Computer Security - December 2001

Africa and Africa Command - 02/2008 Air and Space Power - 09/2007 Aleutian Campaign - 01/2000 Amphibious and Littoral Warfare - 05/2002 Arab-Israeli War, 1967 - 07/2002 Asymmetric Warfare - 01/2002 Battle of Britain - 07/2002 Battlespace Management - 11/2001 Civilian Control of the Military - 07/2005 Commander's Estimate - 12/2001 Computer Security/Network Defense - 12/2001 Consequence Management - 12/2001 Drug Interdiction - 02/2002 Effects Based Operations - 11/2005 End State - 09/2000 Ethics - 04/2001 Falkland Islands War - 11/2001 The Fog of War - 02/2002 Force Protection - 12/2001 Gallipoli - 06/2002 Gettysburg - 07/2004 Global War on Terrorism - 12/2006 Homeland Defense - 01/2002 India-Pakistan Relations - 01/2000 Information Warfare - 01/2002 Interagency Coordination - 06/2007 The Joint Task Force - 05/2003 Kosovo/Allied Force - 12/2001 Leyte Gulf, Battle of, 1944 - 07/2002 Military-Media Relations - 04/2004 Non-Lethal Weapons - 01/2002 Noncombatant Evacuation Operations - 11/2000 Operation Anaconda - 05/2005 Operation Desert Fox - 01/2002 Operation Eagle Claw (Desert One) - 11/2002 Operation Earnest Will - 08/2007 Operation Enduring Freedom - 08/2003 Operation Iraqi Freedom - 09/2003 Operation Torch - 04/2004 Operation Uphold Democracy - 05/2004 Operation Urgent Fury - 01/2002 Posse Comitatus - 01/2002 Space Warfare - 01/2002 United States Force Transformation - 08/2005 Urban Warfare - 01/2002 Vicksburg Campaign, 1863 - 11/2000 Weapons of Mass Destruction - 05/2002 Women, Then and Now - 03/2008 Women in the Armed Services - 03/2005 Yorktown-Seige, 1781 - 01/2000

- Books And Documents
- Periodicals
- Doctrine
- Laws
- Electronic Resources

BOOKS AND DOCUMENTS

Q 180 .A1 R36 CF151 1999
Anderson, Robert H.Research and Development Initiatives Focused on Preventing, Detecting, and Responding to Insider Misuse of Critical Defense Information Systems: Results of a Three-Day Workshop. Santa Monica, CA: Rand, 1999.

Q 180 .A1 R36 CF163 2000
----------.Research on Mitigating the Insider Threat to Information Systems--#2; Proceedings of a Workshop Held in August, 2000. Santa Monica, CA:Rand, 2000.

Q 180 .A1 R36 MR993 1999
----------.Securing the U.S. Defense Information Infrastructure: A Proposed Approach.Santa Monica, CA:Rand, 1999.

U 163 .B282 1996
Barac, Gregory G.Interoperability: The Cornerstone of Information Warfare.Carlisle Barracks, PA:Army War College, 1996.

QA 76.9 .A25 B48 2000
Berkowitz, Bruce D. and Allan E. Goodman. Best Truth:Intelligence and Security in the Information Age. New Haven:Yale University Press, 2000.

U 163 .B388 2001
Best, Carole N.Computer Network Defense and Attack:Information Warfare in the Department of Defense. Carlisle Barracks, PA:Army War College, 2001.

QA 76.9 .A25 C92 1998
CSIS Global Organized Crime Project. Cybercrime-Cyberterrorism-Cyberwarfare: Averting an Electronic Waterloo. Washington:CSIS Press, 1998.

TK 5105.59 .D254 2001
Daigle, Richard C.An Analysis of the Computer and Network Attack Taxonomy. Wright-Patterson AFB, OH: Air Force Institute of Technology, 2001.

MF/AD A372 298
Dhillon, Joe.The Legal Limitations on Defending the National Information

Infrastructure against a Cyber Attack.Houston, TX:Houston University, 1999.

U 163 .F67 1999
Forno, Richard and Ronald Baklarz. The Art of Information Warfare: Insight into the Knowledge Warrior Philosophy. Parkland, FL: Universal Publishers, 1999.

QA 76.9 .A25 H355 1997
Hall, Larry P.National Military Strategy:Information Warfare.Carlisle Barracks, PA:Army War College, 1997.

TK 5105.59 .H387 2001
Hernandez, Ernest D.Using Operational Risk Management (ORM) to Improve Computer Network Defense (CND) Performance in the Department of the Navy (DON). Monterey, CA:Naval Postgraduate School, 2001.

CRS Report RL30735
Hildreth, Steven A.Cyberwarfare. Washington: Congressional Research Service, 2000.

Q 180 .A1 R36 P7988 1996
Hundley, Richard O. and Robert H. Anderson. A Qualitative Methodology for the Assessment of Cyberspace-Related Risks.Santa Monica, CA:Rand, 1996.

Q 180 .A1 R36 P7893 1994
----------.Security in Cyberspace:An Emerging Challenge for Society.Santa Monica, CA:Rand, 1994.

TK 5105.875 .I57 K633 1997
Koba, Michael G.Express Lanes and Potholes of the Information Superhighway: The Internet and the Operational Planner. Fort Leavenworth, KS: School of Advanced Military Studies, Army Command and General Staff College, 1997.

QA 76.9 .A25 L49 2001
Levy, Steven.Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age. New York:Viking, 2001.

U 163 .M36 1999
McKeown, Wendell B.Information Operations:Countering the Asymmetric Threat to the United States. Carlisle Barracks, PA: Army War College, 1999.

UB 212 .M62 1997
Mobery, Gloria Dyer.Operational Protection of C4I.Newport, RI:Naval War College, 1997.

CRS Report 98675STM
Moteff, John.Critical Infrastructures:A Primer. Washington: Congressional Research Service, 1998.

U 163 .C982 1999
Nelson, Bill.Cyberterror: Prospects and Implications. Monterey, CA: Center for the Study of Terrorism and Irregular Warfare, 1999.

CRS Issue Brief IB96039
Nunno, Richard M.Encryption Technology:Congressional Issues.Washington: Congressional Research Service, 2000.

U 163 .P297 1999
Payne, Allan D.The Impact of Computer Network Attacks on Infrastructure Centers of Gravity. Carlisle Barracks, PA: Army War College, 1999.

QA 76.9 .A25 S354 1994
Schwartau, Winn.Information Warfare:Chaos on the Electronic Highway.New York:Thunder's Mouth Press, 1994.

QA 76.9 .A25 S354 1996
----------.Information Warfare:Cyberterrorism—Protecting Your Personal Security in the Electronic Age. New York: Thunder's Mouth Press, 1996.

U 163 .T56 1997
Thompson, Michael J.Information Warfare—Who Is Responsible?:Coordinating the

Protection of Our National Information Infrastructure. Carlisle Barracks, PA: Army War College, 1997.

QA 76.9 .A25 U75 2000
U.S. Congress.House. Committee on Government Reform. Computer Security: Are We Prepared for Cyberwar? Hearing…106th Congress, 2nd Session.Washington: GPO, 2000.

U 163 .U754 2001
----------.Computer Security:Cyber Attacks—War without Borders.Hearing… 106th Congress, 2nd Session. Washington: GPO, 2000.

QA 76.9 A25 U7 2001
----------.Enhancing Computer Security:What Tools Work Best.Hearing…

106th Congress, 2nd Session. Washington: GPO, 2001.

JC 596.2 U5 U75 1998
U.S. Congress.House. Committee on International Relations.Encryption: Individual Right to Privacy Vs. National Security. Hearing…105th Congress, 1st Session.Washington: GPO, 1998.

JX 1706.25 U7 2001
----------.Oversight of the State Department:Technology Modernization and Computer Security. Hearing…106th Congress, 2nd Session. Washington: GPO, 2000.

QA 76.9 .A25 U753 2000
U.S. Congress.Senate. Committee on Appropriations. Cybercrime. Hearing… 106th Congress, 2nd Session. Washington: GPO, 2000.

Y 4 .C 73/7: S.HRG. 105-1068 (MF)
U.S. Congress.Senate. Committee on Commerce, Science and Transportation.Subcommittee on Science, Technology, and Space. Computer Security in the Federal Government. Hearing…105th Congress, 2nd Session.Washington: GPO, 1998.

QA 76.9 .A25 U745 2000
U.S. Congress.Senate. Committee on Governmental Affairs.Cyber Attack: Is the Government Safe? Hearing…106th Congress, 2nd Session. Washington: GPO, 2000.

Y 4 .G 74/9: S.HRG. 105-614 (MF)
----------.Cyber Attack [microform]:Is the Nation at Risk?Hearing…105th Congress, 2ndSession. Washington:GPO, 1998.

Y 4 .J 89/2: S.HRG. 105-447 (MF)
U.S. Congress.Senate. Committee on the Judiciary. The Nation at Risk [microform]:Report of the President's Commission on Critical Infrastructure Protection. Hearing…105th Congress, 1st Session.Washington: GPO, 1998.

QA 76.9 .A25 P822 2000
U.S. Critical Infrastructure Assurance Office. Practices for Securing Critical Information Assets.Washington: Critical Infrastructure Assurance Office, 2000.

U 163 .R47 1996
U.S. Defense Science Board.Report of the Defense Science Board Task Force on Information Warfare—Defense (IW-D).Washington: Office of the Undersecretary of Defense for Acquisition & Technology, 1996.

UB 247 .U55 1999
U.S. Dept. of Defense.Premises for Policy:Maintaining Military Superiority in the 21st Century, 1999 Final Report. Washington: Strategic Studies Group IV, 1999.

GAO-01-1005T
U.S. General Accounting Office.Critical Infrastructure Protection:Significant

Challenges in Developing Analysis, Warning, and Response Capabilities. Washington: GAO, 2001.

GAO-01-323
----------.Critical Infrastructure Protection:Significant Challenges in Developing National Capabilities. Washington:GAO, 2001.

GAO-01-1132T
----------.Critical Infrastructure Protection:Significant Challenges in Protecting Federal Systems and Developing Analysis and Warning Capabilities.Washington: GAO, 2001.

GAO-01-1168T
U.S. General Accounting Office.Critical Infrastructure Protection:Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks. Washington:GAO, 2001.

GAO/AIMD-99-107
----------.DOD Information Security:Serious Weaknesses Continue to Place Defense Operations at Risk. Washington: GAO, 1999.

GAO-01-341
----------.Information Security:Challenges to Improving DOD's Incident Response Capabilities. Washington: GAO, 2001.

QA 76.9 .A25 U556 1997
U.S. President's Commission on Critical Infrastructure. Critical Foundations: Protecting America's Infrastructures:The Report of the President's Commission on Critical Infrastructure Protection. Washington: GPO, 1997.

TK 5105.59 .U758 1999
U.S. Space Command.United States Space Command (USSPACECOM). Concept of Operations (CONOPS) for Computer Network Defense (CND). Peterson AFB, CO: Space Command, 1999.

U 163 .W23 1996
Ward, Thomas E.Information Warfare:Is It Feasible?: Desirable? Carlisle Barracks, PA:Army War College, 1996.

U 163 .W566 2000
Williamitis, Gregory M.Implementing the National Security Strategy of Critical Infrastructure Protection. Carlisle Barracks, PA: Army War College, 2000.

▲TOP

PERIODICALS

Ackerman, Robert K."Computer Security Experts Warn of Growing System Vulnerabilities." Signal, vol. 54, no. 12, Aug. 2000, pp. 17-18 +.

Adams, James H."Virtual Defense."Foreign Affairs, vol. 80, no. 3, May/June 2001, pp. 98-112.

Arquilla, John, et al."Information-Age Terrorism."Current History, vol. 99, no. 636, Apr. 2000, pp. 179-185.

Baker, Duffy."Pentagon Endorses Biometrics to Enhance Computer Security." National Defense, vol. 85, no. 571, June 2001, pp. 30-31.

Bayles, William J."The Ethics of Computer Network Attack." Parameters, vol. 31, no. 1, Spring 2001, pp. 44-58.

Biros, David P."Human Element Key to Intrusion Detection." Signal, vol. 55, no. 12, Aug. 2001, pp. 31-33.

Dean, Joshua."Risking it."Government Executive, vol. 33, no. 5, Apr. 2001, pp. 28-30 +.

DeMattei, Lou Anne."Developing a Strategic Warning Capability for Information Defense." Defense Intelligence Journal, vol. 7, no. 2, Fall 1998, pp. 81-121.

Forester, Anthony."On Hackers, Crackers, and Phreakers." Jane's Intelligence Review, vol. 11, no. 1, Jan. 1999, pp. 50-54.

Hankins, Michelle L."Layered Approach Security Planning Offers Best Defense against Attacks." Signal, vol. 54, no. 8, Apr. 2000, pp. 55-56.

Hunker, Jeffrey A."Critical Infrastructure Protection."Low Intensity Conflict & Law Enforcement, vol. 7, no. 3, Winter 1998, pp. 151-157.

Isenberg, David."Electronic Pearl Harbor?"National Security Studies Quarterly, vol. 6, no. 4, Autumn 2000, pp. 95-110.

James, Leah."Organised Exploitation of the Information Super-Highway." Jane's Intelligence Review, vol. 12, no. 17, July 2000, pp. 52-55.

Kenyon, Henry S."Internet-Based Attack Risk Distracts Organizations from Internal Trouble." Signal, vol. 54, no. 12, Aug. 2000, pp. 25-26 +.

----------."New Tricks for Old Threats."Signal, vol. 55, no. 5, Jan. 2001, pp. 43-44 +.

Mann, Paul."Cyber Security Plan Called Underfunded." Aviation Week & Space Technology, vol. 152, no. 8, Feb. 2000, p. 111.

----------."White House Pushes Cyber Security Hike."Aviation Week & Space Technology, vol. 153, no. 3, Jan. 2000, pp. 412-413.

Mathonniere, Julien."Educating RITA to Outwit the Hackers in Security War." Jane's Defence Weekly, vol. 33, no. 17, Apr. 26, 2000, pp. 36-38.

Myers, Richard B."New Missions for Space Command."Air Force Magazine, vol. 83, no. 3, Mar. 2000, pp. 77-79.

Post, Jerrold M., et al."From Car Bombs to Logic Bombs:The Growing Threat from Information Terrorism." Terrorism and Political Violence, vol. 12, no. 2, Summer 2000, pp. 97-122.

Robinson, Clarence A., Jr."Geeks in the Wire."Journal of Electronic Defense, vol. 23, no. 10, Oct. 2000, pp. 47-51.

Sheehy, Christian B."Intrusion Detection Technology Closes in on Hackers." Signal, vol. 54, no. 12, Aug. 2000, pp. 21-22 +.

----------."Insider Cybercrime Finds No Place to Hide." Signal, vol. 55, no. 6, Feb. 2001, pp. 57-60.

----------."Space Warriors Defend Information Assets: Initiative Puts Information Security and Reliability First." Signal, vol. 55, no. 8, Apr. 2001, pp. 29-31.

Valeri, Lorenzo."Securing Internet Society:Toward an International Regime for Information Assurance." Studies in Conflict & Terrorism, vol. 23, no. 2, Apr.-June 2000, pp. 129-146.

"White Paper:The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63."Low Intensity Conflict & Law Enforcement, vol. 7, no. 3, Winter 1998, pp. 136-150.

▲TOP

DOCTRINE

Dept. of Defense Directive 5200.28. Security Requirements for Automated Information Systems (AISs). Mar. 21, 1988.

Dept. of Defense Directive 5215.1. Computer Security Evaluation Center.

Oct. 25, 1982.

Dept. of Defense Directive 5215.2. Computer Security Technical Vulnerability Reporting Program (CSTVRP). Sept. 2, 1986.

Dept. of Defense Instruction 5200.40. DOD Information Technology Security Certification and Accreditation Process (DITSCAP). Dec. 30, 1997.

Dept. of Defense Manual 5200.28-M. ADP Security Manual. Jan. 1973.

Dept. of Defense Manual 5220.22-M. National Industrial Security Program—Operating Manual, Chapter 8—Information System Security. May 1, 2000.

Joint Pub 3-13.Joint Doctrine for Information Operations. Oct. 9, 1998. Joint Pub 3-51.Joint Doctrine for Electronic Warfare. Apr. 7, 2000.

TOP

LAWS

Computer Security Act of 1987 . Pub. L. 100-235. Jan. 8, 1988.On-Line. Available at: **http://www.house.gov/science_democrats/archive/compsec1.htm**

Critical Infrastructure Protection .EO 13010. July 17, 1996. On-Line. Available at: **http://www.ciao.gov/pccip/eo13010.pdf**

Critical Infrastructure Protection in the Information Age .EO 13231.Oct. 16, 2001. On-Line. Available at: **http://www.ciao.gov/News/EoonCriticalInfrastructureProtection101601.html**

TOP

ELECTRONIC RESOURCES

ANSER, Inc.ANSER Institute for Homeland Security.On-Line. Dec. 2001. Available at: **http://www.homelandsecurity.org**

Cilluffo, Frank J."Cyber Attack:The National Protection Plan and Its Privacy Implications." Nov. 7, 2001. On-Line. Journal of Homeland Security. Nov. 2000. Available at: **http://www.homelandsecurity.org/journal/Articles/Cilluffo.htm**

Critical Infrastructure Assurance Office. On-Line.Nov. 7, 2001.Available at : **http://www.ciao.gov/index.htm**

Federal Computer Incident Response Center (FedCIRC). On-Line. Oct. 2001. Available at: **http://www.fedcirc.gov**

Garamone, Jim."Center Works to Protect Communications Infrastructure." Nov. 7, 2001. On-Line. Defenselink. Nov. 11, 2001.Available at: **http://www.defenselink.mil/news/Nov2001/n11072001_200111072.html** (Other documents on computer security and network defense can be found at the Defenselink website: **http://www.defenselink.mil** Type your keywords in the SEARCH box.)

GovExec.com."Special Report:Computer Security." On-Line. Government Executive Magazine. Nov. 2001. Available at: **http://www.govex.com/computersecurity/index.htm**

Houle, Kevin J. and George M. Weaver. "Trends in Denial of Service Attack Technology." Oct. 2001. On-Line. CERT Coordination Center. Nov. 7, 2001. Available at: **http://www.cert.org/nav/index_main.html**

INFOSYSSEC.On-Line. Nov. 11, 2001. Available at: **http://www.infosyssec.com**

Lacombe, Phil and David Keyes."Defending the American Homeland's

Infrastructure." Nov. 7, 2001. On-Line.Journal of Homeland Security.Oct. 27, 2000. Available at: **http://www.homelandsecurity.org/journal/Articles/Lacombe.doc**

National Infrastructure Protection Center. On-Line.Nov. 7, 2001.Available at: **http://www.nipc.gov**

Additional information on computer security/network defense can be found by searching other library electronic resources. These can be found as icons on the desktop or within the icon entitled Library Resources:

- **EBSCOhost**
- Lexis-Nexis
- Proquest Direct
- Scientific and Technical Information Network (STINET)

Also, refer to JFSC bibliography on Information Warfare.

TOP

Please see a librarian for assistance in searching the electronic resources found in the library.

Prepared by Reference Librarian