SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

SECRETARY'S FOREWORD

(U) The Department of Defense (DoD) relies on cyberspace to achieve national military objectives in the areas of military, intelligence, and business operations. This reliance provides adversaries a ready avenue of approach to exploit cyberspace to gain strategic, operational, and tactical advantages over the United States. The cyberspace domain is complex and evolves at astonishing rates, increasing the challenge of ensuring strategic advantage in this domain. The National Military Strategy for Cyberspace Operations is an important first step toward ensuring our own freedom of action in this contested domain while denying the same to our adversaries.

(U) Our strategy must remain flexible as our understanding of cyberspace grows and our capacity to conduct cyberspace operations increases. Therefore, the implementation of the strategy will be based on an iterative approach in partnership with other US Government departments and agencies, partner nations, and industry. Supported by fresh thinking attuned to the speed and dynamics at which cyberspace operations occur, the strategy will remain continuously relevant. I direct DoD components to participate in this important process.

DEC 11 2005

CHAIRMAN OF THE JOINT CHIEFS OF STAFF
WASHINGTON, D.C. 20318-9999

MEMORANDUM FOR: Distribution List

Subject: National Military Strategy for Cyberspace Operations (NMS-CO)

1. Operations in cyberspace are a critical aspect of our military operations around the globe. The enclosed NMS-CO is the product of significant reflection and debate within our military and government. It describes the cyberspace domain, articulates threats and vulnerabilities in cyberspace, and provides a strategic framework for action. The NMS-CO is the US Armed Forces' comprehensive strategic approach for using cyberspace operations to assure US military strategic superiority in the domain. The integration of offensive and defensive cyberspace operations, coupled with the skill and knowledge of our people, is fundamental to this approach.

2. Implementation of this strategy will help ensure that our Armed Forces have the capacity to conduct cyberspace operations in support of US national interests in the years ahead.

3. Without enclosure, this memorandum is UNCLASSIFIED.

PETER PACE
General, United States Marine Corps
Chairman
of the Joint Chiefs of Staff

Enclosure

THE NATIONAL MILITARY STRATEGY FOR CYBERSPACE OPERATIONS (U)

December 2006

Chairman of the Joint Chiefs of Staff
Washington, D.C. 20318

Classified By:	VADM N. E. Brown, USN; DJ-6
Reason:	1.4(a)(c)(g)
Declassify On:	19 September 2030

(INTENTIONALLY BLANK)

DEPARTMENT OF DEFENSE
WASHINGTON, D.C. 20318
NOVEMBER 2006

NATIONAL MILITARY STRATEGY FOR CYBERSPACE OPERATIONS

TABLE OF CONTENTS

(INTENTIONALLY BLANK)

SECRETARY'S FOREWORD

(U) The Department of Defense (DoD) relies on cyberspace to achieve national military objectives in the areas of military, intelligence, and business operations. This reliance provides adversaries a ready avenue of approach to exploit cyberspace to gain strategic, operational, and tactical advantages over the United States. The cyberspace domain is complex and evolves at astonishing rates, increasing the challenge of ensuring strategic advantage in this domain. The National Military Strategy for Cyberspace Operations is an important first step toward ensuring our own freedom of action in this contested domain while denying the same to our adversaries.

(U) Our strategy must remain flexible as our understanding of cyberspace grows and our capacity to conduct cyberspace operations increases. Therefore, the implementation of the strategy will be based on an iterative approach in partnership with other US Government departments and agencies, partner nations, and industry. Supported by fresh thinking attuned to the speed and dynamics at which cyberspace operations occur, the strategy will remain continuously relevant. I direct DoD components to participate in this important process.

(INTENTIONALLY BLANK)

MEMORANDUM FOR: Distribution List

Subject: National Military Strategy for Cyberspace Operations (NMS-CO)

1. Operations in cyberspace are a critical aspect of our military operations around the globe. The enclosed NMS-CO is the product of significant reflection and debate within our military and government. It describes the cyberspace domain, articulates threats and vulnerabilities in cyberspace, and provides a strategic framework for action. The NMS-CO is the US Armed Forces' comprehensive strategic approach for using cyberspace operations to assure US military strategic superiority in the domain. The integration of offensive and defensive cyberspace operations, coupled with the skill and knowledge of our people, is fundamental to this approach.

2. Implementation of this strategy will help ensure that our Armed Forces have the capacity to conduct cyberspace operations in support of US national interests in the years-ahead.

3. Without enclosure, this memorandum is UNCLASSIFIED.

PETER PACE
General, United States Marine Corps
Chairman
of the Joint Chiefs of Staff

Enclosure

(INTENTIONALLY BLANK)

EXECUTIVE SUMMARY

(U) ***Purpose.*** The National Military Strategy for Cyberspace Operations (NMS-CO) is the comprehensive strategy of the US Armed Forces to ensure US military superiority in cyberspace. The NMS-CO establishes a common understanding of cyberspace and sets forth a military strategic framework that orients and focuses DOD action in the areas of military, intelligence, and business operations in and through cyberspace. Combatant commands, Military Departments, agencies, field activities, and other DOD organizational entities (hereafter referred to collectively as DOD components) should use the NMS-CO as a definitive reference to plan, execute, and resource cyberspace operations.

(U) ***The Cyberspace Domain.*** Recognizing that the understanding of cyberspace has evolved, for the purpose of this strategy, cyberspace is defined as:

> (U) *"A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."*

(b)(1)

(U) ***Military Strategic Framework.*** The military strategic framework focuses operations toward a strategic goal in terms of ends, ways, and means.

(U) ***Military Strategic Goal.*** The military strategic goal is to ensure US military strategic superiority in cyberspace.

(b)(5)

(b)(1)

(b)(5)

(U) ***Ways.*** The ends are achieved by DOD through the integrated execution of five "fundamental" ways and six "enabling" ways. The fundamental ways are: *Information Operations, Network Operations, Kinetic Actions, Law Enforcement and Counterintelligence,* and *Themes and Messages.* Six enabling ways cut across all mission areas and facilitate execution of cyberspace operations: *Science and Technology, Partnering, Intelligence Data and Support to Operations, Situational Awareness, Law and Policy,* and *People.*

(U) ***Means***. DOD relies on the unified employment of organizations, personnel, capabilities, and resources to fulfil the strategic goal.

(U) ***Implementation***. The Joint Staff will develop an implementation plan and lead an annual assessment process. Development of specific capabilities for cyberspace operations occurs within the context of the current Joint Capabilities Integration and Development System. This strategy identifies eight joint capability areas for special attention: *Joint Battlespace Awareness*; *Joint Force Generation*; *Joint Command and Control*; *Joint Information Operations*; *Joint Net-Centric Operations*; *Joint Global Deterrence*; *Joint Homeland Defense*; and *Joint Interagency Integration, Intergovernmental Organization Coordination, and Nongovernmental Organization Coordination*. In addition, Chapter Six of this strategy directs four strategic priorities that provide focus for a wide range of outcomes:

- (U) Gain and maintain initiative to operate within adversary decision cycles.
- (U) Integrate cyberspace capabilities across the range of military operations.
- (U) Build capacity for cyberspace operations.
- (U) Manage risk for operations in cyberspace.

CHAPTER ONE

PURPOSE (U)

(U) The Impact of Cyberspace. The United States operates in a global environment characterized by interdependence, uncertainty, complexity, and continual change. In this environment, the prosperity and security of our Nation rely on cyberspace to achieve strategic advantage and strengthen the instruments of national power. Cyberspace reaches across geopolitical boundaries and is tightly integrated into the operation of critical infrastructures and the conduct of commerce, governance, and national security. The United States must have cyberspace superiority to ensure our freedom of action and deny the same to our adversaries through the integration of network defense, exploitation, and attack. Therefore, the Department of Defense (DOD) must be prepared to provide military options to the President and Secretary of Defense.

(U) Purpose. The National Military Strategy for Cyberspace Operations (NMS-CO) is the comprehensive military strategy for the US Armed Forces to ensure US superiority in cyberspace. It serves to begin integrating cyberspace operations with DOD's national defense role in the areas of military, intelligence, and business operations. Five elements comprise this strategy:

- (U) *Strategic Context* provides the working definition and cyberspace characteristics.
- (U) *Threats and Vulnerabilities* creates a common understanding of the context, threats, vulnerabilities, and opportunities for cyberspace operations.
- (U) *Strategic Considerations* provide additional clarity to identify priorities.
- (U) *Military Strategic Framework* presents ends, ways, and means.
- (U) *Implementation and Assessment* identifies areas where change is needed and establishes a mechanism to measure progress toward achieving the strategic goal.

(U) Authorities. Authority for actions undertaken by the US Armed Forces is derived from the US Constitution and Federal law. These authorities establish roles and responsibilities that provide focus for organizations to develop capabilities and expertise, including those for cyberspace. Key authorities that apply to DOD include Title 10, *Armed Forces*; Title 50, *War and National Defense*; and Title 32, *National Guard* (see Enclosure A).

(U) National Guidance. *DOD Strategic Planning Guidance* (March 2006) directs the development of the National Military Strategic Plan for Securing Cyberspace. Early in the process of writing this document, the Chairman recognized an urgent need for an overarching strategy that encompassed all aspects of cyberspace. Accordingly, he directed expansion to include all cyberspace operations in the strategy.

(U) DOD Roles in Cyberspace. The NMS-CO builds on the national and DOD guidance listed in Enclosure B. US law and national policy assign DOD three main roles: defense of the Nation, national incident response, and critical infrastructure protection. These missions may be performed simultaneously. Although partner departments and agencies have responsibilities to secure portions of cyberspace, only DOD conducts military operations to defend cyberspace, the critical infrastructure, the homeland, or other vital US interests. If defense of a vital interest is implicated, DOD's national defense mission takes primacy even if that would conflict with, or subsume, the other support missions.

(U) *Defense of the Nation.* DOD will execute the full range of military operations (ROMO) in and through cyberspace to defeat, dissuade, and deter threats against US interests. Also, under the authorities of the Secretary of Defense, DOD will use network exploitation to gather intelligence and shape the cyberspace environment as necessary to provide integrated offensive and defensive options. DOD will leverage the authorities and capabilities of those agencies under the Director of National Intelligence, as appropriate. DOD may conduct cyberspace operations across national boundaries and will, in some cases, require global actions to be coordinated across geopolitical and theater boundaries. DOD will partner with the Intelligence Community (IC), Department of Justice (DoJ), Department of Homeland Security (DHS), and other Federal departments and agencies to further DOD cyberspace operations. As directed, DOD will deploy necessary resources to support efforts of other Federal agencies.

(U) *National Incident Response.* In addition to DOD's responsibility to defend the Nation, DOD will provide military support to civil authorities, as directed. DOD will coordinate with DHS and other Federal departments and agencies, as described in the *National Response Plan* (2004).

(U) *Critical Infrastructure Protection.* Concurrent with its national defense and incident response missions, DOD will support DHS and other Federal departments and agencies to ensure all sectors of cyberspace critical infrastructure are available to support the ROMO. Critical infrastructure protection relies on analysis, warning, information sharing, vulnerability identification and reduction, mitigation, and aiding of national recovery efforts. DOD, in accordance with the draft National Infrastructure Protection Plan (January 2006), has been designated as the Sector Specific Agency for the Defense Industrial Base (DIB) sector. The Defense Information Systems Agency, as the lead agent for the Defense Critical Infrastructure Program Global Information Grid (GIG) sector, is responsible for matters pertaining to the identification, prioritization, and remediation of critical GIG infrastructure. DOD is responsible for coordination of efforts to protect the DIB sector and the GIG sector of the DIB.

CHAPTER TWO

STRATEGIC CONTEXT (U)

> (U) "The Armed Forces must have the ability to operate across the air, land, maritime, space and cyberspace domains of the battlespace."
>
> *National Military Strategy* (2004), p. 18

(U) The Cyberspace Domain. Throughout the history of warfare, opponents have sought technology to gain an advantage. Those responsible for the Nation's defense must appreciate the military's dependence upon cyberspace for cyberspace-specific operations and use it to ensure success in the other domains. The reality of increasing net-centric operations requires DOD to employ our cyberspace resources consistently to achieve and maintain US military strategic advantage.

(U) Definition of Cyberspace. Joint Publication (JP) 3-0, *Joint Operations*, discusses the operational environment as consisting of the air, land, maritime, and space domains and the information environment. However, treating cyberspace as a domain establishes a foundation to understand and define its place in military operations. JP 1-02 currently defines cyberspace as, "The notional environment in which digitized information is communicated over computer networks." Recognizing that the understanding of cyberspace has evolved, for the purposes of this strategy, a working definition of cyberspace is:

(U) "A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures"

(U) Cyberspace Characteristics:

- (U) Created, maintained, owned, and operated by public, private, and government stakeholders and exists across the globe.
- (U) Changes as technology, architectures, processes, and expertise co-evolve to produce new capabilities and operating constructs.
- (U) Subject to the availability of the electromagnetic spectrum.
- (U) Allows high rates of operational maneuver that capitalizes on decision-quality information moving at speeds that approach the speed of light.
- (U) Enables operations across the domains of air, land, maritime, and space.
- (U) Transcends commonly defined organizational and geopolitical borders.
- (U) Formed by the interconnection of information and data transmission systems; supporting critical infrastructure; devices that store, process, and transmit data; and the use of software and hardware applications.
- (U) Includes data, voice, and video "at rest" and "in motion."
- (U) Readily accessible in varying degrees to other nations, organizations, partners, the private sector, and our adversaries.
- (U) Forms the foundation of the information environment.

(U) Key Features of the Domain

(U) *Man-Made Domain.* Sustaining and evolving cyberspace is an ongoing effort requiring continuous operations, significant resources, and a more comprehensive response to extraordinary incidents. For example, the Indian Ocean tsunami in December 2004 resulted in the destruction of the ground-based communications infrastructure causing the interruption of communications and severely impacting cyberspace in the affected regions.

(U) *Technical Innovation.* Cyberspace evolves in response to ongoing technical innovation and is the only domain whose underlying structure can be dynamically reconfigured. In addition, operating requirements for the equipment used in the domain are founded on similar standards, thereby facilitating effects applicability across the range of cyberspace operations. Keeping pace with technological change requires sustained and constant vigilance and high degrees of domain expertise.

(U) *Volatility.* Cyberspace constantly changes, making some targets transitory and offensive and defensive operations challenging. A previously vulnerable target may be replaced or provided with new defenses with no warning, rendering cyberspace operations less effective. Also, an unapproved or uncoordinated change in a US or allied network configuration could introduce unintended vulnerabilities to friendly systems.

(U) *Information Movement.* The lack of geopolitical boundaries and natural boundaries of the electromagnetic spectrum allows cyberspace operations to occur rapidly nearly anywhere.

(U) *Speed.* The speed at which information moves in cyberspace approaches the speed of light. In war, operational speed is a source of combat power. When this speed is exploited, increased efficiency and productivity can result. Cyberspace affords commanders opportunities to make decisions rapidly, conduct operations, and deliver effects at speeds that were previously incomprehensible. In addition, increasing the speed of the policy and decisionmaking process potentially will yield greater effectiveness of cyberspace capabilities. However, speed also can degrade cyberspace operations. In some cases a rapid tempo of operations can trigger unintended detection and evasive actions that would not otherwise have occurred.

(b)(1)

(b)(1)

(U) Cyberspace and the Information Environment. The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.[2] The information environment is made up of three interrelated dimensions: physical, informational, and cognitive. Cyberspace is best understood as relating to the physical and information dimensions of the information environment. The physical dimension of the information environment includes information systems and networks, computers and communications systems, and supporting infrastructures. Similarly, the information dimension of the information environment includes information that is processed, stored, disseminated, displayed, and protected; all of which are important functions that take place within cyberspace. Cyberspace also provides a link into the cognitive dimension.

(U) Envisioning Cyberspace Missions. Framing traditional missions in terms of how they might apply to cyberspace facilitates a deeper understanding of this domain and its impact on warfighting. This includes setting conditions in cyberspace to ensure the availability of the domain; the ability to engage adversaries decisively to establish cyberspace control and superiority; and the ability to conduct cyberspace operations to achieve desired effects in military, intelligence, and business operations or in support of operations in the air, land, maritime, and space domains.

Emerging Concepts

(U) Carrying joint warfare forward into the cyberspace domain, emerging concepts, such as "cyberspace warfare," may be developed to conduct operations in support of US national security objectives. These concepts should be vetted through formal concept development processes to further our understanding of and capacity to conduct cyberspace operations.

(b)(5)

[2] (U) JP 3-13, *Information Operations* (February 2006).

(INTENTIONALLY BLANK)

CHAPTER THREE

THREATS AND VULNERABILITIES (U)

(b)(1)

(U) Vulnerabilities. Actions taken to implement this strategy must identify and address, as deemed appropriate by risk management processes, the full range of vulnerabilities discussed in Enclosure D. In contrast to the physical domains, in cyberspace a risk accepted by one is a risk assumed by all.

(INTENTIONALLY BLANK)

CHAPTER FOUR

STRATEGIC CONSIDERATIONS (U)

(U) Cyberspace is a domain with its own set of risks and imperatives. The following considerations provide additional clarity for identification of implementation priorities.

(U) Risk Considerations. Through the process of risk management, leaders must consider risks to US interests from adversaries using cyberspace to their advantage and from our own efforts to employ the global nature of cyberspace to achieve objectives in military, intelligence, and business operations. The outcome of these efforts helps set the conditions to gain and maintain freedom of action to conduct cyberspace operations. For operational plans development, the combination of threats, vulnerabilities, and impacts must be evaluated in order to identify important trends and decide where effort should be applied to eliminate or reduce threat capabilities; eliminate or reduce vulnerabilities; and assess, coordinate, and deconflict all cyberspace operations.

(U) *US Military dependence on cyberspace will continue to increase.* DOD force transformation hinges largely on a move toward net-centric operations. Significant investments in force structure, infrastructure, and programs have oriented DOD components toward the use of cyberspace as an integral part of warfighting. Threat actors can take advantage of this dependence and adversely affect cyberspace operations. Risk to operational effectiveness increases if inadequate resources prevent the fielding of required capabilities needed to conduct cyberspace operations.

(b)(1)

(U) *Designated lead agencies will unevenly fulfill their responsibilities to secure cyberspace.* The responsibility for securing cyberspace, at a national level, resides with DHS. However, DOD must ensure secure operation of its own portion of cyberspace and depend on other Federal departments and agencies to secure their portions of cyberspace.

(U) *Lack of adequately and consistently trained and equipped personnel increases cyberspace vulnerability.* DOD must establish common training standards across DOD and collaborate with DHS to share those standards and help ensure all USG personnel who operate in cyberspace possess appropriate training.

(U) *Absent significant effort, the United States will not continue to possess an advantage in cyberspace.* Although the United States currently enjoys technological advantages in cyberspace, these advantages are eroding.[3] The United States will not continue to enjoy an advantage in *how* this technology is developed and employed. The United States increasingly depends on technology designed and manufactured by

[3] (U) Gartner Report, March 2006

entities that reside outside the United States who may become adversaries. Unlike the other warfighting domains, the United States risks parity with adversaries.

(b)(1)

(U) Strategic Imperatives. Strategic imperatives are those considerations that must be taken into account to operate successfully in the domain.

(U) *Offensive/defensive operations.* Offensive capabilities in cyberspace offer the United States and our adversaries an opportunity to gain and maintain the initiative. DOD cyberspace operations are strongest when offensive and defensive capabilities are mutually supporting. This requires a long-range focus and dedicated resources to achieve this goal.

(U) *Integration.* Operations to achieve desired effects in and through cyberspace require integration of organizations, capabilities, functions, technologies, and missions. The requirements to comply with law and policy, cooperate with partners, and deconflict operations further drive the need to integrate. Coordinating planning efforts early will reduce seams and gaps in organizational boundaries, limit shortfalls in resources needed to support mission accomplishment, and increase the overall success of cyberspace operations. Also, integration of procedures to ensure lawful targeting must be a cornerstone of planning for cyberspace operations. Finally, integration across time, space, and purpose in cyberspace facilitates the rapid coordination and unified action needed to generate strategic advantage.

(U) *Sharing information.* DOD must be able to use cyberspace to share information in support of operations. The speed at which multiple partners and mission areas must integrate and interoperate in cyberspace means that information sharing must occur rapidly, securely, and systematically. Policies and technical architectures must contribute to effective and secure information sharing with USG partners, allies, and commercial providers in support of military operations as well as DOD business operations.

(U) *Ability to operate through degradation.* Elements of this imperative include domain resilience, redundancy, restorative capacity, consequence management, continuity of operations (COOP) procedures, training, and exercising. In addition, leaders must have confidence in the credibility of the information they receive through cyberspace if they are to act upon that information. Of particular importance in this regard are consequence management and COOP. Consequence management includes actions taken to manage and mitigate problems resulting from environmental disasters and catastrophic events. COOP is the capability of DOD to continue mission-essential functions without unacceptable interruption to maintain military effectiveness, readiness, and survivability. It also includes the ability to assess and decide which is a greater risk or consequence: the continued support of an exploited or affected system or the need for that system to support on-going or planned military operations.

(U) *Command Relationships.* The responsiveness, simplicity, agility, and flexibility of command relationships influence successful application of military power in cyberspace. Coordination of courses of action among combatant commanders is an on-going, collaborative process that begins with plan development and extends through operational execution in the context of continuous cyberspace operations. The United States can achieve superiority in cyberspace only if supported and supporting relationships are clearly defined and executed. These relationships must support unity of effort in achieving combatant commander missions as well as maintaining freedom of action in cyberspace. Senior leaders must establish a structure that integrates all mission areas and dismantles stove-piped organizations that hinder collaboration and lengthen decisionmaking cycles.

(U) *Command and Control (C2).* Cyberspace provides the foundation for C2 of military operations in other domains. C2 in cyberspace operations is achieving unified action vertically and horizontally, among all levels of war, and throughout organizations. Due to the nature of cyberspace, C2 requires extremely short decision-making cycles. Effective C2 integrates, deconflicts, and synchronizes cyberspace operations at the speeds required for achieving awareness and generating effects.

(b)(1)

(U) *Configuration Management.* DOD organizations must have positive control of systems supporting cyberspace. Global force sourcing and interoperability requirements mandate the establishment and enforcement of standardized approaches to providing connectivity to cyberspace. Configuration management enables consistent application of tools, processes, and procedures across cyberspace and is critical for a mature and defensible cyberspace.

(U) *Enforcement.* DOD organizations with insufficient leadership emphasis on developing and enforcing cyberspace policies and regulations are targets for adversaries and place our networks at risk. Leaders at all levels are accountable for ensuring readiness and security to the same degree as in any other domain. Leaders must hold individuals and organizations accountable for violations of laws and policies. In addition, the rapid evolution of cyberspace technology highlights the need to continually adapt policy based on new threats, vulnerabilities, and opportunities while evolving mitigation approaches.

(U) *Understand Cyberspace.* Leaders must understand cyberspace as it relates to DOD's ability to operate in military, intelligence, and business operations. DOD personnel operating in cyberspace must have a thorough understanding of the rapidly evolving procedural and technical mechanisms required to conduct cyberspace operations. This knowledge must be coupled with an understanding of the applications used to conduct military, intelligence, and business processes to optimize effectiveness and mitigate risks.

(U) *Current and Future Military Campaigns and Operations.* The *National Security Strategy* states that the US military's highest priority is to "defend the United States." This strategy must complement all other critical defense undertakings. Cyberspace operations must take into account these national efforts and their requirements for DOD resources.

CHAPTER FIVE

MILITARY STRATEGIC FRAMEWORK (U)

(U) The military strategic framework orients and focuses DOD action in the areas of military, intelligence, and business operations in and through cyberspace. The military strategic goal is to *ensure US military strategic superiority in cyberspace.* The strategic framework focuses on offensive and defensive operations to achieve this goal. This approach is expressed in terms of ends, ways, and means.

(U) Ends. Five specific ends provide further refinement of the strategic goal and are consistent with the existing national cyberspace guidance and the 2005 *Contingency Planning Guidance (CPG)* termination objectives. These ends represent the steady state DOD must establish as the comprehensive military contribution to cyberspace operations.

(U) *Adversaries are deterred from establishing or employing offensive capabilities against US interests in cyberspace.* DOD will deter malicious adversary use of cyberspace, while promoting freedom of action and trust and confidence in US cyberspace operations. Through deterrence, DOD seeks to influence the adversary's decisionmaking processes by imposing political, economic, or military costs; denying the benefits of their actions; and inducing adversary restraint based on demonstrated US capabilities. DOD will act in collaboration with the intelligence community, law enforcement, counterintelligence, and other USG partners and allies.

(b)(1)

(U) *DOD is postured to support homeland security, critical infrastructure protection, and civil support.* DOD could be called upon to lend expertise or assistance in the event of catastrophic incidents affecting US use of cyberspace. DOD must be prepared with appropriate contingency plans and resources to provide coordinated support as directed.

(U) Ways. DOD achieves the strategic goal and complements other USG activities using a variety of ways that require development of particular capabilities.

(U) Fundamental Ways. Five fundamental ways represent proficiencies military forces must develop and execute to accomplish the ends. Although many ways may contribute to achieving the ends, *Network Operations, Information Operations, Kinetic Actions, Law Enforcement and Counterintelligence,* and *Themes and Messages* are fundamental to cyberspace operations. There may be other ways, not explicitly listed here, that contribute to achieving the ends. DOD components should initiate collaboration at the earliest possible stage of the planning process to share relevant knowledge about tools, accesses, techniques, and information. Early collaboration will facilitate deconfliction,[4] integration, and synchronization of military and intelligence operations.

(U) *Network Operations.* Network operations provide integrated network visibility and end-to-end management of networks, global applications, and services across the GIG. Network visibility enables commanders to manage their networks as they would other combat systems.[5] Network operations provide for assured system and network availability, information protection, and information delivery to support military, intelligence, and business functions. DOD must employ an information-centric, layered defense-in-depth approach to operate and defend the GIG using technical and non-technical practices. These practices will further support continuous monitoring, detection, reporting, prevention, and response to ensure authorized and legitimate access to information while preventing unauthorized or illegitimate access and disclosure of information. Network operations must also be integrated with other information operations activities.

(b)(1)

[5] (U) JP 6-0, "Joint Communication System" (20 March 2006).

(b)(1)

(U) *Kinetic Actions.* DOD will conduct kinetic missions to preserve freedom of action and strategic advantage in cyberspace. Kinetic actions can be either offensive or defensive and used in conjunction with other mission areas to achieve optimal military effects.

(U) *Law Enforcement and Counterintelligence.* Rapid coordination among DOD criminal investigative and counterintelligence organizations with international, federal, state, and local law enforcement and other counterintelligence agencies is a force multiplier. Effective law enforcement investigations and the threat of prosecution can deter potential aggressors. However, arrest and prosecution will remain selective and infrequent due to difficulty in ascertaining the identity and status of attackers coupled with complex jurisdictional issues. Counterintelligence goals include: identifying adversary intent, targets, and capabilities; exploiting adversary cyber operations; and providing threat warning.

(U) *Themes and Messages.* DOD can use cyberspace rapidly and more effectively to reach target audiences in support of USG interests and policies. Increasingly, the Internet and wireless networks provide DOD the means to reach foreign audiences as part of support to a comprehensive interagency effort. These activities should be coordinated and integrated with USG objectives through appropriate DOD mechanisms.

(U) Enabling Ways. Enablers enhance the effectiveness and integration of military capabilities and their subsequent effects.

(b)(1)

Operationalizing Intelligence

(U) Cyberspace provides new opportunities for accessibility, maneuverability, and functionality for the intelligence enterprise – not only as an enabler of military operations, but as an operation intrinsically comparable to traditional military operations. Intelligence operations in and through the electromagnetic spectrum can provide DOD the asymmetric edge necessary for military operations and to overcome DOD challenges.

(U) *Science and Technology (S&T).* DOD must continually invest in S&T and leverage emerging, innovative, and disruptive cyberspace technologies, particularly those arising in the commercial arena. Continual advances in operations resulting from pursuit of S&T initiatives are a prerequisite for superiority in cyberspace. DOD must capitalize on S&T to ensure no US peer competitor emerges to challenge US interests in cyberspace.

(U) *Partnering.* In addition to standard military relationships, leaders must recognize that interagency and coalition relationships are critical to successful cyberspace operations. DOD's ability to conduct cyberspace operations freely is fundamentally linked to infrastructures, not all of which are under our control. Therefore, DOD must assist in decreasing vulnerabilities to those infrastructures whenever possible through successful partnerships. Clearly defined partnerships help distinguish between foreign and domestic threats and help resolve procedural and legal issues. These relationships include defense contractors, federally funded research and development centers, academia, commercial infrastructure providers, and other global and regional allies and partners who share similar dependence on cyberspace. To the extent possible, DOD will work with these partners to mitigate vulnerabilities and increase the resilience of the critical infrastructures.

- (U) *Industry.* The continuing evolution of global outsourcing and offshore development of IT increases DOD reliance on industry partnerships. For example, the Information Sharing and Analysis Centers[6] are public and private alliances that facilitate information sharing between the public and private sectors. This permits collaborative actions to create an environment that fosters greater security in cyberspace and enables freedom of action for other mission areas. DOD must be prepared to support and collaborate with these public-private alliances and other government initiatives designed to secure and defend the US against cyberspace threats. DOD has limited influence on the strategic direction of global markets, but can leverage relationships to increase strategic advantage and decrease risk. DOD, in partnership with industry, must ensure adequate measures are in place for the software assurance and security of cyberspace.

- (U) Interagency. The interagency process must provide for integrated planning and operations. The process must also clearly define lines of

[6] Recommended in the "National Strategy for the Physical Protection of Critical Infrastructure and Key Assets."

responsibility among DOD, DHS, DoS, DoJ, IC, and other governmental agencies. Interagency and coalition relationships must be built and maintained so that they may dynamically respond and evolve as the situation dictates. Integrating early planning efforts will reduce seams and close gaps in interagency efforts, limit shortfalls in resources needed to support mission accomplishment, and increase the overall success in conducting operations. For example, the National Cyber Response Coordination Group (NCRCG) is a forum of USG agencies including representatives from the Homeland Security Council and National Security Council. The NCRCG coordinates intra-governmental and public/private preparedness operations to respond to and recover from national cyber incidents.

- (U) International Coalition. The United States must build and maintain coalitions that are adaptable and capable of evolving throughout an operation. Integrating coalition partners early into the planning process reduces operational seams across the coalition and increases the overall success of operations.

(U) *Situational Awareness.* Cyberspace situational awareness enables commanders and planners to assess the current situation, collaborate on courses of action, take action, and anticipate opportunities and challenges in the domain. Automated tools must be employed to provide near-real time notification of anomalous activity and properly inject appropriate data into operational views to characterize the cyberspace activity. This situational awareness combined with proper risk assessments, including intelligence loss or gain determinations, will allow commanders to make the best decisions on courses of action.

(U) *Law & Policy.* Policy influences organizational relationships and partnerships that must be established in order to operate successfully in the domain. DOD must conduct cyberspace operations within applicable US and international law and relevant USG and DOD policies. The legal framework applicable to cyberspace operations depends on the nature of the activities to be conducted, such as offensive or defensive military operations; defense support to civil authorities (security); service provider actions; law enforcement and counterintelligence activities; intelligence operations; and defense of the homeland. Before conducting cyberspace operations, commanders, planners, and operators must understand the relevant legal framework in order to comply with laws and policies, the application of which may be challenging given the ubiquitous nature of cyberspace and the often geographic orientation of domestic and international law. It is essential that commanders, planners, and operators consult with legal counsel during the planning and execution of cyberspace operations. DOD must ensure policy is in place to protect both information and infrastructure to facilitate sharing information securely and appropriately with partners.

(U) *People.* DOD must invest the resources necessary to field an adequately and consistently trained and properly equipped force. Training must encompass the entire workforce, as well as provide specialty training for those directly involved in cyberspace operations. Training must be continuous, and commanders must ensure that training is dynamic and updated to reflect new technology and address new threats. Although the roles and responsibilities of training the force remain a functional responsibility of the Military Departments, combatant commands, and agencies also must integrate mandatory cyberspace training. Adequate and consistent training will ensure that all personnel become an effective first line of defense and a human sensor. In particular, developing and integrating IO and network operations joint learning areas into joint professional military education improves the overall IO education baseline and ensures consistency among the DOD workforce. Military Departments should take advantage of IC training in cyberspace operations disciplines as appropriate to promote common standards and facilitate integrated and collaborative operations. Incorporating IO and network operations into all training and exercise programs is critical to ensure that warfighters gain a better understanding of IO and network operations capabilities and vulnerabilities within a training environment.

(U) Means. The unified employment of the combatant commands, Military Departments, agencies, field activities, and other organizational entities of the DOD and resources along with strategies, plans, policies, and programs constitute the military means for cyberspace operations. Combatant commands are responsible for operational planning and execution; the Military Departments organize, train, and equip forces to present to the joint force commander; and the various agencies and field activities support both. In addition, DOD will continue to leverage Reserve and National Guard contributions for cyberspace operations. In addition, judicious fielding of advanced technologies improves awareness, agility, protection, and response to threats against cyberspace and to our interests in cyberspace.

CHAPTER SIX

IMPLEMENTATION AND ASSESSMENT (U)

(U) Way Ahead. The Joint Staff has the responsibility to advise the Chairman of the Joint Chiefs of Staff on the progress of supporting plans and actions to meet the intent of the priorities and outcomes in Enclosure F. To this end, United States Strategic Command, with Joint Staff as co-lead, will develop an implementation plan and lead an annual assessment process. Within 60 days of approval, terms of reference for the implementation plan should be submitted to the Chairman for approval by the Secretary of Defense. The implementation plan will include representation across the DOD components. Following approval of the terms of reference, the implementation plan will develop specific tasks with lead agencies assigned.

(U) Assessment. Assessment is an important part of implementation. DOD components will provide assessments of progress that will be consolidated into a report to assess the effectiveness of the strategy and forwarded through the Chairman to the Secretary of Defense. The reporting process will be synchronized with the primary DOD decision processes. The assessment will examine metrics through measures of effectiveness that apply to the ways identified in the military strategic framework for cyberspace operations. Mitigating strategies based on the report findings will be executed using plans of action and milestones integrated throughout operations, requirements, planning, budgeting, and acquisition processes. To the extent possible, metrics and reporting will be shared with interagency and coalition partners, and coordinated with other key strategic efforts.

(U) Capabilities. To achieve these ends, forces will combine capabilities to create the necessary effects. Development of capabilities should augment these mission areas and contribute to strategic enablers through the current Joint Capabilities Integration and Development System. Although all Joint Capability Areas apply to cyberspace operations, the areas identified in Enclosure E merit specific emphasis.

(U) Strategic Priorities. DOD components are tasked with translating this strategy into action. The priorities focus DOD efforts to achieve the strategic goal and five specific ends using the ways outlined in the framework. The strategic priorities are:

- (U) *Gain and maintain the initiative to operate within adversary decision cycles.* Warfighters should use cyberspace to accelerate their own decision-making cycle while degrading that of the adversary. This involves maintaining a robust defense of cyberspace while exploiting adversary cyberspace vulnerabilities in order to understand the enemy's decision cycle and defensive weaknesses.

- (U) *Integrate capabilities across the full range of military operations using cyberspace.* DOD components must integrate cyberspace into deliberate and crisis plans. Combatant commands must work closely with Service components and DOD agencies to create fully integrated capabilities to conduct military operations. As capabilities are deployed to various theaters, they must complement or deconflict with existing operations and provide seamless interoperability with interagency, joint, coalition, and industry partners.

- (U) *Build capacity for cyberspace operations*. The Military Departments and certain agencies or commands should develop capabilities necessary to conduct cyberspace operations, including consistently trained personnel, infrastructure, and organizational structures. These organizations should work closely with combatant commands to integrate new capacity into existing operations through aggressive testing, exercises, and continual improvements to operations. Highly capable and agile forces using fully integrated technology are critical to delivering offensive and defensive capabilities cyberspace operations.

- (U) *Manage risk to cyberspace operations*. There are three types of risk: innate risk of operating in cyberspace resulting from threats and vulnerabilities; consequential risk of actions taken in cyberspace; and risk associated with resource choices. Leaders at all levels must balance each type of risk for effective operations.

(U) Outcomes. DOD components must develop and coordinate plans and roadmaps to ensure appropriate resource allocation for which the NMS-CO serves as a definitive reference. The strategic priorities above serve to translate the military strategic framework, described in Chapter Five, into focused efforts to ensure US military strategic superiority in cyberspace. The priorities serve as broad guidelines that DOD components can use to focus activities to attain capabilities organized around the doctrine, organization, training, materiel, leadership, personnel, and facilities (DOTMLPF) construct. DOD components should use the strategy to develop actions leading to the outcomes listed in Enclosure F.

ENCLOSURE A

LEGAL AUTHORITIES TABLE (U)

US Code	Title	Key Focus	Principal Organization	Role in Cyberspace
Title 6	*Domestic Security*	Homeland Security	Department of Homeland Security	Security of US Cyberspace
Title 10	*Armed Forces*	National Defense	DOD	Secure US Interests by Conducting Military Operations in Cyberspace
Title 18	*Crimes and Criminal Procedure*	Law Enforcement	Department of Justice	Crime Prevention, Apprehension, and Prosecution of Cyberspace Criminals
Title 32	*National Guard*	First Line Defense of the United States	Army National Guard, Air National Guard	Support Defense of US Interests in Cyberspace Through Critical Infrastructure Protection, Domestic Consequence Management and Other Homeland Defense-Related Activities
Title 40	*Public Buildings, Property, and Works*	Chief Information Officer Roles and Responsibilities	All Federal Departments and Agencies	Establish and Enforce Standards for Acquisition and Security of Information Technologies
Title 50	*War and National Defense*	Foreign Intelligence and Counter-Intelligence Activities	Intelligence Community Agencies Aligned Under the Office of the Director of National Intelligence	Intelligence Gathering Through Cyberspace on Foreign Intentions, Operations, and Capabilities

(INTENTIONALLY BLANK)

ENCLOSURE B

STRATEGIC GUIDANCE (U)

(U) HSPD-5, *Management of Domestic Incidents* (2003)

(U) HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection* (2003)

(b)(1)

(U) Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans* (2005)

(b)(1)

(U) *Unified Command Plan* (2006)

(U) *National Security Strategy* (2006)

(U) *National Strategy for Homeland Security* (2002)

(U) National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (2003)

(U) *National Strategy to Secure Cyberspace* (2003)

(U) *National Defense Strategy* (2005)

(U) *Security Cooperation Guidance* (2005)

(U) *Quadrennial Defense Review* (2006)

(U) *Strategy for Homeland Defense and Civil Support* (2005)

(U) *National Response Plan* (2004)

(U) *National Military Strategy* (2004)

(U) *DOD Information Assurance Strategic Plan* (2004)

(INTENTIONALLY BLANK)

ENCLOSURE C

EXAMPLES OF THREATS AND THREAT ACTORS (U)

(b)(1)

(U) Cyberspace threats generally fall within six categories: traditional, irregular, catastrophic, disruptive, natural, and accidental.

(U) *Traditional.* Traditional threats typically arise from states employing recognized military capabilities and forces in well-understood forms of military conflict. Within cyberspace, these threats may be less understood due to the continuing evolution of technologies and methods. Traditional threats are generally focused against the cyberspace capabilities that enable our air, land, maritime, and space forces and are focused to deny the US military freedom of action and use of cyberspace.

(U) *Irregular.* Irregular threats can use cyberspace as an unconventional asymmetric means to counter traditional advantages. These threats could also manifest through an adversary's selective targeting of US cyberspace capabilities and infrastructure. For example, terrorists could use cyberspace to conduct operations against our financial and industrial sectors while simultaneously launching other physical attacks. Terrorists also use cyberspace to communicate anonymously, asynchronously, and without being tied to set physical locations. They attempt to shield themselves from US law enforcement, intelligence, and military operations through use of commercial security products and services readily available in cyberspace. Irregular threats from criminal elements and advocates of radical political agendas seek to use cyberspace for their own ends to challenge government, corporate, or societal interests.

(U) *Catastrophic.* Catastrophic threats involve the acquisition, possession, and use of weapons of mass destruction (WMD) or methods producing WMD-like effects. Such catastrophic effects are possible in cyberspace because of the existing linkage of cyberspace to critical infrastructure SCADA systems. Well-planned attacks on key nodes of the cyberspace infrastructure have the potential to produce network collapse and cascading effects that can severely affect critical infrastructures locally, nationally, or possibly globally. For example, electromagnetic pulse events could cause widespread degradation and outright destruction of the electronic components that comprise cyberspace leading to the debilitating destruction of segments of the cyberspace domain in which operations must occur.

(U) *Disruptive.* Disruptive threats are breakthrough technologies that may negate or reduce current US advantages in warfighting domains. Global research, investment, development, and industrial processes provide an environment conducive to the creation of technological advances. DOD must be prepared for the increased possibility of adversary breakthroughs due to the continuing diffusion of cyberspace technologies.

(U) *Natural.* Natural threats that can damage and disrupt cyberspace include acts of nature such as floods, hurricanes, solar flares, lightning, and tornados. These types of events often produce highly destructive effects requiring DOD to support the continuity of operations in cyberspace, conduct consequence management, and restore cyberspace capacity. These events also provide adversaries the opportunity to capitalize on infrastructure degradation and diversion of attention and resources.

(U) *Accidental.* Accidental threats are unpredictable and can take many forms. From a backhoe cutting a fiber optic cable of a key cyberspace node, to inadvertent introduction of viruses, accidental threats unintentionally disrupt the operation of cyberspace. Although post-accident investigations show that the large majority of accidents can be prevented and measures put in place to reduce accidents, accidents must be anticipated.

(U) Cyberspace threat actors generally fall within six categories.

(b)(1)

[7] (U) National Intelligence Estimate: Cyber Threats to the Information Infrastructure, February 2004 [NIE-2004-01D/I] (2004).

[8] (U) Ibid.

(b)(1)

(INTENTIONALLY BLANK)

ENCLOSURE D

EXAMPLES OF VULNERABILITIES (U)

(U) A March 2006 Nielsen survey noted that nearly 70 percent of US citizens use the Internet, with more than 1 billion users worldwide. This access revolutionizes how Americans conduct their finances, shop, invest, entertain, etc. According to VeriSign, a company providing secure transactions, e-commerce resulted in over $12 billion US sales in 2004. Increases in the frequency and sophistication of cyberspace intrusions, coupled with civilian and military dependence, illustrate that any significant interruption of cyberspace could result in a crippling effect on our national defense and society.

(U) *Architecture.* The current cyberspace architecture is permissive to the conduct of malicious activity. Insecure communications protocols and software combined with the huge number of connection points in cyberspace make securing cyberspace an extremely difficult task. In addition, the nature of cyberspace enables military operations intended to be local in scope to become global rapidly in effect.

(U) *Operating with Partners.* Connecting to partner components of cyberspace, such as Federal departments and allies, introduces additional vulnerabilities especially if cyberspace security is not a partner priority or if security has been unevenly applied.

(U) *Technical Vulnerabilities.* Technical vulnerabilities are an inherent aspect of cyberspace operations. Vulnerabilities found in operating systems, software applications, and controlled interfaces can allow threat actors to gain unauthorized access to information systems and data, and enable them to disrupt system functionality at their discretion. Threat actors proficient in software programming, signaling command and control (C2), protocol architecture, or encryption may be able to inject malicious data into software, firmware, hardware, and encryption mechanisms to render the data useless or crack encryption for data collection.

(b)(1)

(U) *Commercial Technologies and Outsourcing.* Exploitation could occur anywhere within the technology life-cycle process. Throughout a product's life-cycle, adversaries can discover potential vulnerabilities in commercial off-the-shelf software and hardware installed on DOD systems and networks.

(b)(1)

(b)(1)

(U) *Physical Protection.* Insufficient protective measures or poor physical protection procedures for cyberspace components such as cables, facilities, sites, structures, and equipment could have significant negative consequences for operations.

(U) *Open Source Information.* Potential threat actors may use publicly available information and employ data mining methods to focus intelligence collection efforts and plan attacks against DOD networks. Proper OPSEC process implementation would assist in denying adversaries access to controlled unclassified information, which, in its aggregate, may be classified.

(U) *Training.* Personnel, including senior leaders, commanders, cyberspace operators, and ordinary users, all require thorough training for effective cyberspace operations. Poor training lessens awareness of adversary techniques such as social engineering to gain access to networks, systems, and information. In addition, since at some level all personnel operate in cyberspace, of paramount concern is adequate training to maintain and improve defense-in-depth measures. Poorly trained personnel may carelessly or incorrectly install, maintain, or secure systems; mishandle passwords; or improperly check for malicious software. Users, whether due to carelessness, lack of training, or lack of adherence to policies and procedures may unwittingly cause system denials, disruptions, or degradations, as well as data loss or compromise. Poorly trained operators can also introduce vulnerabilities to operations.

(U) *Policy Vulnerabilities.* Policies related to cyberspace are designed to codify desired behavior and actions conducive to reducing cyberspace vulnerabilities. Policies also ensure that offensive cyberspace operations are carried out only with appropriate authorities, risk management, and qualified personnel. Policies help guide and ensure deconfliction of cyberspace operations. Poorly enforced or poorly written policies and procedures place our operating environment, our operations, and broader US interests at risk. Lack of awareness of existing policy is another significant vulnerability.

(b)(1)

ENCLOSURE E

APPLICATION TO JOINT CAPABILITIES AREAS (U)

- (U) Joint Battlespace Awareness. Shared awareness and understanding of the battlespace are critical to *situational awareness* while *intelligence* plays a key role in supporting this awareness and understanding of the battlespace. Joint Battlespace Awareness applies across all the ways.

- (U) Joint Force Generation. Creating and developing the force necessary to conduct cyberspace operations applies to *people,* describing the need to ensure personnel receive adequate, consistent training and the tools necessary to accomplish mission objectives. The development of future capabilities is also important to *S&T.* This capability area ensures the necessary forces to implement *IO* and *network operations* are prepared to conduct operations.

- (U) Joint C2. Effective C2 ensures coordinated, deliberate action across *IO, network operations,* and *kinetic actions.* In addition, *intelligence* and *situational awareness* rely on C2 to enable effective collaboration.

- (U) Joint Information Operations. Capabilities identified and developed in this area will build and sustain *IO.* This capability area will also contribute to *intelligence.*

- (U) Joint Net-Centric Operations. Components of joint net-centric operations such as information transport, enterprise services, and information assurance will sustain *IO* and *network operations.* This capability area will also contribute to *situational awareness.*

- (U) Joint Global Deterrence. Development of appropriate force projection facilitates *IO and kinetic actions* mission areas. *Partnering* relies on capabilities developed for coalition military cooperation and integration.

- (U) Joint Homeland Defense. Further development of network defense and critical infrastructure protection capabilities will contribute to *IO* and *network operations.* As key relationships are examined, *law-enforcement & counterintelligence,* and *themes and messages* will be affected. Consequence management applies to *law and policy.*

- (U) Joint Interagency Integration, Intergovernmental Organization Coordination, nongovernmental Organization Coordination. Successful integration is crucial to *partnering* and *law and policy* and applies across all of the ways.

(INTENTIONALLY BLANK)

ENCLOSURE F

STRATEGIC PRIORITIES AND OUTCOMES (U)

(U) The strategic priorities and outcomes are aligned with the appropriate component of the DOTMLPF construct. Military Departments and agencies should consider these as they allocate resources. Combatant commands should incorporate these outcomes into actions as they develop capabilities and plans in their particular areas of responsibility.

(U) *Gain and Maintain the Initiative to Operate Within Adversary Decision Cycle.*

- (U) Develop joint doctrine for all aspects of cyberspace operations. Include revised definition and development of terms to describe emerging cyberspace operations mission areas in accordance with the Joint Doctrine Development and Joint Operations Concept Development processes. [Doctrine]

(b)(1)

- (U) Employ an enterprise-wide system of sensors whose data is automatically distributed to those who need it on detection of malicious activity. [Materiel]
- (U) Maintain continuous active layered defenses using existing information assurance guidance to protect the confidentiality, integrity, availability, authentication, and non-repudiation of information as it is processed, created, and manipulated at rest and in-motion. [Leadership]
- (U) Rapidly synthesize intelligence to support cyberspace operations. [Doctrine]
- (U) Improve the collection and use of intelligence to produce indications and warnings in order to anticipate, not just detect, attacks. [Leadership]
- (U) Refine C2 processes for cyberspace operations so that they are well understood, agile, and integrated with the full range of military operations. [Doctrine]
- (U) Establish readiness reporting for cyberspace operations. [Doctrine]

(U) *Integrate Capabilities Across the Full Range of Military Operations Using Cyberspace.*

- (U) Change and implement the appropriate rules of engagement (ROE) to facilitate cyberspace operations. [Doctrine]
- (U) Conduct collaborative planning for integrated cyberspace operations, synchronizing with other military and intelligence operations. [Leadership]

(b)(1)

- (U) Transform organizations to enable joint cyberspace operations and integrate Military Department-focused efforts to shape cyberspace. [Organization]
- (U) Augment and integrate intelligence support into all aspects of cyberspace operations. [Personnel]
- (U) Describe the complete set of capabilities required to improve secure information sharing in a phased, incremental approach. [Materiel]

- (U) Transform operations to implement increased self-defense and self-healing capabilities using emerging automated tools to respond more quickly to cyberspace events. [Organization]
- (U) Ensure allied and coalition contributions are integrated into US efforts to secure cyberspace. [Organization]
- (U) Develop processes for cyberspace targeting, collateral damage estimation, standing and special ROE, and measures of effectiveness assessments that are integrated within the joint force targeting process and result in tailored, effects-based operations that support joint commander objectives, guidance, and intent. [Organization]
- (U) Develop modeling and simulation tools and methods to support cyberspace capability development, adaptive planning, and integrated operations. [Materiel]

(U) *Build Capacity for Cyberspace Operations.*

(b)(1)

- (U) Improve abilities to conduct and share analysis of military effects in cyberspace, cyber intelligence preparation of the environment (CIPE), and post-event forensic analysis. [Leadership]
- (U) Increase investments and acquisition in tools for cyberspace operations. Build on cyberspace exploitation dual-use capabilities as appropriate. [Materiel]
- (U) Conduct appropriate reviews and source code testing to identify malicious code or unauthorized functionality. [Organization]
- (U) Establish a mechanism and a managed process to ensure system configuration facilitates joint operations. [Leadership]
- (U) Architect the GIG to support different levels of information assurance and INFOCON across regional and functional boundaries. [Facility]
- (U) Conduct enterprise-wide acquisition of tools and infrastructure equipment using a clearing-house concept to reduce duplication, enhance collaboration, and reduce acquisition and training costs. [Materiel]

(b)(1)

- (U) Establish coalition cyberspace operations processes and exercises to include cyberspace capacity building programs, and policies for information sharing. [Training]
- (U) Integrate cyberspace operations into existing exercises. [Training]
- (U) Tailor education and training to meet specific needs of leaders, professionals, and users in cyberspace. [Training]
- (U) Ensure coherence among various compartmented programs. [Leadership]
- (U) Expand information operations range to incorporate integrated cyberspace operations training and exercise. [Facility]
- (U) Make information visible, accessible, and understandable. [Doctrine]

(U) *Manage Risk for Cyberspace Operations.*

- (U) Hold leaders at all levels responsible and accountable for cyberspace operations in the same manner as accountability is addressed in the other domains. [Leadership]
- (U) Identify and manage operational dependencies in the cyberspace domain. [Leadership]
- (U) Develop standardized risk management processes across the range of defensive cyberspace operations and link to resource allocation decisions. [Leadership]
- (U) Understand, mitigate, and manage the effects of foreign ownership, control, or influence (FOCI) on operations using cyberspace. [Leadership]
- (U) Develop integrated vulnerability assessment processes to facilitate protection, detection, and response to cyberspace attacks and intrusions. [Doctrine]
- (U) Assess operational risk of using hardware and software developed outside the United States or by untrusted workers within the United States. [Materiel]
- (U) Review all communications with non-authenticated sources and, where practical, reduce them. [Doctrine]
- (U) Improve OPSEC education and training to support cyberspace operations. [Training]

(INTENTIONALLY BLANK)

ENCLOSURE G

DISTRIBUTION LIST

	Copies
Office of the Secretary of Defense	3
Office of the Deputy Secretary of Defense	2
Secretaries of the Military Departments	2
Under Secretaries of Defense	2
Assistant Secretaries of Defense	5
General Counsel of the Department of Defense	2
Deputy Assistant Secretaries of Defense	5
Chairman of the Joint Chiefs of Staff	3
Vice Chairman of the Joint Chiefs of Staff	3
Chief of Staff, US Army	5
Chief of Naval Operations	5
Chief of Staff, US Air Force	5
Commandant of the Marine Corps	5
Commandant, US Coast Guard	3
Commander, US Joint Forces Command	3
Commander, US Central Command	5
Commander, US European Command	5
Commander, UN Command/Combined Forces Command	3
Commander, US Pacific Command	5
Commander, US Southern Command	5
Commander, US Special Operations Command	3
Commander, US Strategic Command	5
Commander, US Transportation Command	5
Commander, US Northern Command	5
Commander, US Element, NORAD	1
Assistant to the Chairman of the Joint Chiefs of Staff	1
Director, Joint Staff	1
Director for Manpower and Personnel, Joint Staff	1
Director for Intelligence, Joint Staff	5
Director for Operations, Joint Staff	5
Director for Logistics, Joint Staff	5
Director for Strategic Plans and Policy, Joint Staff	5
Director for Command, Control, Communications, and Computer Systems, Joint Staff	5
Director for Operational Plans and Joint Force Development, Joint Staff	3
Director for Force Structure, Resources, and Assessment, Joint Staff	3
US Military Representative, NATO Military Committee	1
Director, Defense Information Systems Agency	1
Director, Defense Intelligence Agency	1
Director, Defense Logistics Agency	1
Director, Defense Security Cooperation Agency	1
Director, Defense Threat Reduction Agency	1
Director, National Geospatial-Intelligence Agency	1
Director, National Security Agency/Chief, Central Security Service	1
Director, National Guard Bureau	1
Director, Combating Terrorism Center, United States Military Academy	1

Director, Combating Terrorism Center, Naval Postgraduate School	1
Director, Missile Defense Agency	1
US National Military Representative to Supreme Headquarters Allied Powers Europe	1
Director, Joint Command and Control Warfare Center	1
Chief, National Military Command Center (Site R)	1
Chief, National Airborne Operations Center	4
Secretary, Joint Staff	7
Information Management Division, Joint Staff	7

GLOSSARY

computer network attack (CNA). Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. [DODI 3600.02]

computer network attack (CNA) operational preparation of the environment (CNA-OPE). CNA-OPE are operations conducted to gain and/or confirm access to, and gather key information on the target network concerning the capabilities and configuration of, targeted networks or systems and to facilitate target acquisition and target analysis in preparation for CNA and/or other offensive missions. [CJCSI 3121.01B]

computer network defense (CND). Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks. CND employs IA capabilities to respond to unauthorized activity within DOD information systems and computer networks in response to a CND alert or threat information. Note: CND also employs intelligence, counterintelligence, law enforcement, and other military capabilities to defend DOD information and computer networks. [DODI 3600.02]

computer network exploitation (CNE). Enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks. [DODI 3600.02]

computer network operations (CNO). Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. [JP 1-02]

continuity of operations plan (COOP). The degree or state of being continuous in the conduct of functions, tasks, or duties necessary to accomplish a military action or mission in carrying out the national military strategy. It includes the functions and duties of the commander, as well as the supporting functions and duties performed by the staff and others acting under the authority and direction of the commander. [JP 1-02]

counterintelligence (CI). Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. [JP 1-02]

global information grid (GIG). The globally interconnected, end-to-end set of information capabilities associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in 40 USC 11103(a) (formerly section 5142 of the Clinger-Cohen Act of 1996) [Section 11103(a) of title 40, USC].

information assurance. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. [JP 1-02]

information environment. The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. [JP 1-02]

information operations (IO). 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. [DODI 3600.02]

intelligence. 1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. [JP 1-02]

network operations. Activities conducted to operate and defend the Global Information Grid. [JP 1-02]

strategic communications (SC). Focused US Government (USG) efforts to understand and engage key audiences in order to create, strengthen, or preserve conditions favorable for the advancement of USG interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all elements of national power. [JP 1-02]

threat. Any circumstance or event with the potential to affect an information system adversely through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. [CNSS Instruction No. 4009]

vulnerability. 1. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. 2. The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. 3. In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system. [JP 1-02]

NOTE: Unless a glossary entry is followed by the caption "[JP 1-02]" to indicate incorporation in the DOD Dictionary of Military and Associated Terms (JP 1-02), the entry is applicable only in the context of this document and not to be used outside that context.

(INTENTIONALLY BLANK)

JOINT CHIEFS OF STAFF