CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

Directive current as of 31 March 2010

J-6 CJCSI 6504.01
DISTRIBUTION: A, B, C, J, S 1 April 2010

INFORMATION ASSURANCE (IA) AND COMPUTER NETWORK OPERATIONS (CNO)

References: "DOD Dictionary of Military and Associated Terms" as amended through 31 October 2009.

1. Purpose. To provide joint policy and guidance for IA and CNO activities in accordance with (IAW) references made in JP 1-02, 12 April 2001 "DOD Dictionary of Military and Associated Terms" as amended through 31 October 2009.

2. Cancellation. CJCSI 6510.01D, 15 June 2004, "Common Definitions for Assurance (IA) and Computer Network Defense (CND)" is canceled.

3. Applicability. This instruction applies to the Joint Staff, combatant commands, Services, Defense agencies, Department of Defense field activities, joint activities, and the United States Coast Guard.

4. Policy. Enclosure A. (original)

5. Definitions. See Glossary. Major source documents for definitions in this instruction are Joint Publication (JP) 1-02, "DOD Dictionary of Military and Associated Terms," (reference a) and Committee on National Security Systems (CNSS) Instruction (CNSSI) No. 4009, "National Information Assurance Glossary" (reference b).

6. Responsibilities. Enclosures B and C. (original)

7. Summary of Changes

a. Identifies current IA and CNO terminologies IAW OAFP guidance.

b. Provides current approved definition for IA and CNO terminologies for use across all JCAS JP documents as of 1 April 2010.

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other Federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page-- http://www.dtic.mil/cjcs_directives.

9. Effective Date. This instruction is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:

WALTER L. SHARPE
Lieutenant General, USA
Director, Joint Staff

DISTRIBUTION

Distribution A, B, C, J and S plus the following:

	Copies
Commandant of the Coast Guard	5

LIST OF EFFECTIVE REFERENCED PAGES

The following is a list of referenced pages for CJCSI 6504.01. Use this list to verify the currency and completeness of the original document.

Pages 31-43 inclusive, plus Appendixes A and F.

1) Strike previous and replace with current "Cyberspace Warfare (Definitions)"

2) Strike reference to previous terms and update throughout publication.

3) No other corrections or changes specified or authorized under this instruction.

4) Contact publication POCs (page 11) for further information or requested/recommended updates.

SUMMARY OF CHANGES

For inclusion in CJCSI 6504.01 pages 31-43 inclusive, as appropriate and indicated, plus Appendixes A and F. Use this list to verify the currency and completeness of the document. An "O" indicates no change in terminology from the original document.

Inserted Section Title: "**Cyberspace Warfare (Definitions)"**

Computer Network Attack (O)

Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA.

Computer Network Defense (O)

Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks. Also called CND.

Computer Network Exploitation (O)

Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.

Computer Network Operations (O)

Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. Also called CNO. See also computer network attack; computer network defense; computer network exploitation.

Controlled Information (O)

Information conveyed to an adversary in a deception operation to evoke desired appreciations

Cyberspace (O)

A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Cyberspace Operations (O)

The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid.

Cyberdeterrence

The act of establishing an operational, cultural, technical, or doctrinal environment that deters qualified cyberwarriors from willing and sustained participation in support of friendly cyberwarfare operations.

Cyberforce protection

Actions applied within a virtual or entirely notional environment to protect friendly personnel and cyber assets from their worst fears and nightmares; correlates with the equally ignored, misrepresented, and misunderstood methods of traditional force protection.

Cyberwar

War using cyberspace operations to achieve sensational yet bloodless results for friendly forces while seeking to inflict massive inconvenience on the adversary in a manner that offers the most photogenic and telegenic depiction for domestic and international public audiences.

Cyberfoxhole

Virtual haven within the electromagnetic spectrum for cyber-combatants to seek refuge from hostilities and replenish their individual and/or unit manna levels.

Cyberterrorism

Term used by information optics elements and/or cyberexperts to describe malicious acts in cyberspace to the uninformed and/or general public. See also Information Optics Element; EFUD; cyberexperts.

Cyberbull

This document. And much of the sensational Washington, DC hype regarding cyberwarfare and cybersecurity made by those who don't have a clue about its realities, ramifications, viability, or effectiveness. See also EFUD.

Cyberexpert

Non-combatant indigenous person able to influence local media outlets and national decision-makers despite having no formal training or holding any relevant or significant operational or analytical experience in the cyberwarfare domain, frequently for the purpose of near-term personal or organizational fiduciary gain at the long-term expense of others. See also deception; EFUD.

Cybersecurity

A noble and elusive, though generally unattainable, reactionary or overly-preemptive process that seeks to deploy friendly and/or allied cyberwar assets to provide total cyber-force protection against any and all adversary threats.

Cyberwarrior

Uniformed and non-uniformed personnel of the Department of Defense, civilian resources, and other government agencies (OGA) conducting full-spectrum cyberwarfare operations.

Cynade

(1) Localized man-portable area-of-effect cyber weapon likely able to resist attribution for its initiator(s). (2) What cyberwarriors consume during prolonged cyber spatial operations to maintain alertness and peak cybering efficiency.

Cymoke

Localized area-of-effect deception capability that can prevent adversarial identification and attribution of friendly forces within the cyber area of operations.

CYCOM

A unified strategic or service operational organizational command of all assigned subordinate cyberwarfare assets intended to transform the conduct of cyberwar from the unconventional realm where it belongs into the conventional realm favored by existing senior leaders, command relationships, organizational culture, and budgeting processes.

CyberTOW

Directed wire-guided crew-served cyber spatial electromagnetic projectile weapon used to disrupt or destroy large mobile attacking cyber units.

CyOps

The collective groupthink present when conducting cyberwarfare planning or analysis resulting from advice from Cyberexperts. See Cyberexpert; EFUD. Not to be confused with psychological operations (PSYOP) although there may be similarities in outcomes.

Deception (O)

Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce the enemy to react in a manner prejudicial to the enemy's interests. See also social engineering; controlled information.

Digital Pearl Harbor

A website in the PACFLT AOR.

Epunji

Camouflaged cyber spatial trap designed to ensnare intruders penetrating friendly cyberspace perimeters.

eSnipe

Precision long-range ranting attacks against cyber spatial assets. Also called trolling by civilian Internet users.

EFUD

Executive Fear, Uncertainty, and Doubt. Information distributed to senior commanders, policymakers, civilian populations, and other friendly or allied assets during cyberwar briefings and planning. See also cyberexpert; deception; information optics element.

Information Operations (O)

The planning and integrated employment of capabilities in the information environment across the spectrum of military operations. Also called IO. See also computer network operations; deception.

Information Optics Element

The elements of headquarters staff, including civilian assets, assigned to conduct higher echelon briefing and outreach activities in support of Operational Cyber Detachments during both combat and non-combat operations. Also called IOE. See also controlled information; social engineering; deception; EFUD; PowerPoint Ranger Team.

Net Porn

The primary information resource transiting the cyber spatial domain and something that must not have its flow disrupted, degraded, or denied to allied forces by adversaries, foreign governments, or friendly commanders.

Network-Centric Warfare (O)

The use of computers and communications to link people through information flows that depend on the interoperability of systems used by all U.S. armed forces. NCW involves collaboration and sharing of information to ensure that all appropriate assets can be quickly brought to bear by commanders during combat operations

Nitwit-Centric Warfare

The eventual outcome of improperly planned or executed NCW.

Operational Cyber Detachment – Alpha

The basic military unit organization of DOD cyberwarfare capabilities.

Operational Cyber Detachment – Bravo

The military elements of combat service and support assigned to forward cyberwarfare units.

Operational Cyber Detachment – Charlie

The requisite civilian contractor elements of combat service and support assigned to both forward and rear-area cyberwarfare units.

Perception Management (O)

Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning as well as to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations. See also psychological operations.

Post Traumatic Cyber Disorder

Diagnosed condition found in cyberwarriors when experiencing networkus interruptus. See also nitwit-centric warfare; net porn. (Reference OSD/HA Memorandum "Post Traumatic Cyber Disorder" dated 1 April 2010.)

PowerPoint Ranger Team

The military elements of headquarters staff assigned to higher echelon briefing and outreach support of Operational Cyber Detachments during both combat and non-combat operations. See also controlled information; social engineering; deception; EFUD; information optics element.

Psychological Operations (O)

Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP. See also controlled information; deception.

Social Engineering

See Deception. Or this document.

Weapon of Mass Disruption

Any cyber strike that disrupts, degrades, or denies friendly cyber assets regardless of how those assets are used. See cyberwar; net porn.

STAFF COORDINATION CONTACT

OPR:	BG April Feulz, USAF (J-6/41) 4E2401
CJCS Staff Coordination:	COL Gat Cha, USA (J-6/41) 4E2401
DOD/OAFP Development:	Mr. Richard Forno @ INFOWARRIOR.ORG (Office of April Fools' Pranking) rforno@infowarrior.org

DOD/OAFP COMMENT

Cyberwarfare indeed is a concern that must be addressed responsibly; however there is such a cacophony of 'noise' in public and private discourse on the subject that it is difficult for many to make sense of the actual cybersecurity issues we need to be thinking about as a Nation.

Let's burst the "cyber-bubble" and deal with the real issues, concerns, effects, and consequences of operating in the "cyber" domain instead of relying on and/or believing questionable analysis and dubious statistics presented in sensational reports, statements and oft-cited soundbites.

Better still, let's all agree that if we want to be proactive in cybersecurity (or cyberwarfare protection) we must ensure our information assets not only are hardened and reinforced but designed with survivability and resiliency in the first place. Doing the former without the latter only will set us up to "lose" in the cyber domain. Our enemies recognize this and will act accordingly, so why don't we?

Until next year….

(image source unknown)

Clever definitions copyright © 2010 Richard Forno. Permission granted to use freely with appropriate credit. Thanks to Joel Harding and several un-named but very well-known IO folks for helping make this moment of zen possible.

REFERENCES

a. Joint Pub 1-02 Series, “Department of Defense Dictionary of Military and Associated Terms”

b. CNSS Instruction No. 4009 Series, “National Information Assurance (IA) Glossary”

c. DOD Directive 8500.1 Series, “Information Assurance (IA)”

d. DOD Directive O-8530.1 Series, “Computer Network Defense (CND)”

e. DOD Instruction 8500.2 Series, “Information Assurance (IA) Implementation”

f. DOD Instruction O-8530.2, 9 March 2001, “Support to Computer Network Defense (CND)”

g. CJCSM 6510.01 Series, “Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)”

h. DOD Directive 8100.1 Series, “Global Information Grid (GIG) Overarching Policy”

i. DOD CIO Memorandum, 6 July 2006, ”Department of Defense (DoD) Information Assurance (IA) and Certification and Accreditation (C&A) Process Guidance”

j. DOD Instruction 8551.1 Series, “Ports, Protocols and Services Management (PPSM)”

k. CJCSI 6211.02 Series, “Defense Information System Network (DISN): Policy, Responsibilities and Processes”

l. CNSSP-1 Series, “National Policy for Safeguarding and Control of Communications Security Materials”

m. DOD Regulation 5200.1-R Series, “Information Security Program”

n. National Security Agency, 2003/2004, “Information Assurance Manual”

o. Title 10, United States Code, Section 2315

p. NSTISSP No. 11 Revised, June 2003, “National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products”

q. Title 15, United States Code, Section 278g-3

r. ASD(NII) memorandum, 28 May 2003, "Open Source Software in the Department of Defense"

s. NIST Special Publication 800-59, August 2003, “Guidelines for Identifying an Information System as a National Security System”

t. DOD Instruction 8552.01 Series, "Use of Mobile Code Technologies in DoD Information Systems"

u. NTISSP No. 200, 15 July 1987, “National Policy on Controlled Access Protection”

v. DOD Regulation 5200.2-R Series, “Personnel Security Program”

w. ASD(C3I) memorandum with amendment, 11 January 2002, “Web Site Administration, Policies and Procedures”

x. DOD Directive 5230.9 Series, “Clearance of DOD Information for Public Release”

y. DOD Instruction 5230.29 Series, “Security and Policy Review of DOD Information for Public Release”

z. DOD CIO Memorandum, 25 April 2006, "Guidance to Facilitate Information Sharing on DoD Information Technology Systems (U)"

aa. DOD Directive 1035.1 Series, “Telework Policy for Department of Defense”

bb. DOD Directive 5200.1 Series, “DOD Information Security Program”

cc. DOD Directive 5200.2, 9 April 1999, “DOD Personnel Security Program”

dd. CJCSI 3213.01 Series, “Joint Operations Security”

ee. NTISSD No. 600, 10 April 1990, “Communications Security (COMSEC) Monitoring”

ff. DOD Directive 4640.6, 26 June 1981, “Communications Security Telephone Monitoring and Recording”

gg. Title 18, United States Code, Section 2510, et seq.

hh. Title 50, United States Code, Section 1801, et seq.

ii. DISA, 4 October 2002, “Application Security Developer’s Guide, Version 1.0”

jj. ASD(C3I) memorandum, 16 January 1997, “Policy on Department of Defense Electronic Notice and Consent Banner”

kk. DOD General Counsel memorandum, 27 March 1997, “Communications Security (COMSEC) and Information Systems Monitoring”

ll. DOD Directive 8520.2, 1 April 2004, “Public Key Infrastructure (PKI) and Public Key (PK) Enabling”

mm. DOD Directive 8570.1 Series, "Information Assurance Training, Certification, and Workforce Management"

nn. DOD 8570.01-M Series, "Information Assurance Workforce Improvement Program"

oo. NSTISSP No. 101, 14 September 1999, “National Policy on Securing Voice Communications”

pp. FIPS 140-2, 25 May 2001, “Security Requirements for Cryptographic Modules”

qq. DOD CIO memorandum, 3 July 2007, "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media"

rr. USSTRATCOM, 11 August 2006, "Joint Concept of Operations for Global Information Grid NetOps"

ss. DOD Directive 3020.40, 19 August 2006, "Defense Critical Infrastructure Program"

tt. DCID 6/3, 5 June 1999, “Protecting Sensitive Compartmented Information Within Information Systems”

uu. CJCSI 3213.01 Series, "Joint Operations Security"

vv. CJCSI 3121.01 Series, “Standing Rules of Engagement/Standing Rules for the Use of Force”

ww. CJCSI 6510.06 Series, “Communications Security Releases to Foreign Nations”

xx. CJCSI 6212.01 Series, “Interoperability and Supportability of Information Technology and National Security Systems”

yy. CJCSI 3137.01 Series, “The Joint Warfighting Capabilities Assessment Process”

zz. CJCSI 3170.01 Series, “The Functional Capabilities Board Process”

aaa. ASD(C3I) memorandum, 26 February 2003, “Guidance for Computer Network Defense Response Actions”

bbb. DOD Directive 8581.1E Series, "Information Assurance (IA) Policy for Space Systems Used by the Department of Defense "

ccc. Strategic Command Instruction (SI) 1009-01, 1 August 2006, "Information Assurance (IA) Implementation for Space Systems Used by the Department of Defense"

ddd. CJCSI 2300.01 Series, ”International Agreements”

eee. CJCSI 5130.01 Series, “Relationships Between Commanders of Combatant Commands and International Commands and Organizations”

fff. CJCSI 5221.01 Series, “Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations”

ggg. DOD Directive 4630.5, 5 May 2004, “Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)”

hhh. DOD 000-151-94, 24 May 1994, “Department of Defense Intelligence Production Program (DoDIPP)”

iii. DIA message 021727Z JUN 98, “Indications and Warning for Information Warfare/Information Operations (CNA-WATCHCON)”

jjj. NSD-42, 5 July 1990, “National Policy for the Security of National Security Telecommunications and Information Systems”

kkk. Initial Capabilities Document (ICD), 6 March 2006, "Initial Capabilities Document (ICD) for Global Information Grid (GIG) Information Assurance (IA)"

lll. NSTISSD No. 503, 30 August 1993, “Incident Response and Vulnerability Reporting for National Security Systems”

mmm. Strategic Command Directive (SD) 527-1, 27 January 2006, "Department of Defense (DOD) Information Operations Condition (INFOCON) System Procedures"

nnn. CJCSM 3402.01 Series, “Alert System of the Chairman of the Joint Chiefs of Staff”

ooo. Military Extraterritorial Jurisdiction Act of 2000, 18 U.S.C. 3261, et seq.

ppp. DOD Instruction 3020.41 Series, “Contractor Personnel Authorized to Accompany the U.S. Armed Forces.”

qqq. JTF-GNO Technical Bulletin 06-005, 191500Z May 2006, "Coordinating Authorized Scanning Activity Across DOD Networks"

rrr. CJCSI 3401.01 Series, “Chairman’s Readiness System”

sss. CJCSI 3401.03 Series, “Information Assurance (IA) and Computer Network Defense (CND) Joint Quarterly Readiness Review (JQRR) Metrics”

ttt. CJCSI 6731.01 Series, “Global Command and Control System Security Policy”

uuu. Deputy Secretary of Defense memorandum, July 2000, “Use and Protection of Portable Computing Devices”

vvv. DOD Directive 8100.2 Series, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG)"

www. DOD Directive, C-5200.19, 16 May 1995, “Control of Compromising Emanations”

xxx. ASD(NII) memorandum, 2 June 2006, "Use of Commercial Wireless Local- Area Network (LAN) Devices, Systems and Technologies in Department of Defense (DoD) Global Information Grid (GIG)"

yyy. PL 104-191, 21 August 1996, Health Insurance Portability and Accountability Act of 1996"

zzz. Title 5, U.S.C., Section 552a, et seq.

aaaa. DOD Directive C-5200.5 Series, “Communications Security (COMSEC)”

bbbb. CJCSI 6510.02 Series, "Cryptographic Modernization Planning"

cccc. CJCSN 6510 Series, "Information Assurance Cryptographic Equipment Modernization Requirements"

dddd. Special Publication 800-34 Series, “Contingency Planning Guide for Information Technology Systems”

eeee. DOD Directive 5200.8, 25 April 1991, “Security of DoD Installations and Resources”

ffff. Title 44, U.S.C. Section 3542, Federal Information Security Management Act of 2002

gggg. American National Standard for Telecommunications, 28 February 2001, “Telecom Glossary”

hhhh. National Military Strategy for Cyberspace Operations, November 2006