~~SECRET~~//NOFORN

Information Operations Roadmap

30 October 2003

~~SECRET~~//NOFORN

PAGE INTENTIONALLY LEFT BLANK

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 an 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) [redacted]

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:
- (S) 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]
  - (S) However, networks are vulnerable now, and barring significant attention, will become increasingly more vulnerable. [redacted]
  - (S) 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.

        - (S) [redacted]

        - (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]
    - (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

capabilities. Defensive EW capabilities are overemphasized in comparison to electronic attack capabilities. There are [redacted]
There is no central investment strategy or vision for EW. To correct these shortcomings:

(U) USD(AT&L) should formally establish and charter an Electronic Warfare Executive Steering Group to develop a coherent multi-Service investment strategy and provide effective oversight of the development of Electronic Warfare system and operational architectures. The primary objective should be to develop a comprehensive EW roadmap to focus DoD's efforts on providing joint forces and component commanders operational level electronic attack options that deny, degrade, disrupt, or destroy a broad range of adversary threats, sensors, command and control and critical support infrastructures.

9. (U) Increase Psychological Operations Capabilities.

(S) Over the last decade, numerous studies have documented the deterioration of PSYOP capabilities and have recommended remedial action. Well-documented PSYOP limitations persist. These include: the [redacted]
insufficient numbers of experienced and well equipped PSYOP personnel; and a limited ability to disseminate products into denied areas. SOCOM and Army PSYOP force enhancement efforts are already underway per IO Roadmap recommendations in the last program review, and they should continue. In addition:

(U) SOCOM should create a Joint PSYOP Support Element to coordinate Combatant Command programs and products with the Joint Staff and OSD to provide rapidly produced, commercial-quality PSYOP product prototypes consistent with overall U.S Government themes and messages.

(U) SOCOM's ongoing PSYOP Advanced Concept Technology Demonstration and modernization efforts should permit the timely, long-range dissemination of products with various PSYOP delivery systems. This includes satellite, radio and television, cellular phones and other wireless devices, the Internet and upgrades to traditional delivery systems such as leaflets and loudspeakers that are highly responsive to maneuver commanders.

10. (U) Clarify Lanes in the Road for PSYOP, Public Affairs and Public Diplomacy.

(U) Future operations require that PSYOP capabilities be improved to enable PSYOP forces to rapidly generate and disseminate audience specific, commercial-quality products into denied areas, and that these products focus on aggressive behavior modification of adversaries at the operational and tactical level of war. The likelihood that PSYOP messages will be replayed to a much broader audience, including the

American public, requires that specific boundaries be established for PSYOP. In particular:

(U) PSYOP should focus on support to military endeavors (exercises, deployments and operations) in non-permissive or semi-permissive environments (i.e., when adversaries are part of the equation).

(U) DoD should collaborate with other agencies for U.S. Government public diplomacy programs and information objectives. PSYOP forces and capabilities can be employed in support of public diplomacy (e.g., as part of approved theater security cooperation guidelines.)

(U) DoD Public Affairs should be more proactive in support of U.S. Government Public Diplomacy objectives to include a broader set of select foreign media and audiences.

11. (U) Assign Advocacy for Operations Security and Military Deception.

(U) Protecting our plans while misdirecting those of the adversary is one of the three broad functions of integrated IO. This cannot be accomplished without significant improvements in both OPSEC and military deception. Therefore:

(~~S~~) The Department should assign advocacy for joint OPSEC and military deception to STRATCOM and ensure their full integration into IO concepts, planning and career force education and training. [redacted]

12. (U) Improve Transparency of IO in the Planning, Programming, Budgeting and Execution System.

(U) DoD should improve IO capabilities through a coordinated investment strategy and senior leader oversight of IO processes. Better insight into the level and distribution of fiscal and personnel resources would be an initial helpful step in this regard:

(U) The Department should establish a virtual Major Force Program for Information Operations to identify what DoD spends on IO and its core capabilities.

4. Roadmap Report (U)

(U) Recommendations by Major IO Roadmap Areas

- (U) Five part agenda. The 2004 Defense Planning Guidance (DPG) mandated 15 Roadmap studies, which the IO Roadmap oversight panel aggregated into five major areas for reform:
  - (U) Policies and Procedural Controls.
  - (U) Command and Control and Supporting Organizations.
  - (U) Trained, Educated and Ready Career Force.
  - (U) Analytic Support.
  - (U) Enhanced Core Capabilities.
- (U) Report format. Specific recommendations to the Secretary to make IO a core military competency are organized for each of the five reform areas in a standard format that reflects the approach adopted by the Roadmap studies:
  - (U) ***DPG Tasking***. Displays the tasking given in the 2004 DPG.
  - (U) ***Current Situation***. Provides an assessment of current ability to contribute to IO as a core military capability, with emphasis on particular problem areas.
  - (U) ***Desired Outcome***. Articulates a specific desired outcome to expedite transformation of IO into a core military competency.
  - (U) ***Recommendations***. Provides specific recommendations to rapidly establish IO as a core military competency and achieve the desired outcome. A general timeline to implement the recommendations is at Appendix A.

A. IO Policy (U)

(U) This major study area incorporates a review of overall policy and procedures for IO as well as review of the relationship of public diplomacy and public affairs in relation to IO.

1. Policies and Procedural Controls (U)

(U) ***DPG Tasking***.

- (U) USD(P) will develop recommendations for policies and procedural controls for IO, in coordination with CJCS and, as necessary, the National Security Council (NSC) and the Intelligence Community. In doing so, USD(P) will actively improve and enforce interagency processes to deconflict Computer Network Exploitation (CNE) and Computer Network Attack (CNA) and enhance CNE activities as an essential precursor for DoD operations.

(U) ***Current Situation***.

- (S) Inadequate policy. A review of existing policy for IO found that policy lags behind operations.
  - (U) There is not a consensus on how to define IO or its contribution to warfighting.
  - (U) Computer Network Defense (CND) lacks up to date policy and legal guidance (including newly acquired authorities provided by the Patriot and Homeland Security Acts) to guide responses to intrusions or attacks on DoD networks.
  - (S) [redacted] that would guide development of desired capabilities, specific weapons development and employment, interagency coordination, and declaratory policy.
  - (U) EW policy is outdated. DoD's overarching policy was published in 1994 after the first Gulf War. The DoD directive is not consistent with the approach or recommendations of this report. It needs to be updated to stress EW as an integral part of Information Operations with important linkages to Computer Network Operations and other IO core capabilities.
- (S) Overly centralized control of IO capabilities.
  - (S) Combatant Commanders conduct some planning for IO, but have [redacted] for execution, even after their plans are approved.

- (U) In March 2002, DPG precursor work on IO was briefed to the Senior Leadership Review Group (SLRG) which consists of the Secretary, CJCS, Service Chiefs, Service Secretaries and OSD principals. The SLRG directed that the Roadmap review delegation of IO authorities to Combatant Commanders as a matter of high priority. Consequently, the Joint Staff DDIO conducted a study of the IO review and approval process. That study found the following:
  - (S) [redacted] The study recommended that much of this capability be delegated to Combatant Commanders.
  - (U) All PSYOP programs are currently approved by USD(P), although after initial product approval by USD(P), similar succeeding products are sometimes delegated to Combatant Commands.
  - (U) The DDIO study concluded that existing approval processes for EW, OPSEC and military deception were satisfactory.
  - (S) In a recent change (supported by the IO Roadmap leadership), the Secretary now delegates some [redacted] to a Combatant Commander in advance when the target effect is reversible and non-destructive.

- (S) Command and control issues.
  - (U) In July 2002, the Operations Deputies of the Services requested the JCS conduct a "Proof of Principle" exercise to test command and control of CNA. The November 2002, Eligible Receiver 03 exercise was used for this purpose.
    - (S) The no-notice JCS scenario exercised STRATCOM as both a supporting and supported commander for [redacted] and examined the role of the [redacted]
    - (S) The exercise highlighted the need to revise the [redacted] and improve the command and control construct.

- (S) Resource management.
  - (S) The Department can not currently identify what is spent on IO or even on specific core capabilities (with the possible exception of PSYOP, which is largely visible under MFP 11).
    - (U) The lack of a systematic methodology to account for IO resources across the Department is a major impediment. This limitation was keenly felt during

the program review when the IO Roadmap leadership was required to recommend adjustments to IO programs, including identification of offsets.

- (U) Services and Agencies often embed IO resources within Program Elements (PEs). Additionally, some IO programs are protected inside Special Access Programs (SAPs). Both factors severely limit the ability of senior leaders to monitor and evaluate the adequacy of IO efforts.

(U) ***Desired Outcome***.(U)

- (U) Clear, unambiguous and streamlined DoD oversight and policy that empowers Combatant Commanders to execute full spectrum IO before, during and after combat operations.

(U) ***Recommendations (Numbers 1 - 5)***.

(U) **Recommendation: Publish IO policy (#1).**

- (U) Upon approval of the IO Roadmap, the USD(P) should immediately publish revised overarching DoD policy on Information Operations to facilitate a common understanding and appreciation of IO, define objectives and delineate IO responsibilities. This 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) **Recommendation: Adopt a full spectrum concept of IO built upon three broad functions and five core capabilities (#2).**

- (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.

  - (S) For example, Combatant Commanders [redacted] to temporarily [redacted] infrastructure and quickly reconstitute them consistent with national objectives.

- (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.

    - (S) [redacted].

    - (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) 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]

  - (S) [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) **Recommendation: Approve a definition of IO based upon the full spectrum concept (#3).**

- (U) At the inception of the IO Roadmap effort the definition of information operations being used in a draft DoD Directive was: "Actions taken to affect adversary information and information systems while defending one's own information and information systems." Roadmap participants agreed that this definition was too open-ended and that it ought to underscore the central importance of the five core capabilities. Moreover, as the Secretary pointed out when briefed on IO Roadmap progress, the definition ought to underscore the centrality of decision-making rather than the general importance of information writ large. Therefore, the IO Roadmap recommended definition is:

> (U) "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."

- (U) Promulgate the approved definition. The approved definition should be included in the revamped DoD Directive on Information Operations and in appropriate updates of joint publications.

- (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.

(U) **Recommendation: Delegate selected execution authority to Combatant Commanders (#4).**

- (S) A common approach to IO based on the aforementioned full spectrum concept will clear the way for development of IO as a core competency, but it will not become one until Combatant Commanders are empowered to rapidly employ IO. The Standing Rules of Engagement should be modified for [redacted] PSYOP.

  – (S) CNA Delegation. [redacted] using all CNA weapons except those that entail high risk of knowledge transfer to enemies.

- (U) PSYOP Delegation. Combatant Commanders should have approval authority for all PSYOP products that do not contain substantial political or strategic content or implication.

(U) **(NOTE**: *To facilitate comprehensive presentation of recommendations related to a core capability area, more detailed discussion of and recommendations for delegating CNA and PSYOP to Combatant Commanders is contained in the sections of the report addressing these capabilities. For the same reason recommendations for national policy for CNA and cooperation with the Intelligence Community on CNA are included in the section on CNA.)*

(U) **Recommendation: Improve visibility and accountability of IO resources (#5).**

- (U) Director, P&E, in coordination with USD(P), USD(I), USD(AT&L) and DoD components, should create a "virtual" IO major force program for resource identification.

  - (U) IO resources are generally a subset of a Program Element (PE). Because resources are embedded within multiple PEs, it has been almost impossible to develop an accurate IO program baseline across DoD.

  - (U) DoD should require components to create whole PEs for IO core and associated capabilities. This would require components to identify embedded IO resources and transfer those resources into whole IO PEs. As an example of associated capabilities, components should identify resources for IO training and education, thereby distinguishing these resources from larger DoD education requirements.

2. Relationship of Public Diplomacy and Public Affairs to IO (U)

(U) ***DPG Tasking***.

- (U) USD(P), in coordination with ASD(PA) will analyze and make recommendations on those policy, strategy and legal issues affected by and related to the proper role for public diplomacy and public affairs in relation to IO. Particular emphasis will be given to examining the appropriate relationship of PSYOP to public affairs as they relate to USG communications strategies for both adversaries and non-adversaries. The analysis will include recommendations on policies, requirements, resources, training and education to support a transformed communications capability in support of military operations in the global information environment.

(U) ***Current Situation***.

- (U) Coherent messages. It is increasingly important to national security objectives that the USG put out a coherent and compelling political message in concert with military operations. Preserving unity of effort and morale has always been important in war. However, the desire for broad political support of military operations, the prevalence of access to global communications in the modern world and the political and cultural origins of terrorism require more comprehensive and proactive USG communication strategies.

  - (U) The USG can not execute an effective communication strategy that facilitates military campaigns if various organs of Government disseminate inconsistent messages to foreign audiences. Therefore, it is important that policy differences between all USG Departments and Agencies be resolved to the extent that they shape themes and messages.

  - (U) All DoD information activities, including information operations, which are conducted at the strategic, operational, and tactical level, should reflect and be consistent with broader national security policy and strategy objectives.

- (S) Coordinating information activities. Major DoD "information activities" include public affairs, military support to public diplomacy and PSYOP. The State Department maintains the lead for public diplomacy, the [redacted] and the International Broadcasting Board of Governors maintains the lead for broadcasting USG messages overseas, often with DoD in a supporting role. DoD has consistently maintained that the information activities of all these agencies must be integrated and coordinated to ensure the promulgation of consistent themes and messages.

  - (U) Historically PSYOP is the IO area considered most in need of coordination and deconfliction with public affairs and public diplomacy. In particular, attention is typically paid to the need to carefully segregate PSYOP from public affairs for fear that PSYOP tactics and techniques would undermine the credibility of public affairs efforts.

  - (U) Department of State practitioners of public diplomacy have historically expressed similar reservations about PSYOP.

- (U) PSYOP in the past, however, often was used to support U.S. Government public diplomacy and information objectives with non-adversarial audiences. These actions include counter-drug, demining and AIDS awareness programs in friendly countries. In most cases, PSYOP used in this capacity was justifiable as support to military operations.

- (U) Other comparisons. In the past some basic similarities and dissimilarities between PSYOP, support to public diplomacy and public affairs generally have been

accepted. Historically all three used truth to bolster credibility, and all three addressed foreign audiences, both adversary and non-adversaries. Only public affairs addressed domestic audiences. In addition, all three activities sought a positive impact for USG interests, but with some differences in the methods employed and objectives sought. The customary position was that "public affairs informs, while public diplomacy and PSYOP influence." PSYOP also has been perceived as the most aggressive of the three information activities, using diverse means, including psychological manipulation and personal threats.

- (U) Impact of the global village. The increasing ability of people in most parts of the globe to access international information sources makes targeting particular audiences more difficult. Today the distinction between foreign and domestic audiences becomes more a question of USG intent rather than information dissemination practices:

  – (U) PSYOP is restricted by both DoD policy and executive order from targeting American audiences, our military personnel and news agencies or outlets.

    - (U) However, information intended for foreign audiences, including public diplomacy and PSYOP, increasingly is consumed by our domestic audience and vice-versa.

    - (U) PSYOP messages disseminated to any audience except individual decision-makers (and perhaps even then) will often be replayed by the news media for much larger audiences, including the American public.

(U) ***Desired Outcome***

- (U) Establish a clear delineation of responsibilities for DoD information activities that properly delimits IO and ensures that IO is fully coordinated with the broad themes and messages promoted by the USG more generally.

(U) ***Recommendations (Numbers 6 – 9).***

- (U) Requirements. To inform and influence a variety of foreign audiences in the increasingly complex global information environment, DoD should:

(U) **Recommendation: Enhance and refocus PSYOP capability (#6).**

- (U) Improvements in PSYOP capability are required to rapidly generate audience specific, commercial-quality products into denied areas.

- (U) Future operations require that PSYOP focus on aggressive behavior modification at the operational and tactical level of war. The likelihood that PSYOP messages will

be replayed to a much broader audience, including the American public, requires specific boundaries be established:

- (U) PSYOP should focus on support to military endeavors (exercises, deployments and operations) in non-permissive or semi-permissive environments (i.e. when adversaries are part of the equation).

  - (U) However, PSYOP forces and capabilities may be employed to support U.S. public diplomacy as part of approved theater security cooperation guidelines. In this case PSYOP personnel and equipment are not conducting a PSYOP mission, but rather are providing military support to public diplomacy. For example, PSYOP forces and capabilities could continue to support U.S. International Broadcasting Board of Governors operations such as Radio/TV Marti when so requested.

(U) **Recommendation: Improve military support to public diplomacy (#7).**

- (~~FOUO~~) While IO is focused on creating effects against adversaries for the joint warfighting commander (and preventing adversaries from doing the same to us), there is a broader set of DoD information activities that serve USG interests. For example, DoD may collaborate with other agencies for public diplomacy programs that directly support DoD's mission. The Department recently provided funds (through the Office of Management and Budget) to purchase a radio transmitter in Afghanistan for use by the Voice of America that makes a direct contribution to improved force protection conditions. The FY2004-2009 Program Decision Memorandum (PDM 1) provided $23M in FY04 to enhance DoD's ability to provide support to public diplomacy.

(U) **Recommendation: Support active public affairs programs that influence foreign audiences (#8).**

- (~~FOUO~~) Clear boundaries for PSYOP should be complemented by a more proactive public affairs effort that expands to include a broader set of select foreign media and audiences. PDM-1 provided $161M to ASD(PA) over the Future Years Defense Plan (FYDP) to implement this intent. These funds will enable ASD(PA) to:

  - (U) Develop a global web site supporting U.S. strategic communications objectives. Content should be primarily from third parties with greater credibility to foreign audiences than U.S. officials.

  - (U) Identify and disseminate the views of third party advocates that support U.S. positions. These sources may not articulate the U.S. position the way that the USG would, but they may nonetheless have a positive influence.

- (U) Implement strict ground rules for media embedded with military forces to protect operational security.

- (U) Maintain quick response public affairs teams with organic linguist support.

- (U) Include coordination between public affairs, civil military operations and IO in major training regimes and ensure that coordination is regularly exercised.

(U) **Recommendation: Develop distinguishing tasks (#9).**

- (U) OSD should develop task lists so that public affairs, public diplomacy and PSYOP practitioners are clear about their objectives and activities. See Appendix C for an initial list of these tasks.

B. Effective Command and Control and Supporting Organizations (U)

(U) ***DPG Tasking***.

- (U) DPG 04 directed the CJCS in coordination with USD(P) and ASD(C3I) to provide recommendations on organizational arrangements for better integrating and synchronizing IO capabilities.

(U) ***Current Situation***.

- (U) Centralized responsibility. At the outset of the IO Roadmap, responsibilities for IO were dispersed across the Combatant Commands and on the OSD staff. Only the Joint Staff has largely centralized IO responsibilities in one office, the DDIO.

- (U) DDIO organization study. An organizational study conducted by the Joint Staff in the summer of 2002 was merged with the IO Roadmap effort. The study recommended empowering STRATCOM with greater IO authority.

  - (U) The IO Roadmap leadership unanimously supported the recommendations proposed by the study.

    - (U) The study noted that previously SPACECOM, although given the mission for CNA, did not have the forces to accomplish the tasks required.

    - (U) SPACECOM highlighted the lack of CNA forces as a major impediment in advancing CNA into a robust warfighting capability when STRATCOM and SPACECOM combined in October 2002.

    - (S) The study also noted that PSYOP capabilities had not kept up with requirements, but did not endorse assigning the PSYOP mission to STRATCOM. The study recommended SOCOM retain the PSYOP mission, but STRATCOM should coordinate with SOCOM to ensure full integration of PSYOP as a core capability of IO.

- (FOUO) Unified Command Plan (UCP) 02, Change 2. This change, approved in January 2003, included recommendations endorsed by the IO Roadmap. Specifically, STRATCOM was assigned responsibility for "integrating and coordinating DoD IO that cross geographic areas of responsibility or across the IO core capabilities."

  - (U) The UCP identified the core IO capabilities as CNA, CND, EW, OPSEC, PSYOP and military deception. It specified STRATCOM's role in IO to include:

    - (U) Supporting other Combatant Commanders for planning.

- (U) Planning and coordinating capabilities that have trans-regional effects or that directly support national objectives.
- (U) Exercising command and control of selected missions, if directed to do so by the Secretary or President.
- (U) Identifying desired characteristics and capabilities for DoD-wide CND, planning DoD-wide CND and directing DoD-wide CND.
- (U) Identifying desired characteristics and capabilities for CNA, conducting CNA in support of assigned missions, and integrating CNA capabilities in support of other Combatant Commanders, as directed.
- (U) Identifying desired characteristics and capabilities for joint EW and planning and conducting EW in support of assigned missions.
- (U) Supporting other Combatant Commanders for the planning and integration of joint OPSEC and military deception.

- (U) Responsibilities across OSD. A major deficiency identified in advancing IO as a core military competency is the "balkanization" of IO responsibilities across OSD.
  - (U) ASD(C3I) promulgates overarching IO policy, but responsibilities for policy, strategy, plans, operations and programs for IO capabilities are diffused across OSD in multiple offices within USD(P), ASD(C3I) and USD(AT&L).
  - (U) Creation of USD(I) introduces another organization with responsibilities related to IO.
  - (U) The need for a more streamlined OSD organizational IO construct became more pronounced once the UCP expanded STRATCOM's IO role on behalf of the other Combatant Commands.

(U) ***Desired Outcome.***

- (U) An effective DoD structure for force development, integration, planning, command and control and joint execution of IO as a core military competency.

(U) ***Recommendations (Numbers 10 - 12).***

(U) **Recommendation: Empower STRATCOM to undertake critical precursor activities for successful IO planning and execution (#10).**

- (U) A single four star Combatant Commander should be given responsibility for advocacy and oversight of IO capabilities to ensure they are capable of supported and supporting operations and that they are fully integrated into planning. This

recommendation is already underway as described above in the discussion on the UCP, Change 2. The terms of reference being developed by the CJCS for UCP implementation should specifically include authority and responsibility for STRATCOM to develop concepts for integrated IO, prioritize IO planning needs among regional Combatant Commanders, develop measures of effectiveness for IO, and promote IO in joint concept development and experimentation activities.

(U) **Recommendation: Streamline CNA and PSYOP organizational constructs and command and control (#11).**

- (U) The IO Roadmap developed a comprehensive series of recommendations for CNA and PSYOP. To aid in clarity and put the recommendations into proper perspective, these specific recommendations have been integrated into the respective CNA and PSYOP sections of this report.

(U) **Recommendation: Consolidate OSD Oversight of IO (#12).**

- (U) Consolidating OSD oversight of IO is advisable for two reasons. First, it would put one source firmly in charge with a level of authority sufficient to promote IO aggressively. Second, having one source in charge of all five core capabilities would improve the likelihood of their effective integration, which will be increasingly necessary to achieve desired effects.

- (U) The USD(P) should lead an Executive Committee to oversee implementation of the policies, programs and recommendations contained in this Roadmap. An immediate priority will be to translate the recommendations in this roadmap into a matrix that identifies the action, the approval authority, the lead for the action, required coordination, the mechanism for completing the action and the due date. All relevant components and agencies should designate a lead individual to support rapid implementation of the Roadmap recommendations. The target for full implementation should be one year. The USD(P) should provide periodic updates on progress to the Deputy Secretary of Defense.

- (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.

C. A Trained and Ready Career Force (U)

(U) This major study area incorporates a review of the personnel, training and education requirements necessary to transform IO into a core military competency.

1. Career Force (U)

(U) ***DPG Tasking***.

- (U) USD(P&R), in coordination with USD(P), ASD(C3I), CJCS and the Services will make recommendations relating to the IO career force. The recommendations will address career paths for IO personnel, accession, retention and promotion opportunities to Senior Executive and Joint Staff and Service flag/general officer level commencing in FY04.

(U) ***Current Situation***.

- (U) Service constructs of IO produce a varying work force. The five core capabilities of IO are not universally defined, understood or applied across the Service Departments. As a result, each Service develops specialists in those disciplines that meet Service-specific requirements.

- (U) Isolated communities of specialists. The complexity and technological growth in EW, PSYOP and CNO tend to isolate the specialists who practice these disciplines from one another.

  - (U) Unfortunately, there is often little application or awareness of the relationships of one core capability to the others.

  - (U) Not having personnel in the five core IO disciplines that are familiar with the other disciplines undermines efforts to apply IO as part of a common integrated approach to joint warfighting.

- (U) Retention of critical personnel may be a problem. Anecdotal evidence from the Services, collected during the course of IO Roadmap development, indicates that retention of personnel possessing these keys skill sets may be a challenge.

- (U) Military deception and OPSEC are often ignored. The growing superiority of U.S. military capabilities against conventional opponents devalues these time-honored skills. As a result, there are few trained practitioners that can demonstrate relevance to the overall planning process.

  - (U) OPSEC is largely an afterthought in planning even though doctrine and policy is widely promulgated. The OPSEC planning process developed for DoD is not widely applied.

  - (U) Personnel assigned to accomplish military deception and OPSEC planning on Combatant Command staffs are often assigned without any knowledge of these planning processes or the relevance to IO.

- (U) Few joint or service billets are coded for IO. Even though duty positions and assignments require personnel that may have IO skill sets, the Department lacks an accepted method of identifying IO qualified personnel to match IO skill requirements.

(U) ***Desired Outcome***.

- (U) DoD requires a cadre of IO professionals capable of planning and executing fully integrated IO in support of Combatant Commanders. An IO career force should be afforded promotion and advancement opportunities commensurate with other warfighting areas and provided opportunities for advancement to senior executive or flag level rank.

(U) ***Recommendations (Numbers 13 - 18)***.

(U) **Recommendation: Establish an IO career force (#13).**

- (U) As IO grows into a full military competency, it may be necessary to consider making IO a dedicated military occupation specialty or career field. For the time being, DoD should establish an IO career force comprising two categories: IO planners and IO capability specialists. To be successful, an IO career force will have to break some cultural norms. Isolated communities of personnel should begin to think of themselves as IO personnel rather than personnel participating in a core component of IO.

(U) **Recommendation: Develop IO planners (#14).**

- (U) These officers emerge from the more traditional warfighting career paths (e.g., fighter pilots, combat arms officers, service warfare officers and planners across all Services) and enter into planning assignments that require expertise in the five core capabilities.

  - (U) IO planners should serve alternating tours with IO assignments and with their basic branch or specialty to remain competitive.

  - (U) IO planners should understand the basic principles associated with CNO, EW and PSYOP and be capable of integrating their effects into Combatant Commander plans or orders.

  - (U) IO planners should be fully educated and trained to understand the planning principles associated with OPSEC and military deception.

(U) **Recommendation: Develop IO capability specialists (#15).**

- (U) IO capability specialists are functional experts in one or more of the highly specialized core capabilities of CNO, EW, or PSYOP.
  - (U) IO capability specialists should serve alternating tours between their specialized core capability and assignments as IO planners.
  - (U) IO capability specialists should possess specialized expertise on a certain IO core capability, but gain experience in the planning and execution of the broader construct of IO.
  - (U) IO capability specialists should be fully educated and trained to understand the planning principles associated with OPSEC and military deception.

(U) **Recommendation: Identify joint and Service IO billets (#16).**

- (U) USD(P&R) should work with the Services, STRATCOM and other joint commands to identify joint and Service IO billets that require IO career force personnel. Identification of these billets should drive Service manpower requirements for IO planners and IO capability specialists.
  - (U) Billet identification (through flag officer level) is the first step to ensure IO planners and IO capability specialists are assigned to the correct duty positions.
  - (U) Services should prioritize assignments to key IO billets within Combatant Command and Service staffs.

(U) **Recommendation: Provide focus for enlisted and civilians (#17).**

- (U) While initial focus of the IO Roadmap is on jump-starting the officer career force, DoD should also extend IO career force objectives to the enlisted and civilian domains.
  - (U) DoD should create opportunities for the enlisted and civilian IO career force specialties to focus on a particular subset of information skills. DoD requires a cadre of enlisted and civilian specialists that maintain proficiency with the guarantee of advancement and continued opportunity.

(U) **Recommendation: Monitor IO career force compliance across DoD (#18).**

- (U) USD(P&R) should establish parameters to monitor accession, retention and promotion rates for personnel in the IO career force.

2. Education and Training (U)

(U) ***DPG Tasking***.

- (U) Services, CJCS and Defense Agencies will make recommendations on expanding IO education and training including Joint Professional Military Education commencing in FY04 to support the development of IO professionals.

(U) ***Current Situation***.

- (U) IO education does not support the assignment process. Education and training for IO is "late to need" for officers reporting to Combatant Commands. All too often, officers assigned to Combatant Commands lack necessary operational IO planning experience and must depend upon on-the-job training. The general military population lacks an understanding of IO as well.

- (U) Education to meet IO career force requirements is not available. IO career force recommendations require a training and education infrastructure. Currently, DoD's education system can not meet these IO career force recommendations.

- (U) No standardized program of instruction to implement a shared DoD view of IO. Numerous schools offer IO instruction, but no accepted, standardized curricula exists for joint IO training or education. No single school or organization has responsibility to oversee joint IO curricula.

- (U) No central database for IO education or training. A central database, identifying all DoD IO courses (either Service or joint) does not exist. Such a repository would minimize training costs by avoiding duplication and provide a common registry of course schedules and capacity. A central database could also identify where potential shortfalls in courses exist as the IO career force evolves.

(U) ***Desired Outcome***.

- (U) A robust joint and Service education and training infrastructure underpinning the IO career force and general military population. IO education and training should focus not only on the specialized technical aspects of the five core capabilities, but also should address integrated planning and employment as well.

(U) ***Recommendations (Numbers 19 - 21)***.

(U) **Recommendation: Integrate IO earlier in education (#19).**

- (U) The general military population requires a deeper appreciation of IO. Incorporating IO into Professional Military Education and Joint Professional Military

Education will expand knowledge across DoD. CJCS should add IO to the joint learning areas that determine the content of joint military education.

- (U) Standardized curricula should be implemented at mid grade (04) and senior level (05-06) schools. Targeting this cross section of the general military population should produce the greatest impact.

- (U) Joint learning areas for IO should be introduced into company grade (03) and flag levels (07) education.

  - (U) Introductory instruction pertaining to IO should be pushed down to junior officers and Flag officers require executive level education on IO as well.

(U) **Recommendation: Expand/modify current IO training courses and/or develop new ones (#20).**

- (FOUO) Although there are several valuable courses and training programs offered across DoD, there is little standardization. Although the existing instruction may satisfy Service unique requirements, it was developed prior to the IO Roadmap with its construct and definition intended to move IO forward as a core military competency. The Joint Forces Staff College should be designated the lead to develop standardized joint IO curricula at mid and senior levels. PDM-1 provides the Joint Forces Staff College $7M over the FYDP with 8 additional military and 1 civilian billets. As the joint IO curricula coordinator, the Joint Forces Staff College should:

  - (U) Develop an expanded Joint IO Planners Course that will be a prerequisite for personnel assigned to the IO career force. This course should establish a common level of understanding for IO planner and IO capability specialists.

  - (U) Collaborate with Service schools to integrate joint IO curricula into their education and make recommendations to the JCS concerning which Service courses serve as an approved substitute to the Joint IO Planners Course.

  - (U) Maintain a central database of all DoD IO education and training for both specialized and full-spectrum IO courses to assist planning and make it web accessible. The data should be integrated into the master joint course database maintained by JFCOM for all joint individual training.

(U) **Recommendation: Establish a DoD Center of Excellence for IO (#21).**

- (U) Transformation requires exploration of new techniques, research and analysis of new concepts and an atmosphere where new ideas can be investigated. Historically, centers of excellence have provided DoD opportunities for rigorous examination of other transformational trends. An IO Center of Excellence will infuse the general military population with new ideas in a rapidly growing DoD core competency.

- (U) The Naval Post-Graduate School (NPGS) is implementing this intent today, but needs and should receive an official charter and funding from DoD.

- (U) The Deputy Secretary should officially designate NPGS as a DoD Center of Excellence to:

  - (U) Provide graduate level, full-spectrum IO core and specialty programs across the technical and psychosocial dimensions.

  - (U) Sponsor short courses for executive and professional development. The IO quarterly seminars, previously conducted at the National Defense University, should be funded.

  - (U) Develop curricular innovations for discussion and dissemination through joint IO curricula conferences to:

    - (U) Enable institutions to share experiences and improve quality of instruction across the Department.

    - (U) Distribute state of the art IO technologies and best practices to DoD educators.

  - (U) Provide assistance to joint doctrine development and innovation through analysis and research.

    - (U) Monitor and analyze commercial technological developments.

D. Focused Analytic and Intelligence Support (U)

(U) This major study area addresses analytic and intelligence support to IO. It includes recommendations to merge kinetic and non-kinetic analysis and makes the case for a single DoD focal point to integrate and collate EW data.

1. Analytic and Intelligence Support (U)

(U) ***DPG Tasking***.

- (U) ASD(C3I), in coordination with the CJCS and Services, should make recommendations to establish in FY04 an integrated IO support capability to Combatant Commanders that effectively characterize targets, improves weaponeering and matures IO measures of effectiveness.

(U) ***Current Situation***.

- (S) Need for analytic support. Combatant Command staffs lack organic capability to rapidly analyze complex systems and generate IO target sets. They need support from a robust analytical center that combines multi-discipline analysis capability with specifically tailored intelligence supporting IO. [redacted] including Joint Warfighting Capability Assessments, the 2000 IO Broad Area Review, the 2001 Quadrennial Defense Review, as well as operational lessons learned in Kosovo and Afghanistan [redacted] Combatant Command staffs can not currently produce rapid solutions for tailored IO effects for the following reasons:
  - (U) Lack of sufficiently detailed intelligence data to support IO planning.
    - (S) [redacted]
    - (S) [redacted]
  - (U) Lack of sufficient staff expertise. Combatant Commanders do not have the trained manpower to conduct the analysis necessary for effective IO planning.
  - (S) [redacted]

- (S) [redacted]

(U) ***Desired Outcome.***

- (U) Rapid, fully integrated nodal and network analysis providing Combatant Commanders with holistic kinetic and non-kinetic solutions for a full range of electromagnetic, physical and human IO targets.

(U) ***Recommendations (Numbers 22 - 26).***

(U) **Recommendation: Develop a program for intelligence support to full spectrum IO (#22).**

- (U) Intelligence is a fundamental prerequisite for full spectrum IO. The growth of IO as a core competency is in some respects contingent upon the quality and timeliness of supporting intelligence. USD(I) should oversee the achievement of accurate and timely intelligence in support of the core IO capabilities to provide the access, precision targeting and rapid battle assessment required for fully developed and integrated IO. Among other things, the USD(I) program should focus on:
  - (U) Timely, multidisciplinary, integrated targeting intelligence that allows commanders to choose the best combination of kinetic and non-kinetic options.
  - (U) Better depiction of the attitudes, perceptions and decision-making processes of an adversary. Understanding how and why adversaries make decisions will require improvements in Human Intelligence (HUMINT) and open source exploitation, as well as improved analytic tools and methods.
  - (U) Timely, accurate, relevant and actionable EW intelligence that is integrated in a single source for rapid exploitation by operators.
  - (U) Greater investment in all types of intelligence to develop and maintain target network access in support of Combatant Commander CNA requirements. Cultural change and new priorities will be required if the intelligence community is to make a commitment to exploitation of networks that may not yield much priority intelligence but which are critical targets in an operation plan.
  - (U) Greater attention to the ability of adversaries to "read" U.S. intentions and capabilities from poor OPSEC practices. These analytic intelligence products would greatly assist efforts to improve OPSEC practices throughout the Combatant Commands.

(U) **Recommendation: Provide dedicated support from a single analytic organization (#23).**

- (U) STRATCOM should create a Joint Integrative Analysis and Planning Capability (JIAPC), with USD(I) and CJCS oversight, that provides focused, timely analysis, planning and targeting in support of Combatant Commanders. The JIAPC constitutes an integrated network of analysis centers that, properly managed, could provide holistic analytic support to Combatant Commanders.

  – (U) JIAPC should provide rapid, responsive analytic support. Based on Combatant Commander needs, JIAPC should provide:

    - (U) Single point access to DoD's entire community of IO analytic experts.
    - (U) Prioritization of requests for intelligence to ensure timely response to critical operational needs.
    - (U) Integrated and mutually supporting analysis and planning in support of Combatant Commander effects-based operations.

  – (U) JIAPC should provide seamless holistic target characterization. JIAPC should present targeting options based on links-and-nodes analysis within and across the human, electromagnetic and physical domains. The focus of this effort should be an integrated IO concept that contributes to the broader plan. JIAPC should prioritize the missions and integrate the capabilities of the following organizations based on Combatant Commander needs:

    - (U) Electronic-Space and Human Factor Analysis Center (HFAC). To facilitate further growth in the analytic community, STRATCOM should establish command relationships with the E-Space Center and HFAC.

      – (U) STRATCOM, in coordination with USD(I), should develop memorandums of agreements with the DIRNSA regarding the E-Space and the Director Defense Intelligence Agency on the HFAC.

    - (U) Joint Warfare Analysis Center (JWAC). JWAC should provide the Combatant Commands, Joint Staff, and other customers with effects based, precision targeting options, for selected networks and nodes.
    - (U) Joint Information Operations Center (JIOC). Already assigned to STRATCOM, the JIOC provides integrated IO planning support to Combatant Commanders. JIOC support teams should work with Combatant Commands to identify and shape analytic requirements.

(U) **Recommendation: Assign JWAC to STRATCOM (#24).**

- (U) The IO Roadmap recommendation was to assign JWAC to STRATCOM. This recommendation would give STRATCOM all the key elements in the IO analytic support chain: intelligence for battlespace characterization, targeting and planning support. It would better permit STRATCOM to support integrated effects-based targeting with consolidated kinetic (nuclear and conventional) and non-kinetic (space and IO) expertise to meet theater and national objectives.

- (U) However, the JWAC affects a wider range of capabilities than IO. For this reason, during a March 2003 briefing on the IO Roadmap, the Secretary asked the CJCS to work with STRATCOM and JFCOM and recommend the best solution for the full range of missions supported by JWAC.

(U) **Recommendation: Enhance analytical capability over time with continual improvements in virtual collaboration (#25).**

- (FOUO) Initially, separate analytic centers at the DIA, NSA and JWAC should operate virtually in a collaborative environment with STRATCOM providing overarching guidance. Linking the centers virtually should maximize integration and minimize costs of physically co-locating the centers. The PDM-1 provided STRATCOM $23M across the FYDP to improve the virtual collaboration. Should virtual integration prove inadequate, DoD should consider a physical co-location.

(U) **Recommendation: Adopt a joint integrated planning capability (#26).**

- (U) The Air Force currently sponsors an IO planning capability. DoD should expand the Air Force's Information Warfare Planning Capability (IWPC) into a standardized IO planning capability at the joint level. This capability will serve as a suite of automated data analysis and decision support software tools designed to facilitate IO planning by Combatant Commanders. It will enable users to:

  - (U) Accomplish intelligence preparation of the battle space.
  - (U) Develop IO strategy and candidate IO campaign targets.
  - (U) Plan IO missions.
  - (U) Monitor and assess execution.

2. Electromagnetic-Space Analysis Center (U)

(U) ***DPG Tasking***.

- (U) ASD(C3I), in coordination with the USD(AT&L), will develop direction for the Electromagnetic-Space (E-Space) Analysis Center to provide analytic and technical

intelligence support to EW operational planning and advanced EA development programs.

(U) ***Current Situation***.

- (U) Requirements. The evolving IO mission area demands new and greater degrees of intelligence support in terms of collection, processing, analysis and dissemination.

- (S) Shortfalls. Current EW support processes do not always meet the needs of today's decision-makers or Combatant Commanders.

  – (S) Shortcomings in actionable (timely and accurate) data, [redacted] sometimes serve to burden operational customers with an abundance of information.

    - (U) Incomplete analysis of information or information at the wrong time or location is as problematic as a lack of information.

  – (S) EW [redacted] and services to individual customers. Adequate smart "push and pull" systems do not exist to disseminate the right data, to the right customer, at the right time.

- (U) Creation of an Electromagnetic-Space Analysis Center. The E-Space Analysis Center was established at Fort Meade, in August 2002 to fill this recognized void.

(U) ***Desired Outcome***.

(S) E-Space Analysis Center should produce operationally actionable, targeting quality information on foreign electromagnetic capabilities and networks, [redacted]

(U) ***Recommendations (Numbers 27 - 28)***.

(U) **Recommendation: E-Space Analysis Center should be DoD's focal point for intelligence support to EW (#27).**

- (U) USD(I) should oversee the evolution of the E-Space Center to provide:

  – (S) Timely, accurate, relevant and actionable EW intelligence that responds to EW user needs.

    - (S) [redacted]

  - (U) Necessary tools and collaborative mechanisms for easy access to and sharing of the data.

  - (U) Reliable knowledge-based data mining techniques, so that EW data is the "best" available to meet particular needs.

- (U) Modeling and simulation capabilities to assist user's asset deployment and employment.

- (U) Resident EW analytic capability to support a full range of user requirements, including assistance in the resolution of data conflicts.

(U) **Recommendation: E-Space Analysis Center should maintain an authoritative source of EW data (#28).**

- (U) When fully developed, the center should act as a single point of contact and the authoritative source for EW data to support operators, planners, and developers. Improvements over the current EW environment include:

  - (U) Enhanced customer access to a single portal for EW data. This precludes sifting through a variety of voluminous and often conflicting data sources.

  - (U) A higher degree of assurance that requests for EW data are the most current and meet mission needs.

  - (U) Greater consistency in and understanding of EW capabilities from requirements through capability development and ultimately operational employment.

E. Enhancing IO Core Capabilities (U)

(U) This major study area incorporates analysis and recommendations for the IO core capability areas of CNO (including separate discussions on CND and CNA), as well as the current status and recommendations for improving EW, PSYOP, military deception and OPSEC.

1. Computer Network Defense (U)

(U) ***DPG Tasking***.

- (U) DPG 04 identified three CND study areas:
  - (U) CND Integration. USSPACECOM (later STRATCOM), in coordination with CJCS, ASD(C3I), Services and Agencies, will make recommendations on integrating detection, protection, analysis and response capabilities for CND across DoD, including vulnerability assessment programs.
  - (U) CND Attribution. ASD(C3I) will coordinate with DISA, NSA and USSPACECOM (later STRATCOM) to develop recommendations that apply resources to achieve the technical capability for rapidly characterizing and attributing the threat in support of CND.
  - (U) CND Insider Threat Mitigation. Services and Agencies will counteract the insider threat by enforcing training and personnel standards and deploying the required tools on the information infrastructure to effectively monitor and manage the networks.

(U) ***Current Situation***.

- (S) Networks are growing faster than we can defend them. [redacted] As a result, greater vulnerability results from enterprise expansion. Specifically:
  - (S) Unprotected networks surrender asymmetric advantage. DoD has focused attention on improving the security of its networks, but the Department's [redacted]
  - (S) Attack sophistication is increasing. The sophistication and capability of both hackers and nation-states to degrade system and network operations are rapidly increasing. [redacted]

- (S) Number of events is increasing. The number of detected events on DoD networks continues to grow while [redacted]

- (S) Exercises demonstrate our vulnerabilities. Exercise ELIGIBLE RECEIVER 03 demonstrated gross vulnerabilities resulting from [redacted]

  - (S) [redacted]

- (S) [redacted]

  - (S) Latest tools are not available. [redacted]

  - (S) Near and long-term threats. [redacted]

(U) ***Desired Outcome***.

- (U) A robust, layered defense across DoD enhanced through global and enclave situational awareness with the centralized capability to rapidly characterize, attribute and respond to attacks.

(U) ***Recommendations (Numbers 29 - 34)***.

(U) **Recommendation: DoD should implement a Defense in Depth strategy (#29).**

- (U) This strategy should be based on the premise that the Department will "fight the net" as it would a weapons system.

  - (U) The strategy must be carefully constructed and managed to give senior leaders high confidence that additional investments in network defense will ensure the graceful degradation of the network rather than its collapse. Like any real strategy it should take into account the limited resources and balance them against known risks.

  - (U) The strategy must embrace a concept of operation that self-consciously identifies and manages risk. 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 with the goal of ensuring:

- (U) Sufficient protection of the information architecture to initiate combat operations in all circumstance and on preferred timelines (harden).
- (U) Sufficient information architecture during conflict to defeat an adversary (battle management).
- (U) The ability to quickly reconstitute information architecture to pre-conflict levels in order to restore readiness for the next conflict.

- (U) The Defense in Depth strategy should include:
  - (U) Robust network defensive infrastructure including demilitarized zones, insider threat protection and firewalls.
  - (U) Well-configured networks that slow down and channel the attacker.
  - (U) Vertical and horizontal situational awareness and configuration management to enable effective command and control of defensive operations.
  - (U) A CND concept of operations that allows for varied defensive postures consistent with minimum required functionality.
  - (U) The ability to conduct reconstitution operations that enable the DoD infrastructure to absorb attacks, minimize degradation and maintain critical network functionality.
  - (U) Well-integrated CNA/CND efforts that permit us to maximize opportunities for CNA and minimize vulnerabilities in our CND efforts.
  - (U) Situational awareness and battle management tools to provide the capability for attack sensing and warning, event correlation, attribution and forensics.

- (U) Other near-term recommendations to implement the Defense in Depth strategy include:
  - (U) Expand and standardize the DoD vulnerability management and reporting capabilities.
  - (U) Develop and implement a cyber-event attribution capability.
  - (S) Coordinate with the [redacted] to expand upon the current, [redacted] and analysis capability to achieve improved situational

- (S) Coordinate with the [redacted] that mitigates DoD-wide risk while providing continued support to the operational mission.
  - (U) These capabilities result in reduced response times associated with detection and response.
  - (U) These capabilities also support rapid reconstitution of affected portions of the enterprise.

(U) **Recommendation: DoD should develop a full-time, well-trained professional cadre of certified system and security administrators (#30).**

- (U) To keep pace with and protect the expanding network, it is imperative to provide sufficient manpower and enforce education and training certification requirements.
- (U) Ultimately, however, the Department should raise a dedicated force of network defenders separate from the system administrators. System administrators will always tend to focus on day-to-day functionality, rather than train and prepare for deliberate large-scale attacks that happen infrequently. Therefore, the Department should develop a plan for gradually raising up and integrating dedicated network defenders who will be able to respond immediately to limit and actively channel attacks.

(U) **Recommendation: Fully implement Public Key Infrastructure (#31).**

- (U) Public Key Infrastructure (PKI) should be fully implemented on classified and unclassified networks. PKI will add protection in the form of both authentication and access control on automated networks. Additionally, PKI:
  - (U) Allows only authorized personnel have access to the network.
  - (U) Complicates masquerading as another individual and increases the ability to track down insider threats.
  - (U) Helps force an adversary to target specific machines to obtain unencrypted data, instead of gaining network level access.

(U) **Recommendation: Review STRATCOM's relationship to DoD CND forces (#32).**

- (U) STRATCOM can better integrate CND efforts if they have a defined command and control relationship with Services and Agencies. Currently, STRATCOM has Tactical Control of Service CND forces, but not a formal relationship to the defense agencies. STRATCOM, in coordination with CJCS, ASD(NII), the Services and

Defense Agencies should conduct a study and make recommendations to the Secretary by 1 December 2003 on improvements for CND command and control.

(U) **Recommendation: Incorporate CND recommendations in program reviews (#33).**

- (U) Remedial action to improve network protection in the manner described above should be given a high priority in subsequent program reviews.
  - (U) As the Department continues to move toward dependence on automated networks, a balance should be struck between functionality and protection.

(U) **Recommendation: Develop supplemental guidance for DoD's CND response actions (#34).**

- (U) Recent CND policy established three tiers of response actions with corresponding levels of approval authority. The objective of this policy is to strengthen DoD's defensive posture, halt or minimize attack effects or damage and support rapid, complete attack characterization.
  - (U) The three tiers of authorized activity are:
    - (U) Tier 3: Local and intermediate commanders are authorized to take internal and administrative actions that do not extend outside the local enclave.
    - (U) Tier 2: STRATCOM and component commanders are authorized to take actions that affect DoD networks and CND operations across multiple DoD networks.
    - (U) Tier 1: STRATCOM is authorized to take defensive measures/activities that may minimally and temporarily adversely affect adversary systems and may have a similar affect upon intermediate systems.
  - (U) STRATCOM should articulate supplemental DoD guidance to identify and develop specific response actions and determine the appropriate range of those response actions within the hierarchy above.

2. Computer Network Attack (U)

(U) ***DPG Tasking***.

- (S) SPACECOM (later [redacted] should propose to the CJCS recommendations to [redacted] with measures of effectiveness that address collateral damage and probabilities of success.

(U) ***Current Situation***.

- (S) [redacted]
  - (S) A comprehensive interagency process is underway to evaluate the use of offensive cyber tools and develop national policy. USD(P), in coordination with USD(I), CJCS, and DoD GC, is providing DoD's input to develop the [redacted]
- (FOUO) UCP responsibility. The UCP02, Change 2 assigns STRATCOM responsibility for identifying desired capabilities and characteristics for CNA, conducting CNA in support of assigned missions and integrating CNA capabilities in support of other Combatant Commanders as directed.
- (S) Confidence in CNA. There is a [redacted] between the Combatant Commander's expectations, the [redacted] and [redacted]
- (S) Current approval authority. Currently, the [redacted], intelligence gain/loss arbitration and deconfliction of operational CNA plans with the Intelligence Community.
- (S) [redacted]
- (S) Intelligence support. Combatant Commanders have provided generic target types, requirements and desired effects [redacted] and weapons development organizations to provide operational CNA capability.
- (S) Exploitation versus attack. [redacted]
- (S) <u>Prioritization</u>. DoD does not adequately prioritize CNA requirements between Combatant Commands.

(U) ***Desired Outcome***.

- (U) Forces trained with well-tested and reliable CNA weapons that are aligned with appropriate target sets and integrated with other IO capabilities and weapon systems.

(U) ***Recommendations (Numbers 35 - 44)***.

(U) **Recommendation: Develop national policy for offensive cyber operations (#35).**

- (S) The IO Roadmap effort identified key issues that should be addressed in the [redacted] that is currently under development.
  - (S) [redacted]
    - (S) [redacted]
    - (S) [redacted]
  - (S) [redacted]
  - (S) [redacted]
  - (S) [redacted]
    - (S) [redacted]
    - (S) [redacted]
    - (S) [redacted]

- (S) [redacted]

– (U) Employment policy issues.

- (S) [redacted]

– (U) Declaratory policy. The USG should have a declaratory policy on the use of cyberspace for offensive cyber operations based on the following points:

- (S) [redacted]
- (S) [redacted]
- (S) [redacted]
- (S) [redacted]
- (S) [redacted]
- (S) [redacted]
- (S) [redacted]
- (S) [redacted]

– (U) Review of legal authorities.

- (S) A decision on when CNA constitutes a use of force is needed to clarify legal authorities both for using and responding to computer network attacks:
  - (U) A legal review should determine what level of data or operating system manipulation constitutes an attack. This distinction is necessary to clarify which actions can be appropriately taken in self-defense and whether an action is an attack or an intelligence collection operation.
  - (S) DoD requires a legal regime that responds separately to domestic and foreign sources of CNA. A legal regime for handling the difficulty of distinguishing between domestic and foreign sources of attack in cyberspace is required. It should capitalize on newly acquired authorities provided by the Patriot and Homeland Security Acts.
  - (U) Legal review should determine if appropriate authorities permit attack through unwitting hosts (merely transiting or controlling the host in order to launch the attack) if the action elicits an attack against the host computer system.
  - (U) Legal review should determine what level of certainty about the origin of an attack is required before the U.S. can respond in kind.
- (U) Intelligence Support Requirements.
  - (S) [redacted]
  - (S) [redacted]
  - (S) Greater integration of intelligence and operations, and a major increase in priority for these activities is required.

(U) **Recommendation: Adopt a common understanding of the "CNA battlefield" (#36).**

- (S) CNA can be executed at the tactical, theater or strategic levels. Delineating these levels of CNA in cyberspace is difficult. In some cases, tactical means of access can enable strategic targeting and vice versa. Nevertheless, some general rules of the road concerning targets are possible.

- (S) At the strategic level, targets include [redacted] and sensitive targets (national, nuclear command and control, etc.) that may have a high operational and/or intelligence value.
  - (S) [redacted]
  - (S) For most of these targets, effective exploitation of these targets will require [redacted] with a high standard of stealth, characterized, not only by non-attribution, but also non-[redacted].
  - (S) [redacted]

- (S) [redacted]
  - (S) [redacted] can facilitate theater [redacted] but often, assigned [redacted]

- (S) [redacted]
  - (S) [redacted]
    - (S) In addition, since the [redacted]
    - (S) [redacted]

(U) **Recommendation: Assign combatant command (COCOM) of CNA forces to STRATCOM (#37).**

- (S) [redacted] constitute small pockets of expertise embedded in [redacted]. The [redacted] are closely aligned with, and in many cases are, [redacted].

Assigning them to Commander STRATCOM enables shaping and focusing these forces to better accomplish DoD's emerging joint CNA mission.

- (S) A COCOM relationship allows STRATCOM to conduct real-time planning, integration, and execution of trans-regional CNA. It also facilitates STRATCOM's ability to mold this capability by standardizing joint training, designating objectives, (i.e., specifying lanes in the roads for Service components) and effectively organizing to better plan and execute CNA as a supporting or supported command.

(S) Recommendation: STRATCOM should develop a robust [redacted] that [redacted] (#38).

- (S) Commander STRATCOM is creating a subordinate Joint Force Headquarters-Information Operations (JFHQ-IO) led by the Deputy Commander STRATCOM, with subordinate components to be assigned attack planning, integration, coordination, deconfliction and execution functions for CNA.

- (S) USD(I) should prepare a memorandum for the Secretary assigning [redacted] authority to plan, integrate and, when directed, [redacted]. With this memorandum, [redacted] can:

  - (S) Capitalize on [redacted] to facilitate the planning and integration of CNA.

  - (S) Deconflict [redacted] between the [redacted] and DoD.

  - (S) [redacted]

  - (S) Secure necessary assistance from the [redacted] to conduct [redacted] on those [redacted] requirements identified by the Combatant Commanders and prioritized by [redacted].

  - (S) [redacted].

- (S) Commander STRATCOM should establish a staff element [redacted] to carry out [redacted]. This staff should combine personnel from [redacted]. PDM-1 provides $62M over the FYDP to integrate intelligence capabilities into STRATCOM's CNA mission.

- (S) With COCOM of Service CNA forces, Commander STRATCOM could delegate operational control to his subordinate commands.

- (S) These arrangements provide unity of effort and allow for the [redacted] who have been responsible for exploiting a particular target in peacetime--or working side by side [redacted] doing so--to attack targets with high confidence of success when directed by Commander STRATCOM.

(S) Recommendation: Use the [redacted] relationship to deconflict [redacted] (#39).

- (S) [redacted]

  - (S) [redacted] should use [redacted] should provide STRATCOM recommendations on:

    - (S) [redacted]

    - (S) [redacted] on those CNA requirements identified by the Combatant Commanders and prioritized by STRATCOM. Specifically, he should coordinate CNA intelligence taskings, access development and research and development to support attainment of desired affects and capabilities.

    - (S) STRATCOM should use its relationship with [redacted]

      - (S) [redacted]

- (S) [redacted]

- (S) DoD and the [redacted] should develop a deconfliction memorandum of agreement. As the Department improves its ability to [redacted] as a core IO capability, DoD should fully leverage [redacted], while balancing intelligence and operational equities. USD(I), in coordination with USD(P) should work with the [redacted] and develop policy and procedures to:

  - (S) Coordinate [redacted] and operating concepts.

    - (S) Ensure the [redacted] provides required [redacted] targets.

  - (S) Enhance DoD and [redacted] collaboration on [redacted] capabilities.

  - (S) Appoint the [redacted] as the focal point for the [redacted] and DoD (under STRATCOM sponsorship) to coordinate [redacted] efforts.

(U) **Recommendation: Delegate specific CNA targets to Combatant Commanders (#40).**

- (S) In coordination with Commander STRATCOM and upon approval by the Secretary, the CJCS should modify the [redacted] as follows:

  - (S) Once the [redacted] has approved military operations, [redacted] should have [redacted] to facilitate rapid response and provide additional strike options, i.e.

    - (S) [redacted]

  - (S) [redacted]

- (S) In addition, Combatant Commanders are encouraged to submit requests for specific other CNA targets not included in these categories. [redacted]

(U) **Recommendation: Categorize and delegate selected CNA weapons (#41).**

- (S) DIRNSA, as the Executive Agent for the [redacted] should engage IOTC to apply its technical expertise to make recommendations to STRATCOM on the categorization of [redacted] STRATCOM should then forward recommendations through the CJCS, to OSD to support weapon apportionment and allocation recommendations. [redacted] should direct IOTC to use the following criteria to categorize CNA weapons:

- (S) [redacted]
  - (S) [redacted]
  - (S) [redacted]
    - (S) [redacted]
    - (S) [redacted]
    - (U) [redacted]
  - (U) From these criteria, STRATCOM should recommend that weapons be grouped into one the following categories:
    - (U) Category I: Capabilities allocated to a Combatant Commander.
    - (U) Category II: Capabilities pre-allocated to support a specific aspect of an operations plan (OPLAN) or contingency plan (CONPLAN).
    - (U) Category III: Capabilities not allocated to Combatant Commanders and therefore requiring Secretary or Presidential approval to employ.
  - (S) The [redacted] and should be ensured the necessary visibility to determine whether [redacted]

(U) **Recommendation: Develop an integrated network of IO and CNA ranges (#42).**

- (U) STRATCOM, in coordination with OSD and the Services, should oversee development of an integrated network of ranges that test emerging IO capabilities.

- (U) DoD requires an integrated test range to increase confidence and better assure predictable outcomes. The test range should support exercises, testing, and development of CNA, EW and other IO capabilities.

- (U) Funds were allocated to STRATCOM as part of PDM-1 to lay the foundation for funding this integrated network in FY05.

(U) **Recommendation: Establish assurance testing standards (#43).**

- (U) Although each Service has a CNA acquisition process, there are no well-defined CNA assurance standards. DoD should develop common standards for technical testing and evaluation.

  - (U) DIRNSA, as Executive Agent for the Information Operations Technology Center (IOTC), should engage the IOTC to employ its technical expertise in developing and applying assurance standards for validation and promulgation in conjunction with the Directorate of Operational Testing and Evaluation (DOT&E).

    - (S) The [redacted] and should be ensured the necessary visibility to determine whether CNA tools have gone through assurance testing and been categorized as potential weapons.

  - (U) Services should apply these assurance standards as they conduct operational testing evaluations.

(U) **Recommendation: Assign STRATCOM executive agency for joint CNA (#44).**

- (U) As executive agent, STRATCOM should serve as the primary DoD point of contact and proponent for joint CNA doctrine, training and equipment and should lead, coordinate and integrate the activities of the other DoD Components on such matters.

  - (U) STRATCOM should develop and promulgate joint tactics, techniques and procedures for CNA and coordinate the training of CNA forces.

  - (U) STRATCOM should maintain visibility on all DoD CNA and related programs to minimize duplication of effort.

  - (U) STRATCOM should be the focal point for CNA requirements in DoD. To do this, STRATCOM should assist Combatant Commanders in identifying requirements, then prioritize these requirements across each area of operations.

3. Electronic Warfare (U)

(U) ***DPG Tasking***.

- (U) DPG 04 tasked USD(AT&L), in coordination with the CJCS and Services, to develop recommendations to transform and extend EW capabilities, including the EA-6B follow-on, to detect, locate and attack the full spectrum of globally emerging telecommunications equipment, situation awareness sensors and weapons engagement technologies operating within the electromagnetic spectrum.

(U) ***Current Situation***.

- (U) Lessons "not learned." A number of studies over the past several years, including Joint Warfighting Capabilities Assessments (JWCA) and the Airborne EA Analysis of Alternatives Study, reached the following conclusions with respect to current EW capabilities.
  - (S) [redacted], with disproportionate emphasis on the Suppression of Enemy Air Defense mission.
  - (S) [redacted]
  - (U) No central investment strategy. DoD lacks a coherent EW vision. EW enhancements are largely service specific with decentralized development efforts and operations.
  - (S) [redacted].
- (S) [redacted]
  - (S) Current programs do not address low probability of [redacted] capabilities, agile and spread-spectrum waveforms and advanced networking.
  - (U) While some of these concepts are not yet widely fielded, EW concepts and technologies should be developed today to successfully counter them in future operations.

  - (S) [redacted]

- (S) [redacted]

  - (U) Investment in EW may provide alternative options for protecting and attacking potential targets by costly or unsuitable kinetic capabilities. Examples include the non-kinetic disruption of WMD facilities and disabling/disruption of missiles prior to launch.

- (S) EW net assessment. Although afforded only a cursory review of classified programs, the following assessment of current EW programs is not generally disputed:

  - (S) Current EW capabilities largely focus on electronic protection and the Suppression of Enemy Air Defense mission.

  - (S) There is no effective joint advocacy or planning for EW.

  - (S) [redacted]

  - (S) Future EW systems will need to be flexible enough to counter the rapid development and fielding, and likely proliferation of inexpensive weapon systems founded on sophisticated commercial-off-the-shelf technologies.

  - (S) [redacted]

  - (S) Future capabilities should contain modular systems with common technology, hardware and software on multiple platforms and common technical requirements that can be updated rapidly through technical or intelligence efforts.

(U) ***Desired Outcome***.

- (U) Achieve "Dial an Option" Electronic Attack capabilities that deny adversary situational awareness, disrupt command and control and develop targeting solutions to defeat weapons while protecting ours against the same.

(U) ***Recommendations (Numbers 45 - 46)***.

(U) **Recommendation: Formally establish and charter an EW Executive Steering Group (#45).**

- (U) USD(AT&L) should chair an EW Executive Steering Group that includes senior representation from USD(P), USD(I), DDR&E, Joint Staff, Services and STRATCOM. The Executive Steering Group should be empowered to develop and implement a coherent multi-Service EW investment strategy based on a comprehensive joint EW operational architecture that supports a concept of operations for integrated IO. The EW architecture and investment strategy should:
  - (U) Cover the full range of EW missions and capabilities, including navigation warfare, offensive counterspace, control of adversary radio frequency systems that provide location and identification of friend and foe, etc.
  - (U) Provide a future EW capability sufficient to provide maximum control of the entire electromagnetic spectrum, denying, degrading, disrupting, or destroying the full spectrum of globally emerging communication systems, sensors, and weapons systems dependant on the electromagnetic spectrum.
- (U) The steering group should oversee development of both the EW operational architecture and the supporting investment strategy. To execute this mandate the Executive Steering Group should:
  - (U) Have oversight of all EW programs (including special access and compartmented programs).
  - (U) Have direct linkage and interaction with Combatant Commands on EW concepts of operation and capability needs.
- (U) A subordinate EW Integrated Process Team (IPT) should report to the Executive Steering Group and have the primary objective of developing the comprehensive EW roadmap as described below.

(U) **Recommendation: Develop an EW roadmap (#46).**

- (U) To fulfill the mandate assigned to the Executive Steering Group, the EW Roadmap should:
  - (U) Provide an EW architecture that:
    - (U) Controls the electromagnetic spectrum with integrated but decentralized execution.
    - (U) Functions across service and platform boundaries.

- (U) Acts across the full range of the electromagnetic spectrum.
- (U) Is distributed and scalable to operations.
- (U) Delivers timely information and knowledge of environment in compatible formats.

– (U) Develop a coherent and comprehensive EW investment strategy for the architecture that:

- (U) Identifies capability shortfalls and accelerates high-payoff emerging technologies.
- (U) Pays particular attention to:

  – (U) Projecting electronic attack into denied areas by means of stealthy platforms.

    - (U) As a matter of priority, accelerates joint development of modular EW payloads for the Unmanned Combat Aerial Vehicle.

  – (U) Provide for common, affordable active and passive countermeasures.

    - (U) As a matter of priority, provide effective countermeasures for non-fixed wing aviation consistent with the recommendations of the Non-Fixed Wing Aviation Study directed by PDM-1.

- (U) Exploits other transformational EW initiatives, including use of the E-Space Analysis Center to correlate and fuse all available data that creates a real time electronic battlespace picture.

– (U) Develop options for improving operator access to classified EW programs and make recommendations on whether changes are required in policies and procedures for delegation of authority to apportion, allocate and use classified EW capabilities.

4. Psychological Operations (U)

(U) ***DPG Tasking***.

- (U) DPG 04 tasked USSOCOM to provide, in coordination with the CJCS and the Services, options and recommendations to enhance the current PSYOP force structure, modernize PSYOP capabilities and create a strategic PSYOP force.

(U) ***Current Situation***.

- (S) Degradation of capability. Over the last decade, numerous studies have documented the deterioration of the PSYOP capabilities and recommended remedial action. Although not officially categorized as such, PSYOP has long been recognized as a low-density, high-demand asset, which is particularly valued in the war on terrorism. Well-documented PSYOP limitations include:

  - (U) Inability to rapidly generate and immediately disseminate sophisticated, commercial-quality products targeted against diverse audiences.

  - (U) Insufficient numbers of experienced fully qualified and well equipped PSYOP personnel with diverse linguistic capabilities.

  - (S) Limited ability to disseminate PSYOP products into denied areas.

    - (U) Leaflets, handbills, AM radio and Commando Solo have a limited range and/or are resource intensive.

(U) ***Desired Outcome***.

- (U) A PSYOP force ready to conduct sophisticated target-audience analysis and modify behavior with multi-media PSYOP campaigns featuring commercial-quality products that can be rapidly disseminated throughout the Combatant Commanders area of operations.

(U) ***Recommendations (Numbers 47 - 51)***.

(U) **Recommendation: Coordinate DoD and USG themes and messages (#47).**

- (U) OSD oversight of PSYOP should include the requirement to ensure PSYOP messages are congruent with national themes and objectives.

(U) **Recommendation: Create a Joint PSYOP Support Element (#48).**

- (S) DPG 04 directed the creation of a "strategic" PSYOP unit. The title of this unit was changed to reflect IO Roadmap recommendations on the proper relationship of PSYOP to public diplomacy and public affairs (see previous section on this topic). However, the intent remains the same, which is that the Joint PSYOP Support Element should:

  - (S) Coordinate Combatant Command programs and products with the Joint Staff and OSD to ensure PSYOP integration with overall USG themes and messages.

  - (S) Rapidly develop commercial-quality prototypes on behalf of the Combatant Commanders and the Secretary.

  - (U) Contract for commercial sources for enhanced product development.
  - (U) Determine appropriate subject matter experts as proxies for target audiences to pre-test anticipated effects whenever possible.

- (FOUO) PDM-1 authorizes $48 million across the FYDP to the Joint PSYOP Support Element with 15 civilian funded spaces in FY04 and 55 military billets commencing in FY05.

(U) **Recommendation: Delegate product approval for select categories of PSYOP products (#49).**

- (U) USD(P) should retain PSYOP program approval authority. Product approval for the following categories should be delegated to Combatant Commanders.
  - (U) Products that support friendly force protection.
  - (U) Products associated with safety or mine awareness.
- (U) USD(P) should retain product approval authority for those products with substantial political or strategic content or implication. This responsibility requires dedicated staff and clear procedures in order to avoid costly delays in the approval process.
  - (U) Once an operation is underway, USD(P) should delegate approval authority to Combatant Commanders for additional products and modifications of pre-approved products.

(U) **Recommendation: Enhance the current PSYOP force structure (#50).**

- (U) The IO Roadmap endorses the SOCOM and the Army expansion efforts that are already underway.
  - (U) Expansion provides two additional active component regional PSYOP companies within the 4th PSYOP Group, one to support CENTCOM (FY05) and a second to support PACOM (FY06). It also activates four additional reserve component regional companies (FY05).
    - (FOUO) PDM-1 provided $50M for the required procurement, military construction and operations and maintenance funding to create these units.
    - (U) These increases will enable the Army PSYOP force structure to have multi-component battalions (2 x active and 1 x reserve companies) focused on each regional Combatant Commander's area of operations -- SOUTHCOM, EUCOM, PACOM and CENTCOM.

(U) **Recommendation: Modernize PSYOP force capabilities (#51).**

- (U) PSYOP equipment capabilities require 21st Century technology. This modernization would permit the long-range dissemination of PSYOP messages via new information venues such as satellites, the Internet, personal digital assistants and cell phones:

  – (U) PSYOP ACTD. Commencing in FY04, SOCOM initiates an Advanced Concept Technology Demonstration (ACTD) to address dissemination of PSYOP products into denied areas. The ACTD should examine a range of technologies including a network of unmanned aerial vehicles and miniaturized, scatterable public address systems for satellite rebroadcast in denied areas. It should also consider various message delivery systems, to include satellite radio and television, cellular phones and other wireless devices and the Internet.

  – (FOUO) PSYOP recapitalization. PDM-1 provided funding across the FYDP to modernize the family of loudspeakers and acquire and improve leaflet delivery systems. This includes wind-supported air delivery systems and precision guided canister bombs. Loudspeakers will incorporate technologies that improve range, battery life and remote capability. These systems are integral PSYOP capabilities and improvement facilitates PSYOP mission accomplishment.

  – (FOUO) PSYOP Broadcast System (POBS). [redacted] the acquisition of the first of two required POBS sets to enhance PSYOP dissemination capability. [redacted]. This additional capability provides five receive and transmit and five receive-only systems that will enable better communication between PSYOP forces and allows for the distribution and dissemination of PSYOP products from Ft. Bragg, N.C. to additional locations.

5. Operations Security (U)

(U) ***DPG Tasking.***

- (U) ASD(C3I), in coordination with CJCS, will establish training objectives in OPSEC to include Red Teaming. Components will ensure they provide training in OPSEC and have sufficient Red Team capabilities (in both numbers and expertise) to assess continually the full spectrum of vulnerabilities and the effectiveness of both offensive and defensive measures designed to thwart adversary attack/exploitation attempts by technical, physical and human means.

(U) ***Current Situation.***

- (S) Mission critical information compromised. Numerous OPSEC violations across DoD have occurred within the last five years. The potential harm of these violations

represents a serious threat to our security and may provide potential adversaries with critical information to attack our vulnerabilities.

- (S) [redacted]
- (S) [redacted]. The Interagency OPSEC Support Staff (IOSS), located at Fort Meade, consists of 19 personnel and is the only dedicated element to support the USG. [redacted].
  - (S) No Red Teaming policy and doctrine. Along with the need for review and update of overall OPSEC policy, there is no policy on Red Teaming.

- (S) Inadequate training. Although there are several DoD institutions that offer instruction in OPSEC, training is not standardized and will not meet the IO career force or training and education goals recommended in the IO Roadmap.

(U) ***Desired Outcome.***

- (U) All plans are built, and operations executed, with priority attention to operations security.

(U) ***Recommendations (Numbers 52 - 55).***

(U) **Recommendation: Enhance OPSEC support (#52).**

- (U) The IO Roadmap recommended, and PDM-1 funded, the creation of an OPSEC Support Element at STRATCOM in FY04. In line with this recommendation, UCP02 also tasked STRATCOM to "….support other Combatant Commanders for the planning and integration of joint OPSEC…."

(U) **Recommendation: Revise OPSEC policy and doctrine (#53).**

- (U) All OPSEC doctrine across DoD should be revised. A task force led by OSD, STRATCOM and JCS with service, command and agency representatives has been formed to accomplish this task.
  - (U) OPSEC training objectives were developed and should be incorporated into OPSEC policy and doctrine revisions.

- (U) Each DoD component should revise their OPSEC policy and doctrine publications and reflect OSD/JCS guidance not later than one year from the publication of the new DoD Directive and the JCS Publication.

- (U) OSD and Joint Staff should work with the NSC and other departments and agencies to revise USG policy.

(U) **Recommendation: Institute vulnerability assessments (Blue/Red Teaming) (#54).**

- (U) Blue Team OPSEC assessments should be conducted to assist Combatant Commanders in evaluating their security profile and to prepare them for Red Team events.

- (U) Red Team OPSEC assessments should be conducted to determine the adequacy of the execution of OPSEC plans, programs, tactics, techniques and procedures. Red Team OPSEC assessments should identify OPSEC problems and serve as the basis for corrective actions.

(U) **Recommendation: Provide command emphasis (#55).**

- (U) OSD, STRATCOM and JCS should promote command emphasis by keeping OPSEC processes visible in preparing and disseminating periodic reminders from DoD leadership and implementation of training objectives.

  - (U) Emphasis should also come by ensuring a DoD Inspector General review of OPSEC is conducted throughout the Department in FY04.

- (U) STRATCOM should provide a robust OPSEC management oversight program for the Combatant Commanders.

6. Military Deception (U)

(U) ***DPG Tasking***.

- (U) No tasking exists; however, IO Roadmap participants unanimously agreed that military deception should be one of the five core capabilities of IO required to achieve the three broad IO functions. Therefore, the IO Roadmap also considered how to improve military deception as a critical component of integrated IO.

(U) ***Current Situation***.

- (U) The value of military deception, like OPSEC, is intuitive. Less immediately apparent is the reality that effective military deception requires centralized planning, security, and close integration with operational planning.

- (S/NF) Classification of [redacted] that full integration is difficult to achieve.

- (U) Service research and development centers focus largely on tools and capabilities that provide tactical advantage.

- (U) Military deception is taught in Service and joint schools, but instruction is Service specific and not presented as an integrated part of IO.

(U) ***Desired Outcome.***

- (U) All plans are built, and operations executed, with military deception considered a core capability in an integrated approach to information operations.

(U) ***Recommendations (Numbers 56 - 57).***

(U) **Recommendation: Establish advocacy for military deception to ensure its integration in IO (#56).**

- (FOUO) STRATCOM should be the advocate for military deception and ensure that it is integrated in all of its IO activities. As noted in the section on "Effective Command and Control and Supporting Organizations," UCP 02 Change 2 provides STRATCOM with the authority to execute this recommendation.

(S) Recommendation: Review management of military deception (#57).

- (U) STRATCOM, in concert with the CJCS and USD(P) (in light of USD(P) Title X responsibilities for oversight of plans), should conduct an assessment and make recommendations to the Secretary to:

  - (S) Clarify the role, authorities and boundaries for the execution of military deception.

  - (S) Determine how military deception could be better integrated into plans.

  - (S) Enhance traditional military deception methods by fully exploiting emerging technologies.

(U) NOTE: The full implementation of the recommendations in the IO Roadmap sections on Policies and Procedures, Career Force and Training and Education will further serve to advance military deception as a core IO capability.

Appendix A, Timeline (U)

IO Recommendation Milestones

	Oct 03 – FY 04	Oct 04 – FY 05	Oct 05 – FY 06 – Oct 06
Policies and Procedural Controls	• NSPD 16 USD(P) • CND Response Policy ASD(C3I) • DOD/DCI MOA USD(P) • CNA/PSYOP Delegation USD(P)/CJCS • PA/PD Lanes in Road USD(P) • DoD IO Directive ASD (C3I)		
Organizations	• IO CMD IOC STRATCOM •Reorganize OSD for IO SECDEF	• IO CMD FOC STRATCOM	
Analytical Support	• JWAC to STRATCOM STRATCOM • HFAC Expansion* DIA/STRATCOM [redacted]	• JIAPC IOC * STRATCOM [redacted]	• IW Planing Capability JIAPC/STRATCOM
Carcer Force	• Officer Billets Identified SERVICES/CJCS	• Enlisted & Civilian Program Developed SERVICES/CJCS	• Monitor Compliance USD(P&R)
Training and Education	• IO JPME Expanded CJCS	• Develop Joint IO Planners Course NDU • IO Graduate Center of Excellence Navy	• Accredit Service IO Instruction NDU
Computer Network Defense			
PSYOP		• ACTD 04 Denied Area Access SOCOM • Activate AC PSYOP Company* Army/SOCOM • Expand 11th PSYOP BN Structure* Army/SOCOM • PSYOP Recapitilization* SOCOM	• 4 x RC, 1 x AC PSYOP Companies Activated * Army/SOCOM
Computer Network Attack	• CNA Executive Agency STRATCOM • CNA C2 STRATCOM • CNA Weaponization IOTC/DOT&E	• CNA Test Range Study • DOT&E [redacted]	
OPSEC	• OPSEC Policy & Doctrine ASD(C3I) • Command Emphasis Letter ASD(C3I)	• OPSEC Support Element* STRATCOM	
Electronic Warfare	• Create ESG for EW AT&L • EW Investment Strategy USD(AT&L)		

* Indicates activity across FYDP

Appendix B, IO Roadmap Recommendations (U)

#	Description	#	Description
1.	Publish IO policy (p. 20)	30.	DoD should develop a full-time, well-trained professional cadre of certified system and security administrators (p. 47)
2.	Adopt a full spectrum concept of IO built upon three broad functions and five core capabilities (p. 20)	31.	Fully implement Public Key Infrastructure (p. 47)
3.	Approve a definition of IO based upon the full spectrum concept (p.22)	32.	Review STRATCOM's relationship to DoD CND forces (p. 47)
4.	Delegate selected execution authority to Combatant Commanders (p. 23)	33.	Incorporate CND recommendations in program reviews (p. 48)
5.	Improve visibility and accountability of IO resources (p. 24)	34.	Develop supplemental guidance for DoD's CND response actions (p. 48)
6.	Enhance and refocus PSYOP capability (p. 26)	35.	Develop national policy for offensive cyber operations (p. 50)
7.	Improve military support to public diplomacy (p. 27)	36.	Adopt a common understanding of the "CNA battlefield" (p. 52)
8.	Support active public affairs programs that influence foreign audiences (p. 27)	37.	Assign combatant command of CNA forces to STRATCOM (p. 53)
9.	Develop distinguishing tasks (p.27)	38.	[redacted]
10.	Empower STRATCOM to undertake critical precursor activities for successful IO planning and execution (p. 30)	39.	[redacted]
11.	Streamline CNA/PSYOP organizational constructs and C2 (p. 31)	40.	Delegate specific CNA targets to Combatant Commanders (p.65)
12.	Consolidate OSD Oversight of IO (p.31)	41.	Categorize and delegate selected CNA weapons (p. 57)
13.	Establish an IO career force (p. 33)	42.	Develop an integrated network of IO and CNA ranges (p. 57)
14.	Develop IO planners (p. 33)	43.	Establish assurance testing standards (p. 58)
15.	Develop IO capability specialists (p.34)	44.	Assign STRATCOM executive agency for joint CNA (p. 58)
16.	Identify joint and Service IO billets (p.34)	45.	Formally establish and charter an EW Executive Steering Group (p. 60)
17.	Provide focus for enlisted and civilians (p.34)	46.	Develop an EW roadmap (p. 61)
18.	Monitor career force compliance across DoD (p. 34)	47.	Coordinate DoD and USG themes and messages (p. 63)
19.	Integrate IO earlier in education (p. 35)	48.	Create a Joint PSYOP Support Element (p. 63)
20.	Expand/modify current IO training courses and/or develop new ones (p. 36)	49.	Delegate product approval for select categories of PSYOP products (p. 64)
21.	Establish a DoD Center of Excellence for IO (p. 36)	50.	Enhance the current PSYOP force structure (p. 64)
22.	Develop a program for intelligence support to full spectrum IO (p. 39)	51.	Modernize PSYOP force capabilities (p. 64)
23.	Provide dedicated support from a single analytic organization (p. 40)	52.	Enhance OPSEC support (p. 66)
24	Assign JWAC to STRATCOM (p. 40)	53.	Revise OPSEC policy and doctrine (p. 66)
25.	Enhance analytical capability over time with continual improvements in virtual collaboration (p. 41)	54.	Institute vulnerability assessments (Blue/Red Teaming) (p. 66)
26.	Adopt a joint integrated planning tool (p. 41)	55.	Provide command emphasis (p. 67)
27.	E-Space Analysis Center should be focal point for intel support to EW (p. 42)	56.	Establish advocacy for military deception (p. 68)
28.	E-Space Analysis Center should maintain authoritative EW data (p. 43)	57.	Review and assess management of military deception (p. 68)
29.	DoD should implement a Defense in Depth strategy (p. 45)		

Appendix C, Distinguishing Tasks (U)

	Public Affairs	DoD Support to Public Diplomacy	Psychological Operations
Strategic	- Brokering press availability for senior leaders (speeches, interviews, etc.) - Inoculations: Preemptive global communications to demonstrate past behavior or spotlight transgressions - Rapid Response/Truth Squads and "Briefings Plus" - Humanitarian road shows - Media embeds - Official press releases and maintenance of overseas DoD information web sites - Domestic opinion pieces and editorials by senior DoD officials	- Content of speeches or OP/ED pieces by senior DoD officials to foreign audiences - Content of pubs projected for trans-regional audiences - Talking points for private exchanges with foreign leaders - Guidance to Defense Attaches on themes and messages for foreign militaries - DoD support to other agency information activities; e.g. VOA	
Operational	- Town Hall meetings by Combatant Commanders - Position papers to military and civilian leaders in AOR - News releases - Press conferences - Joint Information Bureaus - Armed Forces Radio and Television	- Presentations and briefings concerning DoD policy, e.g., Defense attaché presentation to foreign military audiences - Overt dissemination of USG policy, e.g. Asia-Pacific Forum - Oversee Regional Centers	- Radio/TV/Print/Web media designed to directly modify behavior and distributed in theater supporting military endeavors in semi or non-permissive environment - When called upon, support to theater public diplomacy - DoD advisors to assist friendly forces in developing PSYOP programs - Foreign language products disseminated in support of local commanders in non- or semi-permissive areas - Tactical application of loudspeakers, print and media dissemination to a local adversarial public or combatants - When called upon, support to local public affairs activities
Tactical	- Town Hall meetings in a tactical commander's area of operations - Press conferences - News releases to local foreign media - Combat Camera products on events not accessible to news media		

Appendix D, Glossary (U)

ACTD	Advanced Concept Technology Demonstration
ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
ASD(NII)	Assistant Secretary of Defense (Networks and Information Integration)
ASD(PA)	Assistant Secretary of Defense for Public Affairs
C2	Command and Control
CJCS	Chairman Joint Chiefs of Staff
CMO	Civil-Military Operations
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations
COCOM	Combatant Command
CONPLAN	Contingency Plan
DASD	Deputy Assistant Secretary of Defense
DDIO	Deputy Director for Information Operations
DIA	Defense Intelligence Agency
DIRNSA	Director National Security Agency
DPG	Defense Planning Guidance
DoD	Department of Defense
DOT&E	Directorate of Operation Testing and Evaluation
EA	Electronic Attack
EP	Electronic Protect
EW	Electronic Warfare
FYDP	Future Years Defense Plan
HFAC	Human Factors Analysis Center
HUMINT	Human Intelligence
IADS	Integrated Air Defense Systems
IC	Intelligence Community
IO	Information Operations
IOSS	Interagency OPSEC Support Staff
IOTC	Information Operations Technology Center
ISR	Intelligence, Surveillance and Reconnaissance
JFHQ-IO	Joint Force Headquarters for Information Operations
JIAPC	Joint Integrative Analysis and Planning Center
JIOC	Joint Information Operations Center
JPOTF	Joint PSYOP Task Force
JWAC	Joint Warfare Analysis Center
MIST	Military Information Support Team
NSA	National Security Agency
NSC	National Security Council

OPCON	Operational Control
OPLAN	Operations Plan
OPSEC	Operations Security
OSD	Office of the Secretary of Defense
PA	Public Affairs
PD	Public Diplomacy
PDM	Program Decision Memorandum
PE	Program Element
PKI	Public Key Infrastructure
POBS	PSYOP Broadcast System
PSYOP	Psychological Operations
SAP	Special Access Program
SEAD	Suppression of Enemy Air Defense
SCADA	Supervisory Control and Data Acquisition
SCE	Service Cryptologic Element
SOCOM	Special Operations Command
SPACECOM	Space Command
SROE	Standing Rules of Engagement
STRATCOM	Strategic Command
UCAV	Unmanned Combat Aerial Vehicle
UCP	Unified Command Plan
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USG	United States Government
WMD	Weapons of Mass Destruction

PAGE INTENTIONALLY LEFT BLANK