Information Operations Roadmap

30 October 2003

~~SECRET~~//NOFORN

PAGE INTENTIONALLY LEFT BLANK

Table of Contents (U)

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) ██
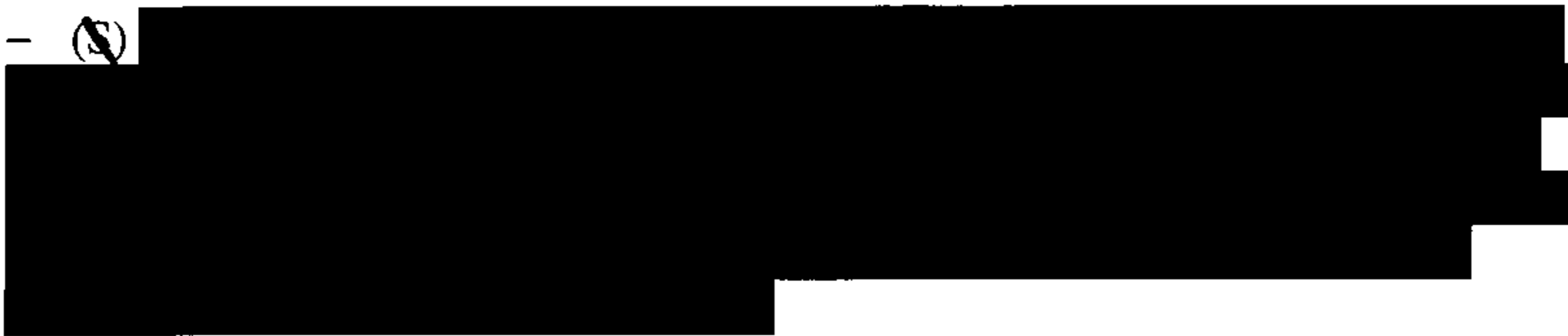
A. Approach (U)

- (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) <u>Method</u>. The principal work of the oversight panel was to guide the 15 separate supporting study efforts required by the DPG.[*] Each of the supporting study teams developed and briefed its terms of reference to the oversight panel. After terms of reference were agreed upon, each study team researched its topic, culling insights from multiple sources and antecedent studies. Study teams then provided an assessment of factors that currently constrain that IO area from contributing to IO as a core military competency. The study groups then drafted output statements sufficient to correct the limitations identified and developed prioritized recommendations that collectively would be sufficient to achieve the desired outcome.

  - (FOUO) Study leaders were appointed for the 15 supporting studies and specific milestones were assigned. Those studies assigned completion dates in September and October 2002 by the DPG were intended to influence the program and budget review, which they did. Approximately $383M was provided through the FY04-09 Program Decision Memorandum supporting interim IO Roadmap recommendations, which were vetted by the oversight panel leadership.

  - (U) The study leads presented in-progress reviews and final reports to the oversight panel. Between June and December 2002, the oversight panel met weekly to address issues raised by the studies. The DASD(R&P), DASD(S&IO) and DDIO also met on a weekly basis to review which study action recommendations should be included as major IO Roadmap conclusions.

  - (U) Senior leadership reached agreement on all but a handful of recommendations. In those cases where agreement was not possible, USD(P), as the DPG-directed lead for the Roadmap, resolved the difference of opinion or elevated options for decision by the Secretary of Defense.

B. Key Assumptions and Objective (U)

- (U) Key assumptions. Information, always important in warfare, is now critical to military success and will only become more so in the foreseeable future. Three key assumptions underscore the growing importance of information:

  - (U) Effectively communicating U.S. Government (USG) capabilities and intentions is an important means of combating the plans of our adversaries. The ability to rapidly disseminate persuasive information to diverse audiences in order

---

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

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

- (U) Networked C4ISR is a critical prerequisite for transforming our forces, providing for an increasingly transparent battle space, swift and effective decision-making, and rapid, parallel, effects-based operations.

- (U) Networked C4ISR is dependent upon automated decision-making and support, broadband networks, and electromagnetic capabilities, with a corresponding increase in associated vulnerabilities that should be planned for and managed.

- (U) Objective: IO becomes a core competency. The importance of dominating the information spectrum explains the objective of transforming IO into a core military competency on a par with air, ground, maritime and special operations. The charge to the IO Roadmap oversight panel was to develop as concrete a set of action recommendations as possible to make IO a core competency, which in turn required identifying the essential prerequisites to become a core military competency.

- (U) IO as a core competency requires a common understanding and appreciation within the Office of the Secretary of Defense, the Services and Combatant Commands on the value of IO. IO as a core military competency also requires:

  - (U) Policies and procedures that:

    - (U) Clearly define IO, provide a common understanding and clarify authorities and boundaries for execution.

    - (U) Delegate the maximum possible authority to Combatant Commanders to plan and execute integrated IO.

  - (U) Plans, operations and experimentation that:

    - (U) Incorporate IO in contingency planning within all joint force headquarters.

    - (U) Integrate IO into the broader development of new operational concepts.

    - (U) Include IO in all major training regimes and exercises.

  - (U) IO force development made possible by:

    - (U) Four-star Combatant Commander advocacy of IO for experimentation, concept development and definition of needed capabilities.

    - (U) Streamlined organizational and command and control relationships.

- (U) A trained and educated career force.

- (U) Joint program equivalents to develop dedicated IO capabilities.

- (U) The recommendations of this report address all the requirements to make IO a core military competency just identified.

3. Executive Summary (U)

A. Conclusions (U)

- (U) The IO Roadmap participants collectively identified three matters of key importance that require immediate attention:

- (C) We Must Fight the Net. DoD is building an information-centric force. Networks are increasingly the operational center of gravity, and the Department must be prepared to "fight the net." ███████████████████████ but be fully prepared to ensure critical warfighting network functionality and to ███████████████████████████

  - (C) However, networks are vulnerable now, and barring significant attention, will become increasingly more vulnerable. ██████████████████████ ██

  - (C) The recommendations of this report offer a good start point for remedial action for network security to maintain decision superiority. A robust, layered, defense in depth strategy is the next necessary step in providing Combatant Commanders with the tools necessary to preserve warfighting capability.

- (U) We Must Improve PSYOP. Military forces must be better prepared to use PSYOP in support of military operations and the themes and messages employed in a PSYOP campaign must be consistent with the broader national security objectives and national-level themes and messages. Currently, however, our PSYOP campaigns are often reactive and not well organized for maximum impact.

  - (U) PSYOP enhancements outlined in this report, and clarification of the respective responsibilities and tasks associated with PSYOP, DoD support to public diplomacy and public affairs, will enhance DoD's ability to aggressively conduct IO and to do so fully consistent with broader national security objectives.

  - (U) In particular, PSYOP must be refocused on adversary decision-making, planning well in advance for aggressive behavior modification during times of conflict. PSYOP products must be based on in-depth knowledge of the audience's decision-making processes and the factors influencing his decisions, produced rapidly at the highest quality standards, and powerfully disseminated directly to targeted audiences throughout the area of operations.

- (U) We Must Improve Network and Electro-Magnetic Attack Capability. To prevail in an information-centric fight, it is increasingly important that our forces dominate the electromagnetic spectrum with attack capabilities.

- (S) [REDACTED]

- (S) When implemented the recommendations of this report will effectively jump-start a rapid improvement of CNA capability. Moreover, the follow-on EW roadmap should define an overall investment strategy for the Department that will [REDACTED]

- (U) Collectively, the recommendations of this report begin the transformation of IO into a core military capability for Combatant Commanders. If aggressively implemented, these recommendations will produce the following benefits for the Department in general and the Combatant Commanders in particular:

  - (U) A common lexicon and approach to IO, including support to integrated information campaign planning.

  - (U) More execution authority delegated to Combatant Commanders.

  - (U) A trained and educated career force capable of IO planning and execution.

  - (U) Centralized IO planning, integration and analysis support from STRATCOM.

  - (U) Enhanced IO capabilities for the warfighter, including:

    - (U) Improved ability to disseminate powerful messages in support of adversary behavior modification.

    - (U) Protection of networks with a real defense in depth strategy.

    - (U) A robust offensive suite of capabilities to include full-range electronic and computer network attack, with increased reliability through improved command and control, assurance testing and refined tactics and procedures.

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

- (U) A uniform understanding and appreciation of IO should be based on a common DoD framework that includes a full spectrum concept of IO built upon three broad IO functions, five integrated core IO capabilities and a supporting definition as described below.

- (U) Three integrated IO functions. The Department's concept of IO should emphasize full spectrum IO that makes a potent contribution to effects based

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

- (U) Deter, discourage, dissuade and direct an adversary, thereby disrupting his unity of command and purpose while preserving our own.

- (U) Protect our plans and misdirect theirs, thereby allowing our forces to mass their effects to maximum advantage while the adversary expends his resources to little effect.

- (U) Control adversarial communications and networks and protect ours, thereby crippling the enemy's ability to direct an organized defense while preserving effective command and control of our forces.

  - (U) By extension, when executed to maximum effect, seizing control of adversary communications and networks will allow Combatant Commanders to control the enemy's network and communications-dependent weapons, infrastructure, command and control and battlespace management functions.

- (U) Peacetime preparation. The Department's IO concept should emphasize that full-spectrum information operations are full-time operations requiring extensive preparation in peacetime.

  - (U) Well before crises develop, the IO battlespace should be prepared through intelligence, surveillance and reconnaissance and extensive planning activities.

    - (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) ███████████████████████████████████████

      - (S) ███████████████████████████████████████

      - (S) ███████████████████████████████████████

      - (S) ██████████████████████████████ and information in support of a broader military deception plan.

      - (S) ██████████████████████████████████ by undermining the adversary's confidence in his capabilities (e.g. ██████ ██████████████████

    - (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 ████████████████████████████ to rapidly employ IO capabilities. The Standing Rules of Engagement should be modified ████ and PSYOP. In particular:

(S) The CJCS in coordination with STRATCOM should propose to SecDef modifications to the Standing Rules of Engagement for ███████████████ ██████████████, *so that* █████████████████████████ ███████████ *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.

(█) 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 ████████████████████████████████ 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.*

> - *(█) STRATCOM, in coordination with USD(I), should develop memorandums of agreements with the* ███████████████████████████ ██████████████████ *and the Director Defense Intelligence Agency on the Human Factors Analysis Center.*

> - *(█) USD(I), in coordination with the USD(AT&L), will develop direction for the* ████████████████████████████ *to provide* ██████████ ████████████████████████████ *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) ███. The UCP assigned STRATCOM authority for CNA. ████████████
██

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

(S) ██
██
██

(S) ██
██
██

(S) ██
██

(S) ██
██
██

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 ███████████████████████████
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.

(█) 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 ████████████████████████████
████████████████████████████
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.* ██████████████████

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) ███████████████████████████ 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 ███████ ███████████████████ 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) ██████████████████████████████████████ ████████████████████ 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 ████████████████████████ 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 ████ and examined the role of the ████████ ████████████████████

    - (S) The exercise highlighted the need to revise the ████████████████ ████████████████ 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 ████████████ to temporarily ████████████████████████████████ 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) ██.

    - ▪ (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) ██

  - (S) ██

  - (S) ██

  - (S) ██

  - (S) ██

- (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 ███████ PSYOP.

  - (S) CNA Delegation. ███████████████████████████ ████████████████████████ 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 ███████████████ ███████████ 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.