 72, 83(*n*23), 135  
Issue Motivated Group (IMG) 67, 69, 72–73  
Japan Defense Agency (JDA) 141, 147(*n*79)  
Jiabao, Premier Wen 42  
Jindalee Operational Radar Network (JORN) 20, 126  
Joint Functional Component Command:  
    Joint Functional Component Command for Network Warfare (JFCC-NW) 138–39;  
    Joint Functional Component Command for Space and Global Strike (JFCC-SGS) 139  
Joint Information Operations Warfare Center (JIOWC) 139  
Joint Strike Fighter (JSF) (*see under* Aircraft)  
Lasers 20, 99, 136 (*see also under* Weapons)  
Legislation 10, 48–49, 52, 55(*n*66), 56(*n*56), 57(*n*67), 90–91, 103, 135  
Libicki, Martin 37

- Local Area Network (LAN) 23, 96  
 Wireless Local Area Network (WLAN) 126
- Logistics 10, 12, 14–15, 21, 24–25, 60, 67, 74, 80, 92, 97, 109, 121, 126, 129, 134
- Lord, William 43
- malicious software (malware) 45, 48, 71, 73, 83(*n*21), 97, 100, 107–108;  
 computer virus 4, 39, 42, 44–45, 48, 53, 58(*n*80), 73, 77, 92–93, 96, 99–103, 109–110, 127–28, 132, 134, 139–42;  
 Trojan horse 4, 45, 48, 65, 77, 127–28, 132, 134, 139, 142;  
 worm 44–45, 48, 58(*n*80), 73, 77, 96, 99, 101, 127–28, 132, 134;  
     Blaster worm 101, 128;  
     Code Red worm 101, 128;  
     MyDoom worm 101, 128;  
     Myfip worm 39;  
     Santy worm 128;  
     Sasser worm 96;  
     Slammer worm 128;  
     SoBig worm 96, 101–102, 128;  
     Witty worm 128
- management:  
     access management 88–89, 110;  
     identity management 88–91, 106, 110, 113, 128;  
     risk/threat management 44, 82(*n*12), 88–89, 102, 104  
 (*see also under network*)
- Maritime Advanced SATCOM Terrestrial Infrastructure System (MASTIS) (*see under Satellite*)
- Maritime Tactical Wide Area Network (MTWAN) 23–24
- Merkel, Angela 42
- Multidimensional Manoeuvre (MDM) 7–8, 12, 16, 44
- National Counter-Terrorism Committee (NCTC) 88, 106, 116(*n*96)
- National Illicit Drug Strategy (NIDS) 125
- National Information Infrastructure (NII) (*see under Infrastructure*)
- National Intelligence Service (NIS) 141 (*see also Intelligence*)
- National Open Source Center (NOSC) 35–36
- National Security Agency (NSA) 138 (*see also intelligence agencies under Intelligence*)
- Naval Communications Area Master Station Australia (NAVCAMSAUS) 138
- Naval Communications Station Canberra (NAVCOMMSTA) 138
- Naval Network Warfare Command (NNWC) 139
- Naval vessels 4, 20, 41, 76, 124, 143;  
 Air Warfare Destroyer (AWD) 21, 24–25, 28, 119, 127;  
 ANZAC frigate 21, 24;  
 Canberra-class amphibious ships 26, 28
- network:  
     architecture of 2, 19–20, 26, 88, 96–97, 99, 110, 112, 127;  
     management of 17–44, 77, 88, 90, 96, 110;  
     Network Access Point (NAP) 130;  
     Network Admission Control (NAC) 128;  
     Network Operations Centre (NOC) 126;  
     robustness of 9, 11–12, 22, 26–27, 99, 109, 112–13, 137  
 (*see also Internet*)
- Network Centric Warfare (NCW) 1, 2, 5–8, 11–22, 26–28, 65, 85–86, 112–13, 120–24, 126–27, 130–32, 135–37, 143;  
 NCW Concept paper 7, 10–16, 120, 135;  
 NCW Integration 122–23;  
 NCW Roadmaps 2, 10, 15–18, 20, 22–23, 120, 123, 131, 135, 143;  
     milestones of 22–24, 26, 28, 30(*n*43), 120;  
     Roadmap Integration Plan 20;  
 Network Centric Warfare Project Office (NCWPO) 122–23;  
 priorities and benchmarks of 14–15  
 (*see also under Infrastructure; see also Warfare*)
- Networked Battle Group 22–24
- Networked Coalition Combat Force 23, 26
- networking 1, 3, 6–7, 12, 19–20, 24–27, 99, 108, 119, 121, 131–32, 136–37, 143
- New Zealand 21
- Non-classified Internet Protocol Router Network (NIPRNet) (*see under Internet*)
- Non-Governmental Organisation (NGO) 77, 85
- Nye, Joseph 35
- OODA loop (observe-orient-decide-act) 82(*n*2)
- Open Source Intelligence (OSINT) (*see under Intelligence*)
- Parakeet radio 20
- Pearl, Daniel 83(*n*15)

Australia and Cyber-warfare

- People's Liberation Army (*see under* People's Republic of China)
- People's Republic of China (PRC) 42–43, 76, 82(*n1*, *n11*), 139–40;  
People's Liberation Army (PLA) 43, 139
- Personal Computer (*see under* Computers)
- Personal Digital Assistant (PDA) 60, 110
- Personal Identification Number (PIN) code 106, 125
- Product Security Incident Response Team (PSIRT) 126
- psychological operation (*psyop*) 59, 67, 74–75, 77–78, 80–81, 95 (*see also* psychological warfare *under* Warfare)
- Public Key Infrastructure (PKI) 110
- radio frequency (RF) 126 (*see also* high-frequency; *see also under* Weapons)
- Rapid Prototyping and Development (RPD) 15–16, 18;  
Rapid Prototyping, Development and Evaluation (RPDE) 18, 20, 27 (*see also* *NCW Roadmaps under* Network Centric Warfare)
- Remberg, Hans Elmar 42
- research and development (R&D) 27–28, 46, 104, 106, 125–28
- Revolution in Military Affairs (RMA) 138
- Ronfeldt, David 34
- Royal Australian Air Force (RAAF) 20, 119, 124
- Royal Australian Navy (RAN) 20, 119, 130, 138
- Rules of Engagement (ROE) 3, 78, 121, 134–35
- Satellite 7, 20, 27, 36, 38, 41, 50, 61–63, 74, 78, 80, 95, 123, 129–30, 136, 138, 140;  
Australian Defence Satellite Communications Capability (ADSCC) 138;  
Maritime Advanced SATCOM Terrestrial Infrastructure System (MASTIS) 23;  
Optus satellite 17, 126;  
*Palapa* satellite system 123;  
*Rhyolite* geostationary SIGINT satellite 136;  
satellite communications 17, 20–21, 25, 27, 41, 119, 123, 127, 134;  
satellite telephone (Satphone) 123
- Security Impact Statement (SIS) 52
- Short Message Service (SMS) 75, 125
- signals intelligence (SIGINT) (*see under* Intelligence)
- situational awareness 6, 19–21, 128, 131, 143;  
shared situational awareness 7, 11–14, 16, 26, 120, 124, 131, 143
- Small-to-Medium Enterprise (SME) 107–108
- Special Air Services Regiment (SASR) 24
- Special Operations Command (SOCOMD) 24
- Standard Defence Supply System (SDSS) 25
- Subscriber Identity Module (SIM) 70, 120
- Supervisory Control and Data Acquisition (SCADA) 95–96
- Synchronisation 7, 9, 12–14, 21, 27–28, 38, 86;  
Synchronous Optical Network (SONET) 130
- Szafranski, Dick 37
- Toffler, Alvin and Heidi 34
- training and education 9, 11–12, 14–16, 18, 20, 27–28, 35–36, 39, 46–47, 60, 70, 93, 100, 110, 112, 140
- Trusted Information Sharing Network (TISN) 105–106, 116(*n96*) (*see also* Trusted Information Infrastructure *under* Infrastructure)
- Tzu, Sun 37
- ultra high-frequency (UHF) (*see under* high-frequency)
- ultra-wide band (UWB) weapon (*see under* Weapons)
- Uniform Resource Locator (URL) 45, 56(*n51*)
- uninterrupted power systems (UPS) 63
- United Kingdom 21, 42
- United Nations Security Council (UNSC) 142
- United States 2, 20–21, 27, 42–43, 49, 65, 82(*n9*), 85, 88–89, 91–94, 126, 138–39, 141;  
Oak Ridge, TN 42;  
terrorist attacks of 11 September 2001 on 66, 85, 93;  
US Commerce Department 42;  
US Congress 19, 35, 42–43;  
US Department of Defense 42, 49, 62, 98, 139;  
US Department of Homeland Security 42–43, 104, 138;  
US National Intelligence Council 35;  
US Pentagon 43, 135;  
US State Department 42;  
US Strategic Command (USSTRATCOM) 42, 138

- Unmanned Aerial Vehicle (UAV) (*see under*  
Aircraft)
- very high-frequency (VHF) interception (*see*  
*under* high-frequency)
- Voice Over Internet Protocol (VOIP) (*see under*  
Internet)
- Waltz, Ed 5, 33, 37–38, 54(*n*19), 102
- 'war on terror' 2, 120, 132
- Warfare:
- command and control warfare 34, 37–38,  
41;
  - cyber-attack capability 42–43, 72, 75, 93,  
112;
  - cyber-warfare 1, 3–4, 43, 55, 99, 108, 121,  
123–26, 128, 130, 132–44;
  - Cyber-warfare Centre 4, 10, 36, 112–13,  
119–22, 127–30, 132–34, 136–38, 142–44;
  - economic information warfare 38;
  - Electronic Warfare (EW) 1, 25, 37, 41,  
124, 139–40;  
*Bunyip* 25;
  - Electronic Warfare Operational Support  
Unit (EWOSU) 124;
  - hackers 37, 42, 44, 51, 53, 58(*n*80), 73, 93,  
95–96, 99, 101, 133, 140–41;
  - Information Warfare (IW) 1–4, 10, 33,  
36–40, 46, 51, 53, 54(*n*19), 55(*n*28),  
119–20, 124, 131–35, 139–43;
  - intelligence-based warfare 37;
  - psychological warfare 37, 59, 67–70,  
74–75, 142
- Warfighting 7–8, 10–12, 14, 16–18, 20–21, 24,  
26, 37, 60, 67, 74, 76, 120;  
Office of Warfighting Integration (USAF)  
43
- Weapons 2, 6, 33–34, 37, 40–41, 63, 76, 78,  
93, 97, 103, 131;
- electro-magnetic pulse weapon 40;
  - laser weapon 41, 78;
  - radio frequency weapon 41;
  - high-power microwave weapon 41;
  - ultra-wide band weapon 41;
- weapon systems 4, 6, 17, 21, 40, 124, 127,  
131, 142
- whole-of-government approach 8, 26, 34, 36,  
85, 107, 111
- whole-of-nation approach 2, 7, 10, 111
- wireless application protocol (WAP) 41, 127
- Wireless Local Area Network (WLAN) (*see*  
*under* Local Area Network)
- World Wide Web (*see* Internet)