

~~SECRET//NOFORN~~



Information Operations Roadmap

30 October 2003

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

PAGE INTENTIONALLY LEFT BLANK

~~SECRET//NOFORN~~

Table of Contents (U)

1. SECRETARY'S FOREWORD (U)	1
2. IO ROADMAP CHARTER (U).....	2
A. APPROACH (U)	2
B. KEY ASSUMPTIONS AND OBJECTIVE (U)	3
3. EXECUTIVE SUMMARY (U)	6
A. CONCLUSIONS (U)	6
B. THE FOUNDATION FOR BUILDING A CORE MILITARY COMPETENCY (U)	7
C. RECOMMENDATIONS (U)	10
1. (U) Approve a common understanding of IO.....	10
2. (U) Consolidate Oversight and Advocacy for IO.....	11
3. (U) Delegate Capabilities to Combatant Commanders.	12
4. (U) Create a Well Trained and Educated Career Workforce.	12
5. (U) Provide Consolidated and Comprehensive Analytic Support.....	13
6. (U) Correct Immediate Shortfalls and Develop a Long-Term Defense in Depth Strategy for CND.....	13
7. (U) Mature CNA into a Reliable Warfighting Capability.	14
8. (U) Develop an Electronic Warfare Investment Strategy.....	14
9. (U) Increase Psychological Operations Capabilities.....	15
10. (U) Clarify Lanes in the Road for PSYOP, Public Affairs and Public Diplomacy.....	15
11. (U) Assign Advocacy for Operations Security and Military Deception.	16
12. (U) Improve Transparency of IO in the Planning, Programming, Budgeting and Execution System.....	16
4. ROADMAP REPORT (U)	17
A. IO POLICY (U)	18
1. Policies and Procedural Controls (U).....	18
2. Relationship of Public Diplomacy and Public Affairs to IO (U).....	24
B. EFFECTIVE COMMAND AND CONTROL AND SUPPORTING ORGANIZATIONS (U)	29
C. A TRAINED AND READY CAREER FORCE (U)	32
1. Career Force (U).....	32
2. Education and Training (U).....	35
D. FOCUSED ANALYTIC AND INTELLIGENCE SUPPORT (U)	38
1. Analytic and Intelligence Support (U)	38
2. Electromagnetic-Space Analysis Center (U).....	41
E. ENHANCING IO CORE CAPABILITIES (U)	44
1. Computer Network Defense (U).....	44
2. Computer Network Attack (U)	48
3. Electronic Warfare (U).....	59
4. Psychological Operations (U).....	62
5. Operations Security (U).....	65
6. Military Deception (U).....	67
APPENDIX A, TIMELINE (U).....	69

APPENDIX B, IO ROADMAP RECOMMENDATIONS (U)..... 70
APPENDIX C, DISTINGUISHING TASKS (U) 71
APPENDIX D, GLOSSARY (U)..... 72

1. Secretary's Foreword (U)

(U) The Information Operations Roadmap provides the Department with a plan to advance the goal of information operations as a core military competency. It provides a common framework for understanding IO, and policies and procedures to empower Combatant Commanders with authority to plan and integrate IO. It consolidates oversight, advocacy, and analytic support for IO. It calls for a dedicated work force and improved training and education for IO. Lastly, it mandates innovative organizational structures that advance operational capabilities to keep pace with warfighter needs and support defense transformation. Like any plan, it will evolve over time as the Department gains experience through implementation. For that reason, I will review the implementation effort after one year and the plan will be adjusted as appropriate.

(U) The Roadmap stands as another example of the Department's commitment to transform our military capabilities to keep pace with emerging threats and to exploit new opportunities afforded by innovation and rapidly developing information technologies. The recommendations in the Information Operations Roadmap begin the process of developing IO into a warfighting capability that will enable Combatant Commanders to target adversary decision-making while protecting our own.

(U) I approve the Roadmap recommendations and direct the Services, Combatant Commands and DoD Agencies to fully support implementation of this plan.

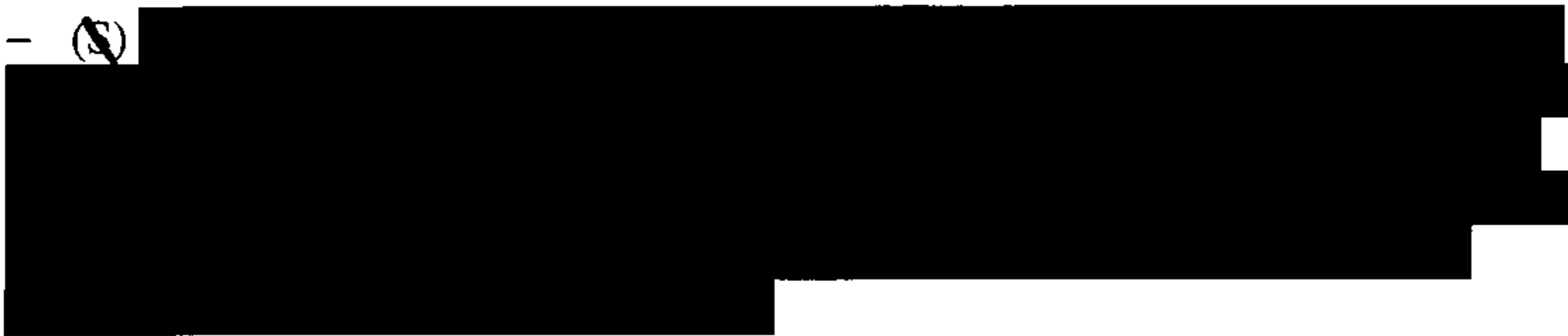
Original Signed

Donald H. Rumsfeld
Secretary of Defense

2. IO Roadmap Charter (U)

- (U) The 2001 Quadrennial Defense Review identified Information Operations (IO) as one of the six critical operational goals that focus transformation efforts within DoD. It required the Department to treat IO, along with intelligence and space assets, not simply as an enabler of current military forces, but rather as a core capability of future forces.
- ~~(S)~~ Subsequently, the Defense Planning Guidance (DPG) for FY2004-2009 directed that IO become a core military competency, fully integrated into deliberate and crisis action planning and capable of executing supported and supporting operations. The DPG encapsulated expected output from the Roadmap as follows:

- ~~(S)~~



A. Approach (U)

- (U) Mandate. The DPG assigned the Under Secretary of Defense (Policy) [USD(P)], in coordination with the Assistant Secretary of Defense (Command, Control, and Communications) and the Chairman, Joint Chiefs of Staff (CJCS), to develop a comprehensive IO Roadmap for presentation to the Secretary of Defense. The IO Roadmap was to address the full scope of IO as a core military competency and include supporting studies focused on policy, plans, organization, education, career force, analytic support, Psychological Operations (PSYOP), Operations Security (OPSEC), Electronic Warfare (EW), Military Deception and Computer Network Operations (CNO).
- (U) Leadership. USD(P) established an IO Roadmap oversight panel led by the Deputy Assistant Secretary of Defense (Resource and Plans) [DASD(R&P)]. The Deputy Assistant Secretary of Defense (Security and IO) [DASD(S&IO)] and the Deputy Director for Information Operations (DDIO) on the Joint Staff served in senior leadership roles for their respective organizations. The panel included representatives from other offices within the Office of the Secretary of Defense (OSD), the Services and Defense Agencies and also included regular attendance by representatives of Special Operations Command (SOCOM) and Space Command (SPACECOM). SPACECOM responsibilities transferred to Strategic Command (STRATCOM) on 1 October 2002.

- (U) Method. The principal work of the oversight panel was to guide the 15 separate supporting study efforts required by the DPG.* Each of the supporting study teams developed and briefed its terms of reference to the oversight panel. After terms of reference were agreed upon, each study team researched its topic, culling insights from multiple sources and antecedent studies. Study teams then provided an assessment of factors that currently constrain that IO area from contributing to IO as a core military competency. The study groups then drafted output statements sufficient to correct the limitations identified and developed prioritized recommendations that collectively would be sufficient to achieve the desired outcome.
 - (~~FOUO~~) Study leaders were appointed for the 15 supporting studies and specific milestones were assigned. Those studies assigned completion dates in September and October 2002 by the DPG were intended to influence the program and budget review, which they did. Approximately \$383M was provided through the FY04-09 Program Decision Memorandum supporting interim IO Roadmap recommendations, which were vetted by the oversight panel leadership.
 - (U) The study leads presented in-progress reviews and final reports to the oversight panel. Between June and December 2002, the oversight panel met weekly to address issues raised by the studies. The DASD(R&P), DASD(S&IO) and DDIO also met on a weekly basis to review which study action recommendations should be included as major IO Roadmap conclusions.
 - (U) Senior leadership reached agreement on all but a handful of recommendations. In those cases where agreement was not possible, USD(P), as the DPG-directed lead for the Roadmap, resolved the difference of opinion or elevated options for decision by the Secretary of Defense.

B. Key Assumptions and Objective (U)

- (U) Key assumptions. Information, always important in warfare, is now critical to military success and will only become more so in the foreseeable future. Three key assumptions underscore the growing importance of information:
 - (U) Effectively communicating U.S. Government (USG) capabilities and intentions is an important means of combating the plans of our adversaries. The ability to rapidly disseminate persuasive information to diverse audiences in order

* The 15 supporting study efforts reflected 2004 DPG guidance. They were as follows: Overarching Information Operations Roadmap Requirements; Policies & Procedural Controls; Relation of IO with Public Diplomacy and Public Affairs; IO Organization; IO Career Force; IO Education and Training; IO Analytic Support; Computer Network Attack; Computer Network Defenses; Computer Network Defense Threat Attribution; Computer Network Insider Threats; Electronic-Space Analysis Center; Transforming Electronic Warfare Capabilities; Psychological Operations; Operations Security.

to directly influence their decision-making is an increasingly powerful means of deterring aggression. Additionally, it undermines both senior leadership and popular support for employing terrorists or using weapons of mass destruction.

- (U) Networked C4ISR is a critical prerequisite for transforming our forces, providing for an increasingly transparent battle space, swift and effective decision-making, and rapid, parallel, effects-based operations.
- (U) Networked C4ISR is dependent upon automated decision-making and support, broadband networks, and electromagnetic capabilities, with a corresponding increase in associated vulnerabilities that should be planned for and managed.
- (U) Objective: IO becomes a core competency. The importance of dominating the information spectrum explains the objective of transforming IO into a core military competency on a par with air, ground, maritime and special operations. The charge to the IO Roadmap oversight panel was to develop as concrete a set of action recommendations as possible to make IO a core competency, which in turn required identifying the essential prerequisites to become a core military competency.
- (U) IO as a core competency requires a common understanding and appreciation within the Office of the Secretary of Defense, the Services and Combatant Commands on the value of IO. IO as a core military competency also requires:
 - (U) Policies and procedures that:
 - (U) Clearly define IO, provide a common understanding and clarify authorities and boundaries for execution.
 - (U) Delegate the maximum possible authority to Combatant Commanders to plan and execute integrated IO.
 - (U) Plans, operations and experimentation that:
 - (U) Incorporate IO in contingency planning within all joint force headquarters.
 - (U) Integrate IO into the broader development of new operational concepts.
 - (U) Include IO in all major training regimes and exercises.
 - (U) IO force development made possible by:
 - (U) Four-star Combatant Commander advocacy of IO for experimentation, concept development and definition of needed capabilities.
 - (U) Streamlined organizational and command and control relationships.

- (U) A trained and educated career force.
- (U) Joint program equivalents to develop dedicated IO capabilities.
- (U) The recommendations of this report address all the requirements to make IO a core military competency just identified.

3. Executive Summary (U)

A. Conclusions (U)


- (U) The IO Roadmap participants collectively identified three matters of key importance that require immediate attention:
- ~~(C)~~ We Must Fight the Net. DoD is building an information-centric force. Networks are increasingly the operational center of gravity, and the Department must be prepared to “fight the net.” [REDACTED] but be fully prepared to ensure critical warfighting network functionality and to [REDACTED]
 - ~~(C)~~ However, networks are vulnerable now, and barring significant attention, will become increasingly more vulnerable. [REDACTED]
 - ~~(C)~~ The recommendations of this report offer a good start point for remedial action for network security to maintain decision superiority. A robust, layered, defense in depth strategy is the next necessary step in providing Combatant Commanders with the tools necessary to preserve warfighting capability.
- (U) We Must Improve PSYOP. Military forces must be better prepared to use PSYOP in support of military operations and the themes and messages employed in a PSYOP campaign must be consistent with the broader national security objectives and national-level themes and messages. Currently, however, our PSYOP campaigns are often reactive and not well organized for maximum impact.
 - (U) PSYOP enhancements outlined in this report, and clarification of the respective responsibilities and tasks associated with PSYOP, DoD support to public diplomacy and public affairs, will enhance DoD’s ability to aggressively conduct IO and to do so fully consistent with broader national security objectives.
 - (U) In particular, PSYOP must be refocused on adversary decision-making, planning well in advance for aggressive behavior modification during times of conflict. PSYOP products must be based on in-depth knowledge of the audience’s decision-making processes and the factors influencing his decisions, produced rapidly at the highest quality standards, and powerfully disseminated directly to targeted audiences throughout the area of operations.
- (U) We Must Improve Network and Electro-Magnetic Attack Capability. To prevail in an information-centric fight, it is increasingly important that our forces dominate the electromagnetic spectrum with attack capabilities.

- ~~(S)~~ [REDACTED]
- ~~(S)~~ When implemented the recommendations of this report will effectively jump-start a rapid improvement of CNA capability. Moreover, the follow-on EW roadmap should define an overall investment strategy for the Department that will [REDACTED]
- (U) Collectively, the recommendations of this report begin the transformation of IO into a core military capability for Combatant Commanders. If aggressively implemented, these recommendations will produce the following benefits for the Department in general and the Combatant Commanders in particular:
 - (U) A common lexicon and approach to IO, including support to integrated information campaign planning.
 - (U) More execution authority delegated to Combatant Commanders.
 - (U) A trained and educated career force capable of IO planning and execution.
 - (U) Centralized IO planning, integration and analysis support from STRATCOM.
 - (U) Enhanced IO capabilities for the warfighter, including:
 - (U) Improved ability to disseminate powerful messages in support of adversary behavior modification.
 - (U) Protection of networks with a real defense in depth strategy.
 - (U) A robust offensive suite of capabilities to include full-range electronic and computer network attack, with increased reliability through improved command and control, assurance testing and refined tactics and procedures.

B. The Foundation for Building a Core Military Competency (U)

- (U) A uniform understanding and appreciation of IO should be based on a common DoD framework that includes a full spectrum concept of IO built upon three broad IO functions, five integrated core IO capabilities and a supporting definition as described below.
- (U) Three integrated IO functions. The Department's concept of IO should emphasize full spectrum IO that makes a potent contribution to effects based

operations across the full range of military operations during peace, crisis and war. The concept includes three integrated IO functions of overriding importance:

- (U) Deter, discourage, dissuade and direct an adversary, thereby disrupting his unity of command and purpose while preserving our own.
- (U) Protect our plans and misdirect theirs, thereby allowing our forces to mass their effects to maximum advantage while the adversary expends his resources to little effect.
- (U) Control adversarial communications and networks and protect ours, thereby crippling the enemy's ability to direct an organized defense while preserving effective command and control of our forces.
 - (U) By extension, when executed to maximum effect, seizing control of adversary communications and networks will allow Combatant Commanders to control the enemy's network and communications-dependent weapons, infrastructure, command and control and battlespace management functions.
- (U) Peacetime preparation. The Department's IO concept should emphasize that full-spectrum information operations are full-time operations requiring extensive preparation in peacetime.
 - (U) Well before crises develop, the IO battlespace should be prepared through intelligence, surveillance and reconnaissance and extensive planning activities.
 - ~~(U)~~ 
 - (U) Similarly, considerable effort should be made to characterize potential adversary audiences, and particularly senior decision-makers and decision-making processes and priorities. If such human factors analysis is not conducted well in advance of the conflict, it will not be possible to craft PSYOP themes and messages that will be effective in modifying adversary behavior.
 - (U) Computer Network Defense (CND) and OPSEC are vital capabilities in all phases of conflict, but should be given priority especially during peacetime to prevent adversaries from preparing effective information operations or exploiting vulnerabilities against our forces. Protecting our plans and networks

will ensure our ability to make decisions effectively and execute plans with minimum disruption.

- (U) Five core capabilities. Full spectrum IO employs five core capabilities to achieve desired Combatant Commander effects or else prevent the enemy from achieving his desired effects: EW, PSYOP, OPSEC, military deception and CNO.
 - (U) The focus on five core capabilities is a significant change from the IO construct promulgated in December 1996 that included thirteen primary capabilities. There are three reasons why IO has been narrowed to these five core capabilities:
 - (U) They are operational in a direct and immediate sense; they either achieve critical operational effects or prevent the adversary from doing so.
 - (U) They are interdependent and increasingly need to be integrated to achieve desired effects. For example:
 - ~~(S)~~ [REDACTED]
 - ~~(S)~~ [REDACTED]
 - ~~(S)~~ [REDACTED]
 - ~~(S)~~ [REDACTED] and information in support of a broader military deception plan.
 - ~~(S)~~ [REDACTED] by undermining the adversary's confidence in his capabilities (e.g. [REDACTED]) [REDACTED]
 - (U) They clearly define the capabilities the Services and SOCOM are expected to organize, train, equip and provide to the Combatant Commander. A broader conceptualization of IO dilutes its focus on decision-making, and serves to divorce IO from the three primary operational IO objectives of greatest importance to the warfighter.
- (U) Identify supporting and related capabilities. All IO Roadmap participants agreed with the need to identify supporting and related capabilities. Like all core military competencies, information operations can not be successfully executed without diverse supporting capabilities.

- (U) Capabilities such as physical security, information assurance, counter intelligence and physical attack make important contributions to effective IO. Like many supporting capabilities, such as logistics and surveillance and reconnaissance, they also serve other core competencies besides IO.
- (U) Public affairs and civil military operations remain related activities as first identified in the original 1996 construct of IO.
 - (U) These capabilities are related in the sense that the effects they achieve may be similar to some aspects of IO, particularly PSYOP.
 - (U) One result of public affairs and civil military operations is greater support for military endeavors and thus, conversely these activities can help discourage and dissuade enemies, which PSYOP does more directly with its own tactics, techniques and procedures.
- (U) IO requires coordination with public affairs and civil military operations to complement the objectives of these related activities and ensure message consistency.

C. Recommendations (U)

- (U) The IO Roadmap recommendations are condensed and in some cases consolidated in the following paragraphs along with a brief background statement in order to summarize the essence of the IO Roadmap effort.

1. (U) Approve a common understanding of IO.

(U) The Services, Combatant Commands and Agencies do not have a common understanding of IO. Services do not uniformly equip and train for IO and Combatant Commands do not adequately assist in requirement generation. As a result, IO is not fully integrated in plans and orders. The first step in making IO a core military competency is agreement on a common framework for IO, including a standardized definition and a uniform approach to using IO in joint warfighting; i.e.:

(U) IO should focus on degrading an adversary's decision-making process while preserving our own. To that end, IO should:

- *(U) Deter, discourage, and dissuade an adversary by disrupting his unity of command while preserving ours.*
- *(U) Protect our plans and misdirect theirs.*
- *(U) Control their communications and networks while protecting ours.*

(U) To accomplish these functions, IO should integrate the five core capabilities, and be applied across the full range of military operations. To be successful, full spectrum IO must be a full time endeavor with continuous planning and preparation prior to a crisis or conflict. To best communicate this approach to IO, the following definition should be included in a revised DoD Directive on Information Operations and in appropriate updates of joint publications:

“The integrated employment of the core capabilities of Electronic Warfare, Computer Network Operations, Psychological Operations, Military Deception and Operations Security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making while protecting our own.”

2. (U) Consolidate Oversight and Advocacy for IO.

(U) A major deficiency identified in advancing IO as a core military competency is the “balkanization” of IO responsibilities across OSD, the Services and Combatant Commands. During the development of the IO Roadmap, a revised Unified Command Plan (UCP) expanded STRATCOM’s IO role on behalf of the other Combatant Commands. With respect to OSD, USD(P) has been assigned lead for implementation of the IO Roadmap but the need for consolidating OSD oversight of IO remains an issue. In the near term:

(U) USD(P) should chair an IO Roadmap Executive Committee for the purpose of coordinating the efforts of USD(AT&L) USD(I), USD(P&R), ASD(NII), Director PA&E, CJCS, Commander STRATCOM, and Commander SOCOM to implement the recommendations included in this report.

- (U) The IO Roadmap Executive Committee will be supported by a Deputy Assistant Secretary of Defense (DASD)-level group, chaired by DASD(R&P), that includes Service participation and provides guidance and routine oversight and is supported by an IO Implementation Team overseeing daily activity to achieve Roadmap recommendations.*

(U) Following the first full year of IO Roadmap implementation, the USD(P) should present to the Secretary any additional recommendations necessary for consolidation of OSD oversight of IO. These recommendations should be coordinated among the IO Roadmap Executive Committee. In the case(s) of principled differences between or among Committee members, options with pros and cons should be presented.

3. (U) Delegate Capabilities to Combatant Commanders.

~~(S)~~ Information Operations will not become an established core competency until [REDACTED] to rapidly employ IO capabilities. The Standing Rules of Engagement should be modified [REDACTED] and PSYOP. In particular:

~~(S)~~ *The CJCS in coordination with STRATCOM should propose to SecDef modifications to the Standing Rules of Engagement for [REDACTED], so that [REDACTED] except those that entail high risk of knowledge transfer to enemies (see p.57). Plans for such attacks should be prepared in accordance with existing procedures.*

~~(S)~~ *USD(P) should modify the PSYOP approval process so that overall PSYOP program approval and approval for all products with substantial political or strategic content or implication remains with USD(P). All other PSYOP product approval should be delegated to Combatant Commanders.*

4. (U) Create a Well Trained and Educated Career Workforce.

(U) The five core IO capabilities are not understood and applied the same way across the Services. Instead, each Service develops specialists in IO disciplines to meet Service-specific requirements. In addition, the growing complexity and technological growth in EW, PSYOP and Computer Network Operations tend to isolate the specialists who practice these disciplines from one another, thus hindering integration of core IO capabilities. Therefore:

(U) USD(P&R) should lead the establishment of an IO career force comprised of planners and capability specialists. It should also oversee the designation of Service and joint IO billets to provide IO opportunities up to senior executive or flag level rank. Follow-on actions should establish parameters to monitor accession, retention and promotion rates for personnel in the IO career force.

(U) The CJCS and USD(P&R) should ensure joint and Service training is aligned to support the career force objective.

(U) The Joint Forces Staff College should be designated the lead to develop standardized joint IO curricula at mid and senior levels including an expanded Joint IO Planners Course. The Joint Forces Staff College should collaborate with Service schools to integrate joint IO curricula into their education.

(U) The Deputy Secretary should officially designate the Naval Post Graduate School as a DoD Center of Excellence to provide graduate level, full-spectrum IO

core and specialty programs, as well as assistance to joint doctrine development and innovation through analysis and research.

5. (U) Provide Consolidated and Comprehensive Analytic Support.

~~(S)~~ Multiple studies (Joint Warfighting Capability Assessments, the 2000 IO Broad Area Review and the 2001 Quadrennial Defense Review) and operational lessons learned (Kosovo and Afghanistan) have [REDACTED] Combatant command staffs currently cannot produce rapid solutions for tailored IO effects due to the lack of sufficient staff expertise and no single support center for integration of IO analysis, planning and targeting. To alleviate these well-documented shortfalls:

(U) STRATCOM, in coordination with USD(I) and CJCS, should develop a Joint Integrative Analysis and Planning Capability (JIAPC) to provide timely analysis, planning and targeting in support of Combatant Commander's IO requirements. This capability should integrate the analysis products of the Electromagnetic-Space Analysis Center at NSA, the Human Factors Analysis Center at DIA, the Joint Information Operations Center and the Joint Warfighting Analysis Center. The JIAPC constitutes an integrated network of analysis centers that, properly managed, could provide holistic analytic support to Combatant Commanders.

- ~~(S)~~ STRATCOM, in coordination with USD(I), should develop memorandums of agreements with the [REDACTED] and the Director Defense Intelligence Agency on the Human Factors Analysis Center.
- ~~(S)~~ USD(I), in coordination with the USD(AT&L), will develop direction for the [REDACTED] to provide [REDACTED] operational planning and advanced EA development programs.

6. (U) Correct Immediate Shortfalls and Develop a Long-Term Defense in Depth Strategy for CND.

(U) DoD requires a robust, layered defense across the Department based on global and enclave situational awareness with a centralized capability to rapidly characterize, attribute and respond to attacks. DoD's "Defense in Depth" strategy should operate on the premise that the Department will "fight the net" as it would a weapons system. More specifically:

(U) ASD(NII) should develop the "Defense in Depth" strategy to give senior leaders high confidence that additional investments in network defense will ensure the graceful degradation of the network rather than its collapse. The strategy should take

into account limited resources and balance them against known risks. The starting assumption should be one of attrition, i.e. that the networks will be degraded. However, the strategy should be engineered to sustain required capabilities across the range of military operations.

7. (U) Mature CNA into a Reliable Warfighting Capability.

~~(S)~~ [REDACTED]. The UCP assigned STRATCOM authority for CNA.
[REDACTED]

~~(S)~~ *STRATCOM should be assigned combatant command of CNA forces.*

~~(S)~~ [REDACTED]

~~(S)~~ [REDACTED]

~~(S)~~ [REDACTED]

~~(S)~~ [REDACTED]

8. (U) Develop an Electronic Warfare Investment Strategy.

~~(S)~~ A number of studies over the past several years, to include Joint Warfighting Capabilities Assessments (JWCA) and the Airborne Electronic Attack Analysis of Alternatives Study reached the following conclusions with respect to current EW

