

**Department of Defense  
Homeland Defense  
and  
Civil Support  
Joint Operating Concept**



**Version 2.0**

**01 October 2007**

The Department of Defense (DOD) Homeland Defense (HD) and Civil Support (CS) Joint Operating Concept (JOC) was produced by the Strategy and Policy Division (J52), United States Northern Command (USNORTHCOM), in accordance with direction set forth in the Transformation Planning Guidance (TPG), dated April 2003, the Joint Operations Concepts (JOpsC) Paper, dated November 2003, Secretary of Defense Memorandum, Subject: Joint Concept Revision Plan, dated 14 October 2004, the Capstone Concept for Joint Operations (CCJO), dated August 2005, and the CJCSI 3010.02B, Joint Operations Concepts Development Process (JOpsC-DP), dated 27 January 2006.

The DOD HD and CS JOC is one of the Joint Requirements Oversight Council (JROC) directed four initial JOCs. Version 2.0 to the JOCs for Deterrence Operations, Major Combat Operations, and Military Support to Stabilization, Security, Transition and Reconstruction Operations have been developed by other Combatant Commands.

This document replaces the DOD Homeland Security (HLS) JOC Version 1.0 dated February 2004. It presents the next iteration in a continuing process to build-on and improve upon the concept presented in Version 1.0.

**Point of Contact for the DOD HD and CS JOC:**

CAPT Bill Cogan, USN, Chief, Strategy and Policy Division (J52),  
USNORTHCOM  
DSN: 692-1097      Commercial: 719-554-1097



Technical cognizance for this assessment was provided by Col Karin Murphy, CDR Donald May, and Mr. Barry Cardwell, USNORTHCOM. CAS, Incorporated provided support for this analysis as the prime contractor (POC: Mr. Jimmie Perryman [910-231-2162]).

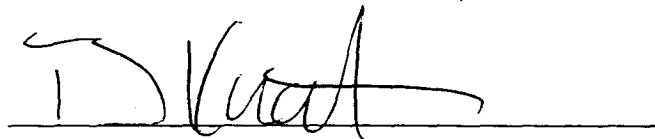
## APPROVAL

As the lead author, U.S. Northern Command matured this concept through the use of joint and Service operational lessons learned and experimentation: numerous co-sponsored joint wargames, seminars, workshops and other concept development venues. This process was guided by direct input from the Joint Chiefs of Staff.

During the development of this concept each Service, combatant command, selected members of the Joint and OSD staffs and selected non-DOD agencies made significant contributions. Also included throughout were a host of active and retired flag and junior officers, academics, and professional strategic thinkers.

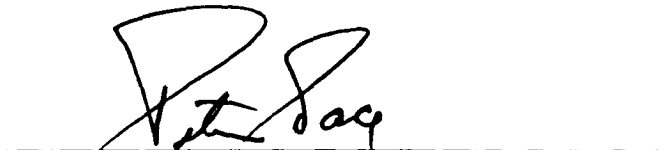
U.S. Northern Command will continue to use experimentation and lessons learned to refine this concept. The next revision period leading to Version 3.0 is expected to commence in the June 2008 timeframe.

APPROVED



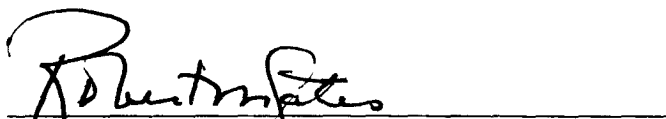
**TIMOTHY J. KEATING**  
Admiral, United States Navy  
Commander, USNORTHCOM

APPROVED



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

APPROVED



**ROBERT M. GATES**  
Secretary of Defense

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

## PREFACE

## EXECUTIVE SUMMARY

<b>1.0 PURPOSE</b> .....	1
<b>2.0 SCOPE</b> .....	1
2.a. DOD Missions to be Accomplished .....	2
2.b. DOD Homeland Defense and Civil Support Paradigm .....	5
2.c. Assumptions and Trends.....	8
<b>3.0 MILITARY PROBLEM</b> .....	10
3.a. Threat Environment.....	11
3.b. Diverse and Uncertain Threats to the Homeland .....	11
3.c. National Challenge .....	13
<b>4.0 SOLUTION</b> .....	17
4.a. Global, Integrated, Active, and Layered Defense .....	17
4.b. Unity of Effort .....	24
4.c. Methods to Reduce Uncertainty.....	27
4.d. Desired End State, Effects, and Required Capabilities .....	33
<b>5.0 RISKS AND MITIGATION</b> .....	45
5.a. Risks to the Concept .....	45
5.b. Mitigation of Risks .....	45
<b>6.0 IMPLICATIONS</b> .....	46
6.a. Essential Characteristics .....	47
6.b. Relationship to Other Concepts.....	50
6.c. Related Issues.....	54

**CONCLUSION** ..... 58

**7.0 APPENDICES**

Appendix A: References.....A - 1

Appendix B: Glossary and Acronyms .....B - 1

Appendix C: Operational Level Effects and Associated Joint  
Capability Areas .....C - 1

Appendix D: Concept Assessment and Experimentation..... D - 1

Appendix E: HD and CS Illustrative Vignettes .....E - 1

## PREFACE

The future Joint Force<sup>1</sup> will operate in a complex and uncertain global security environment characterized by a combination of persistent and emerging threats to the Homeland<sup>2</sup>. To defend the Homeland, the future Joint Force will require the ability to counter threats from a variety of potential adversaries ranging from nation states to non-state sponsored terrorist organizations and individuals. Since these adversaries are likely to employ asymmetric and unconventional capabilities, successful employment of the Joint Force also will depend upon close coordination with multi-national, interagency<sup>3</sup>, and non-governmental partners. Changes in the security environment will continue to shape the characteristics of joint warfare and require ongoing transformation of the Joint Force.

In response to changes in the security environment and the events of September 11, 2001, the Secretary of Defense issued the Transformation Planning Guidance (TPG) to provide strategic guidance for the transformation of DOD and the Joint Force. The (TPG) also directed the Chairman of the Joint Chiefs of Staff (CJCS) to oversee the development, experimentation, and validation of Joint concepts as a primary mechanism to implement the transformation strategy. The initial Joint Operations Concepts (JOpsC) Paper established a capabilities-based methodology for joint force development through a family of Joint concepts. The JOpsC was based on the Range of Military Operations (ROMO)<sup>4</sup> that identified the activities for which the Joint Force must prepare. The JOpsC, now known as the Capstone Concept for Joint Operations (CCJO), serves as the overarching conceptual

---

<sup>1</sup> As defined in *CJCSI 3010.02B*, the term “the Joint Force” in its broadest sense refers to the Armed Forces of the United States, while the term joint force (lower case) refers to an element of the Armed Forces that is organized for a particular mission or task.

<sup>2</sup> For the purposes of this document, the term “the Homeland” (with a capital H) is considered to include the 50 United States (US), US territories and possessions in the Caribbean Sea and Pacific Ocean, and the immediate surrounding sovereign waters and airspace. For a complete listing of Pacific territories, possessions, and freely associated states that are included in the Homeland, refer to *Strategy for Homeland Defense and Civil Support*, page 8, footnote 2.

<sup>3</sup> The term “interagency” entails the full range of organizations outside DOD down to the state, local, and tribal organizational level. Interagency coordination, as defined in *JP 1-02* within the context of DOD involvement, is the coordination that occurs between elements of DOD and engaged US Government agencies for the purpose of accomplishing an objective.

<sup>4</sup> See *JROCM 023-03*, Interim Range of Military Operations, 28 January 2003.

framework for the family of Joint Operating Concepts (JOCs), Joint Functional Concepts (JFCs), and Joint Integrating Concepts (JICs). This family of Joint concepts describes how the Joint Force is expected to operate in the future and guides the development of future Joint capabilities.

The first version of this document, the Department of Defense Homeland Security Joint Operating Concept, dated February 2004, was approved by the Secretary of Defense on 14 October 2004.

The Secretary of Defense directed<sup>5</sup> that the next version contain more description of how operations will be conducted in the “seam of uncertainty” between DOD responsibilities and other federal and state agencies, and local authorities, and that it contain the following: 1) a theory of war that addresses the National Defense Strategy (NDS); 2) desired effects and end states; 3) descriptions of how operations will be conducted; 4) assessments of associated risks and how they will be mitigated; and 5) identification and prioritization of needed capabilities. This version complies with Secretary of Defense guidance.

---

<sup>5</sup> *Secretary of Defense Memorandum for the Chairman of the Joint Chiefs of Staff*;  
Subject: Joint Concept Revision Plan, dated 14 October 2004.



## **EXECUTIVE SUMMARY**

The DOD Homeland Defense and Civil Support Joint Operating Concept (DOD HD and CS JOC) describes how DOD intends to fulfill its responsibilities associated with securing the Homeland. This JOC describes how the Joint Force will plan, prepare, deploy, employ, and sustain the force in the 2012 - 2025 timeframe to detect, deter, prevent, or if necessary, defeat attacks against the Homeland, provide defense support of civil authorities, and plan for emergencies. Based on the desired end state and effects, this concept serves to guide the development of future capabilities needed within a specific segment of the ROMO that includes HD and CS missions and Emergency Preparedness (EP) planning activities.

A secure United States (US) Homeland is the Nation's first priority and is fundamental to the successful execution of its military strategy. The Homeland is confronted with threats ranging from traditional national security threats (for example, ballistic missile attack) to law enforcement threats (for example, bank robbery). There are clear definitions of both ends and less clarity in the middle where military and civilian roles often overlap. In the middle is a "seam" of ambiguity where threats are neither clearly national security threats (the primary responsibility of DOD) nor clearly law enforcement threats (the responsibility of the Department of Homeland Security [DHS], the Department of Justice (DOJ), or other agencies). In addition, DOD assistance may be required to mitigate the effects and manage the consequences of catastrophic events. This situation highlights the criticality of communication, coordination, and cooperation among DOD and federal, state, local, and international partners.

It is important to understand the distinction between the DOD role with respect to national security and the role of DHS as lead federal agency (LFA)<sup>6</sup> for Homeland Security (HS), as defined in the National Strategy for Homeland Security (NSHS) as well as DOJ, DOS, and other agencies' roles outside of the NSHS in securing the Homeland. Although there is significant overlap between DOD's role and that of DHS and other agencies, DOD's role extends beyond the scope of the NSHS

---

<sup>6</sup> As defined in *JP 1-02*, LFA is "the federal agency that leads and coordinates the overall federal response to an emergency. Designation and responsibilities of a lead federal agency vary according to the type of emergency and the agency's statutory authority."

paradigm (strictly concerned with terrorist attack) to address conventional and unconventional attacks and their effects on the Homeland by **any** adversary (including, but not strictly limited to, terrorists). DOD is responsible for HD, while other federal departments and agencies (DHS or the State Department, for example) support DOD's efforts.

### **Military Problem**

This concept is focused on the military problem of how DOD will fulfill responsibilities of securing the Homeland, including how: 1) DOD detects, deters, prevents, or, if necessary, defeats external threats or aggression to the Homeland, 2) DOD will be prepared to respond to catastrophic incidents as appropriate or as directed, and 3) DOD will integrate and operate with its U.S. and international partners to achieve unity of effort for HD and CS.

### **Solution**

The solution to the military problem described in this JOC is multi-faceted. At the strategic level is an active, layered defense designed to detect, deter, prevent, or, if necessary, defeat threats as far from the Homeland as possible. The solution includes unified action founded on national strategies, 2006 Quadrennial Defense Review (QDR) guidance, and CCJO central and supporting ideas required by the Joint Force to accomplish HD and CS missions. Methods to reduce uncertainty, including a National Homeland Security Plan (NHSP) to enable a coordinated national effort in pre-attack national security measures (detect, deter, prevent, or, if necessary, defeat external threats<sup>7</sup> and aggression) are identified and are another element of the solution. Three campaign frameworks linked to three related "seam" environments in which DOD may operate are used to illustrate conceptually how uncertainty can be reduced between DOD responsibilities and those of DOD's partners. The final element of the solution is the identification of the desired end state, effects, and at the operational level, Joint Force Commander actions and capabilities. How DOD applies the elements of this multi-faceted solution is essential to unified action between DOD

---

<sup>7</sup> As referenced in *Strategy for Homeland Defense and Civil Support* (reference aaa), Homeland Defense includes missions such as domestic air defense. DOD recognizes that threats planned or inspired by "external" actors may materialize internally. The reference to "external threats" does not limit where or how attacks could be planned and executed. DOD is prepared to conduct HD missions whenever the President, exercising his constitutional authority as Commander in Chief, authorizes military actions.

and its partners, especially in the “seam of uncertainty” when roles and responsibilities overlap.

The transit of threats from their source to their target in the Homeland presents DOD and its DOD partners with opportunities to detect, deter, prevent, or if necessary defeat the threat. The central idea of this concept is for DOD to contribute to a national HD / CS system-of-systems that is active and layered. The objective is to deal with threats to the United States as early and as far forward from the Homeland as possible, and in the event of successful attack or natural catastrophe, to support an integrated national response that occurs as quickly and effectively as possible.

This central idea has two key supporting ideas. First, HD and CS (including EP) are ***national*** missions to which DOD contributes. This is a perspective with far-reaching consequences for how DOD and others plan, prepare, and conduct operations. Second, these integrated national HD and CS activities are conducted via an ***active, layered defense*** comprised of a number of overlapping systems-of-systems.

This construct of an active, layered defense conceptually divides the world into three regions (Forward, Approaches, and the Homeland) and depicts “**how**” DOD will coordinate and conduct operations across and within each region to facilitate and produce an active, layered defense. Geographic and functional integration within DOD, as well as with its partners will be required to achieve unity of effort across all three regions since threats may cross domains or overlap areas of responsibility (AOR). The three regions, as well as the “global commons”<sup>8</sup> of international waters and airspace, space, and cyberspace, define a complex battlespace wherein DOD must maintain superiority through strategic access and control. An active, layered defense designed to defeat threats as far from the Homeland as possible requires an adaptive, end-to-end process that operationalizes **how** DOD conducts any HD or CS mission.

Unified action to achieve unity of effort is especially paramount in how DOD will conduct operations in the “seam of uncertainty”. The Joint Force will need to apply three strategic principles, as discussed in the National Military Strategy (NMS), to guide effective operations in the seam. Those principles are agility, decisiveness, and integration. When all three principles are integrated in DOD and its partners’ HD, CS, EP,

---

<sup>8</sup> Refer to the *National Defense Strategy*, *National Military Strategy*, and *Strategy for Homeland Defense and Civil Support* for more information on the Global Commons.

and HS actions, the “seam of uncertainty” between DOD responsibilities and those of other federal, state, and local authorities will be mitigated.

To enhance unified action and reduce the uncertainty in the overlap of responsibilities between DOD and its partners, this document introduces the concept of a NHSP. The NHSP construct, similar in nature to the National Response Plan (NRP), would address integration of detect, deter, prevent, and, if necessary, defeat roles and responsibilities required to ensure a coordinated and integrated national effort between DOD and its partners. This JOC introduces the concept of a NHSP as part of DOD's solution to the military problem in addressing the “seam of uncertainty” through integrated and coordinated DOD and its partners’ efforts. Responsibilities for development and specific content of a NHSP are beyond the scope of this JOC.

## **Conclusion**

The DOD HD and CS JOC identifies the most prevailing problem facing DOD in the 2012 - 2025 timeframe; how DOD will perform responsibilities of securing the Homeland, including detecting, deterring, preventing, or if necessary, defeating external threats or aggression to the Homeland, how to be prepared to respond to catastrophic incidents as appropriate or as directed, and how to integrate and operate with non-DOD and international partners to achieve unity of effort for HD and CS. This JOC proposes a multi-faceted solution with an active, layered defense, unified action to achieve unity of effort, methods to reduce uncertainty (including the proposal for a NHSP), and the desired end state, effects, and capabilities that the Joint Force Commander will need in the 2012-2025 timeframe. Illustrative vignettes are provided that demonstrate how the elements of the solution, as well as the identified desired end state, effects, and required capabilities, relate and contribute to solving the military problem.

## 1.0 PURPOSE

**This DOD HD and CS JOC describes how DOD intends to fulfill its responsibilities associated with securing the Homeland, including HD and CS, in the 2012 - 2025 timeframe.** This concept is intended to spur discussion and debate and provide an azimuth for the development of subsequent Joint Operating, Functional, and Integrating Concepts. This JOC establishes a conceptual framework for analyzing needed HD and CS capabilities as part of the Joint Capabilities Integration and Development System (JCIDS), and identifies potential areas for Joint experimentation. It describes how the future Joint Force will plan, prepare, deploy, employ, and sustain the force in detecting, deterring, preventing, or if necessary defeating attacks against the Homeland, provide defense support of civil authorities, and plan for emergencies. It builds on the fundamental actions that the Joint Force must take to establish, expand, and secure reach; acquire, refine, and share knowledge; and identify, create, and exploit effects as described in the CCJO to ensure a coordinated and effective national effort in securing the Homeland.

The DOD HD and CS JOC does not provide detailed Military Department requirements or address specific platforms or systems. It provides an overarching conceptual perspective to facilitate Joint experimentation and assessment activities and assists in the development and integration of subsequent Joint Operating, Functional, and Integrating Concepts by identifying the desired end state, effects, and operational capabilities needed to conduct HD and CS operations. The JOC also provides the conceptual framework for analyzing HD and CS capabilities and requirements. This document describes how DOD can facilitate unified action with other federal, state, and local authorities to operate effectively in the area where capabilities and responsibilities overlap between DOD and its DOD partners.

## 2.0 SCOPE

The scope of this concept is bounded by several factors, each crucial to understanding the military problem facing DOD, as well as the solution to that problem as presented in this JOC. The scope of this concept is necessarily broad to account for traditional, irregular, catastrophic, and disruptive challenges to DOD in the 2012 - 2025 timeframe. Important in bounding the scope is to understand the mission areas DOD must be prepared to function in to protect the Homeland. Equally important is to understand that although DOD must be prepared to provide support when directed to civil authorities in CS missions, HD missions are the primary focus and a higher priority for

DOD. The scope is also bounded through an understanding of the HD and CS paradigm to appreciate fully the distinction between DOD roles and responsibilities and those of DHS and other agencies. Assumptions and trends provide the context under which this concept applies.

## **2.a. DOD Missions to be Accomplished**

DOD must plan for and be able to defend the Homeland and provide support to civil authorities simultaneously, as directed. By so doing, DOD helps preserve the Nation's freedom of action and ensures the ability of the United States to project and sustain power wherever and whenever required. DOD's responsibilities for securing the Homeland fall into three areas: HD, CS operations, and EP planning activities.

HD operations help ensure the integrity and security of the Homeland by detecting, deterring, preventing, or, if necessary, defeating threats and aggression against the United States as early and as far from its borders as possible so as to minimize their effects on US society and interests.<sup>9</sup> Effective HD operations require an active, externally focused defense conducted in depth by layering integrated military, interagency, and multi-national partner capabilities beginning at the source of the threat. The mission sets for HD include<sup>10</sup>:

**Homeland Defense (HD):** The protection of US sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression, or other threats as directed by the President. The Department of Defense is responsible for HD. *(Strategy for Homeland Defense and Civil Support)*

- ❖ **Air and Space Defense**
- ❖ **Land Defense**
- ❖ **Maritime Defense**
- ❖ **Cyber Defense**

DOD also may be directed to assist civilian authorities in order to save lives, protect property, enhance public health and safety, or to lessen or avert the threat of a catastrophe. DOD maintains many unique capabilities that can be used to mitigate and manage the consequences

---

<sup>9</sup> Deterrence operations and HD are intrinsically related in that each builds upon and supports the other.

<sup>10</sup> HD and CS missions, as well as EP planning activities are defined (with source information) in Appendix B: Glossary and Acronyms.

of both natural and man-made disasters and must be prepared to provide support to federal, state, and local authorities<sup>11</sup>. The President and the Secretary of Defense determine priorities regarding what DOD resources will be made available. The mission sets for CS described in Version 1.0 of this JOC include: Military Assistance to Civil Authorities (MACA); Military Support to Civilian Law Enforcement Agencies (MSCLEA); and Military Assistance for Civil Disturbances (MACDIS). CS is also referred to as Defense Support of Civil Authorities (DSCA).

As an integral part of its HD and CS missions, DOD has responsibilities to help prepare for emergencies through measures taken in advance of an emergency to reduce loss of life and property and protect the Nation's institutions. Responsibilities include support to continuity of operations (COOP) and continuity of government (COG). Federal, state, and local government agencies have COOP plans for their vital functions. These plans ensure continuation of minimum essential functions throughout a range of consequences from natural disasters to acts of terrorism. COOP planning normally includes: line of succession, delegation of authorities, alternate facilities and safekeeping of records, operating procedures, security, equipment, and communications. The COG program ensures the continued performance of essential functions and support of the President during national security emergencies. COG is basic to the survival of the Nation. In addition to COOP and COG, DOD may be tasked with other missions related to EP upon Presidential direction.

There are three circumstances<sup>12</sup> that govern DOD involvement in HD and CS operations and EP planning activities in the Homeland:

- ❖ **In Extraordinary Circumstances**, DOD would conduct military missions such as ballistic missile defense (BMD), air

**Civil Support (CS):** DOD support to US civil authorities for domestic emergencies, and for designated law enforcement and other activities. (JP 3-26)

**Defense Support of Civil Authorities (DSCA):** DOD support, including Federal military forces, the Department's career civilian and contractor personnel, and DOD agency and component assets, for domestic emergencies and for designated law enforcement and other activities. DOD provides DSCA when directed to do so by the President or Secretary of Defense. (Strategy for Homeland Defense and Civil Support)

---

<sup>11</sup> Under the *Robert T. Stafford Disaster Relief and Emergency Assistance Act*, American Indian tribes also may request support from the Federal government.

<sup>12</sup> Source: *The National Defense Strategy of the United States of America*, March 2005, p. 10, and codified in *National Strategy for Homeland Security*, July 2002, p. 13.

patrols, or maritime defense operations as the lead in defending the Homeland, supported by other agencies. Included in this category are cases in which the President, exercising constitutional authority as Commander in Chief and Chief Executive, authorizes military actions to counter threats within the United States, as well as steady-state operations in which DOD is preparing and / or posturing for extraordinary circumstances. On an international level, DOD would work with other nations to resolve regional conflicts and crises lending support of unique capabilities, and in other cases, would be supported by international partners.

- ❖ **In Emergency Circumstances**, DOD could be directed to act quickly to provide unique capabilities when the need surpasses the capacities of civilian responders. In such circumstances, other federal agencies take the lead and DOD supports. Examples of circumstances include responding to an attack or to catastrophic natural / man-made events such as earthquakes, forest fires, floods, hurricanes, tornados, or infectious epidemics.
- ❖ **In Limited-Scope Missions**, such as special events (for example, the Olympics) or assisting other federal agencies to develop capabilities to detect chemical and biological agents, where the other agencies have the lead and DOD supports.

These three circumstances are neither mutually exclusive nor static. At any given time DOD could be conducting multiple operations concurrently under some or all of these circumstances. Although DOD will normally perform a supporting function in response to catastrophic situations within the Homeland, planning should include scenarios where DOD is directed to assume a lead role. Any number of potential scenarios could necessitate a transition (for example, transitioning from a “limited scope” mission to “emergency circumstances” after a terrorist attack at a special event).

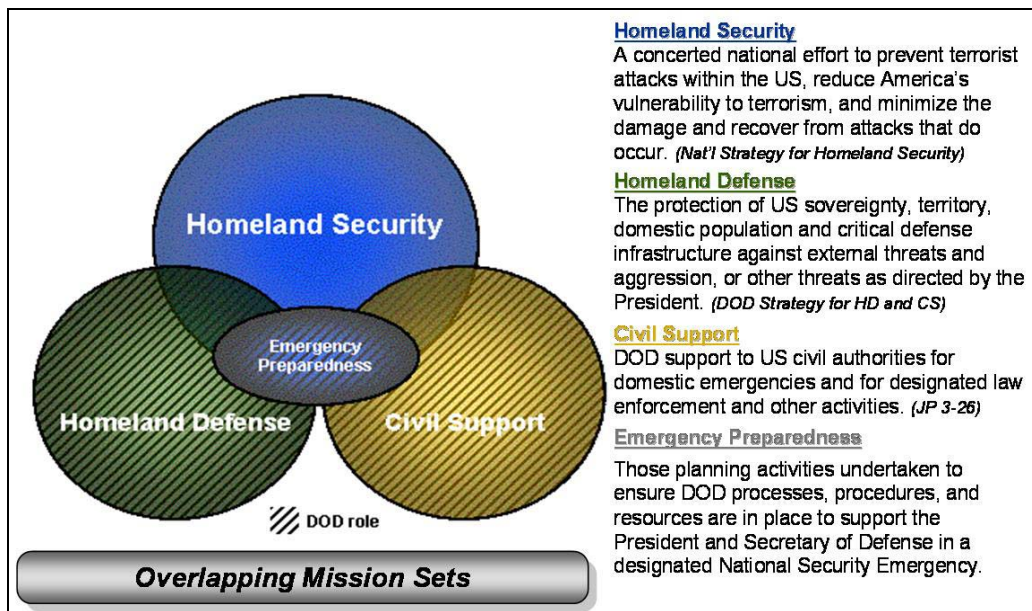
The degree of success in each mission set is difficult to measure, as many of the missions involve deterrence and dissuasion (concepts not easily quantified). Success in the HD mission is defined as detecting, deterring, preventing, and, if necessary, defeating a direct attack upon the Homeland. For CS, success is defined as responding, when directed and within required timeframes, to 100% of requests for assistance (RFA) approved by the Secretary of Defense, effective execution of situational driven DOD responsibilities associated with the RFA, and timely and efficient transfer of responsibilities back to supported agencies in accordance with pre-established policies and procedures.



Success for DOD in EP planning is defined as development and maintenance, in cooperation with the heads of other departments and agencies, of national security emergency plans, programs, and mechanisms that ensure effective mutual support between and among the military, civil government, and the private sector.<sup>13</sup>

**2.b. DOD Homeland Defense and Civil Support Paradigm**

A secure US Homeland is the Nation’s first priority and is fundamental to the successful execution of the Nation’s military strategy. It is also essential to America’s ability to project power,



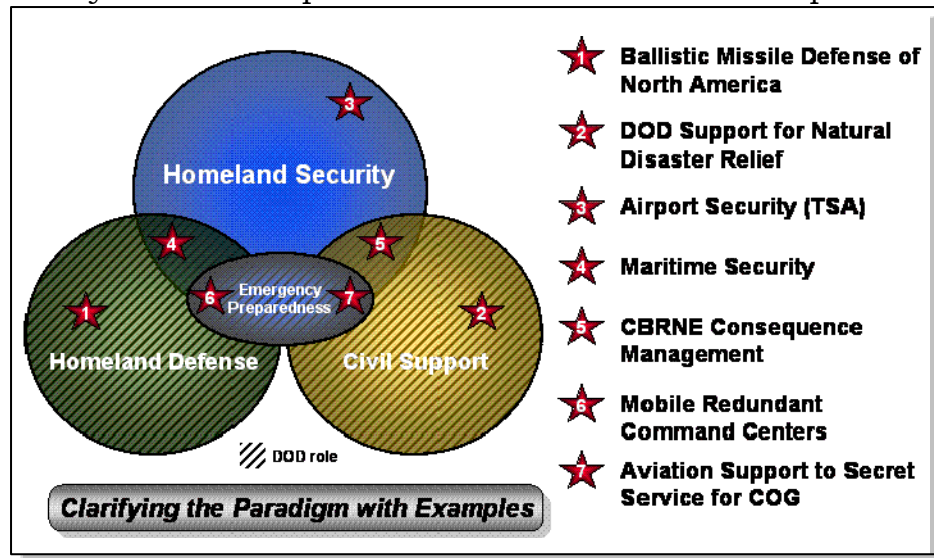
**Figure 1: DOD HD and CS Paradigm**

sustain a global military presence, and honor its global security commitments. The military will continue to play a vital role in securing the Homeland through the execution of HD and CS missions, as well as EP planning activities (as defined in Figure 1 and in Appendix B: Glossary and Acronyms). As shown in Figures 2 and 3, HS is not synonymous with HD, nor are HD, CS, and EP subordinate to HS. On the contrary, although HS, as defined in the NSHS, is concerned solely with preventing and mitigating the effects of terrorist attacks, DOD’s concern cannot be limited to terrorists.

<sup>13</sup> For more detailed information refer to *Executive Order 12656*.

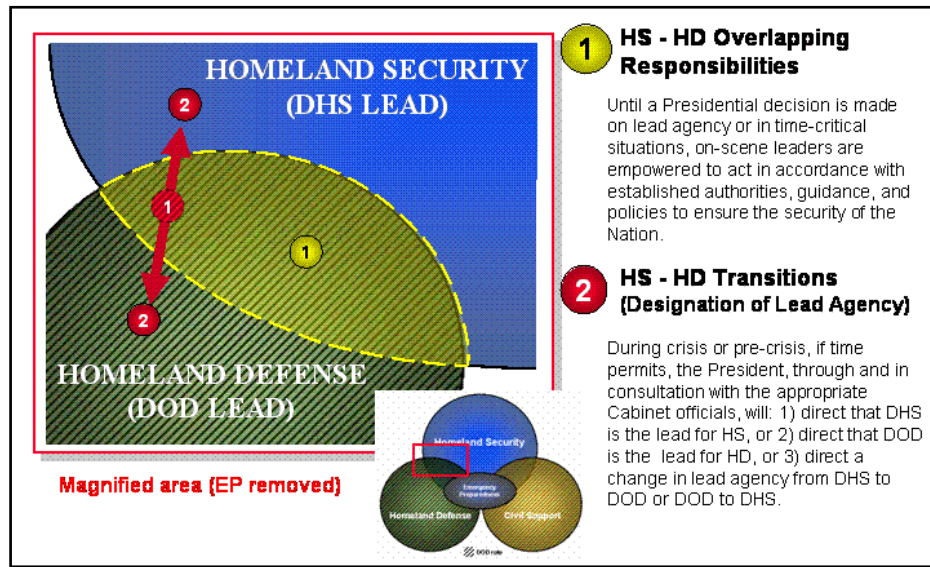
DOD must address both conventional and unconventional attacks by any adversary (including but not strictly limited to terrorists). When DOD conducts military missions as the lead agency to defend the Homeland, this is HD.

DOD has lead responsibility for HD, with other departments and agencies in support of DOD efforts. Circumstances in which DOD supports the broader federal, state, and / or local government efforts, as coordinated by and in cooperation with DHS or other departments or



**Figure 2: Paradigm Examples**

agencies as LFA, are appropriately described as CS. In these cases, DHS (or another LFA) coordinates activities and DOD is prepared to support the plans that are developed. In the same way that some aspects of HD are unrelated to HS, some aspects of DOD’s CS functions are unrelated to terrorism and do not fall under HS, yet DOD can still provide other unique capabilities in support of civilian authorities (for example, support for natural disaster relief). Similarly, as depicted with the examples in Figure 2, some aspects of HS fall outside the purview of DOD. These functions (such as airport security measures enacted by the Transportation Security Administration (TSA)), fall under the lead of DHS (or another LFA).



**Figure 3: Paradigm Overlaps and Transitions**

As shown in Figure 3, determining where a particular scenario or incident falls within this paradigm will be a coordinated effort among appropriate agencies to determine who should lead the effort. This responsibility ultimately rests with the President as Commander in Chief and Chief Executive. In many situations, the answer is unequivocal. In clear cases of foreign aggression and threats to national security, DOD will be the lead and will conduct operations necessary to defeat an attack (including, if applicable, actions taken in anticipatory self-defense to preempt an attack before it takes place) with applicable support from its partners. In cases with clear law enforcement responsibility, DHS, DOJ, or other agencies will coordinate and assume lead responsibility, and DOD may or may not be directed to perform a supporting role. It is also possible for DOD and its partners to coordinate the transition of lead responsibility during a crisis (either on their own or by Presidential direction) to another federal agency or vice versa should changing circumstances warrant (for example, if non-DOD capabilities are unexpectedly exceeded).

Determining LFA responsibility in situations that are neither clearly military nor clearly law enforcement can be a complex challenge, especially in time sensitive situations. In those situations where DOD, DHS, DOJ, or another on-scene agency have the required capabilities but lack formal direction, the on-scene leadership must be empowered to take whatever actions are deemed necessary and appropriate in accordance with pre-established authorities, guidance, and policies to ensure the security of the Homeland.

## 2.c. Assumptions and Trends

The following **assumptions** frame and provide context for the DOD HD and CS JOC:

- ❖ Potential adversaries will benefit from the ongoing proliferation of key technologies such as: tactical, cruise, and ballistic missiles; chemical, biological, radiological, nuclear, or high yield explosives (CBRNE) hazards, including weapons; information operations; and emerging technologies.
- ❖ When appropriate, the United States will act with other nations to provide a multi-national approach to defeating shared threats (for example, participation in coalitions or pursuant to international agreements, such as the North American Aerospace Defense Command (NORAD). However, the United States will maintain a unilateral capability to act militarily to protect vital national interests.
- ❖ Security cooperation arrangements, alliances, and coalitions will continue to enable the United States and its partners to shape the strategic landscape, protect mutual and shared interests, and promote regional stability.
- ❖ DHS will continue to have lead responsibility for the national HS mission and the DOJ will continue to have lead responsibility for counter-terrorism in the Homeland.
- ❖ DHS and other federal, state, local, tribal, and private authorities will continue to enhance and improve their capabilities and their ability to interface and coordinate with DOD on the employment of those capabilities.
- ❖ Improved interagency integration, coordination, policy, and directives among DOD and its non-DOD partners will continue to enhance situational lead responsibility determination at the operational level.

This concept also is based on several evolving **trends** in the strategic environment that have implications for policy, authorities, and responsibilities posed by the “seam” between war and crime as discussed in the National Challenge section of this JOC. These trends form the backdrop against which DOD will operate while conducting operations in the 21st century. Trends include a continued:

- ❖ **Requirement for military power** to protect and advance US global interests and commitments.

- ❖ **Requirement for global space services** (for example, satellite communications and navigation), as well as associated support.
- ❖ **Complex joint force battlespace** that spans the operating areas of multiple combatant commands, extending from the Homeland to critical regions overseas, including the “global commons” of international waters and airspace, space, and cyberspace.
- ❖ **Increase in the use of asymmetric approaches** in lieu of more traditional military means and methods that avoid US strengths and attack US vulnerabilities.
- ❖ **Vigilance and adaptation** to adversary capabilities with a focus on HS by the United States.
- ❖ **Increase in the speed and scale of the proliferation** of missile technology and the spread of CBRNE weapons and their means of delivery, posing a fast-growing challenge to land, maritime, air, cyber, and space capabilities at home and abroad.
- ❖ **Heavy reliance by DOD** on integration, coordination, and synchronization with interagency and multi-national partners.
- ❖ **Re-assessment of the use** of US military forces in domestic situations (e.g., disaster response or border control support).
- ❖ **Requirement for state governor commanded military forces** until mobilized as federal assets by order of the President.
- ❖ **Ability by potential adversaries to have increasing access** to a global commercial, industrial, and information base, providing them with niche capabilities intended to impede or defeat the capabilities or will of the United States.
- ❖ **Adaptation by potential adversaries** as US capabilities evolve and the need for DOD to be postured to contend with this new and uncertain threat for the indefinite future.

### **3.0 MILITARY PROBLEM**

This concept is focused on the military problem of how DOD will fulfill responsibilities of securing the Homeland, including how: 1) DOD detects, deters, prevents, or if necessary, defeats external threats or aggression to the Homeland; 2) DOD will be prepared to respond to catastrophic incidents as appropriate or as directed; and 3) DOD will integrate and operate with its US and international partners to achieve unity of effort for HD and CS.

Detecting, deterring, preventing, or if necessary defeating threats to the Homeland is complicated by America's free and open society. The challenge for DOD, given the diversity and uncertainty of state and non-state actor threats, is detecting and deterring these threats often without a clear understanding of the threat, their goals, or the tactics they may employ. Understanding the threat environment and the challenges of that environment are vital to understanding the military problem facing DOD and the ways that threats can be prevented or if necessary defeated.

In addition to detecting, deterring, preventing, or, if necessary, defeating threats to the Homeland, DOD also must be prepared to provide support to its partners when directed for catastrophic events. The challenge for DOD is to be prepared to fight our Nation's wars while simultaneously being ready to convert some or all of those same capabilities into humanitarian relief efforts when appropriate and when directed.

A national challenge for DOD is integrating and operating with its partners to determine when a particular threat to the Homeland is a national security threat requiring DOD action or a law enforcement threat requiring law enforcement agency action. This situation and others involving DOD HD and CS missions in the Homeland require close cooperation and coordination between DOD and its partners, especially situations where roles and responsibilities overlap and complicate operational planning for DOD.

The problem facing DOD of how to operate in a diverse and uncertain threat environment and the challenges associated with that environment, the national challenge of determining roles and responsibility for particular threats to or events within the Homeland (including natural disasters and catastrophic events), and the challenges associated with how DOD will operate within different environments with its US and international partners to achieve unity of effort are further detailed in the following sub-sections.



### 3.a. Threat Environment

As described in current and previous National strategy documents, the highest priority of the US military is to defend the Nation from national security threats and foreign aggression. Confronting the United States in this pursuit is a dangerous, changing, and uncertain strategic environment that will continue to pose persistent and emerging challenges. Increasing political, economic, ethnic, and religious divisions and extremism; the diffusion of power among hostile state and non-state actors; population growth and a scarcity of natural resources; and the proliferation of dangerous technologies and weaponry are dramatically increasing the potential for threats against the Homeland and US global interests. Persistent and emerging challenges of the future threat environment are categorized in the NDS and NMS as traditional, irregular, catastrophic, or disruptive.

These challenges will tend to overlap in most geopolitical situations. Potential adversaries may employ threat capabilities from more than one category. Adversaries proficient in one category may attempt to reinforce their position by adopting methods and capabilities from other categories. For example, a terrorist group may pose a persistent irregular threat, but also seek catastrophic capabilities. It is this diverse threat environment that will increasingly challenge the security of the Homeland.

**“Our first duty in the war on terror is to protect the Homeland....the best way to prevent attack is to stay on the offense against the enemy overseas”.**

*(President George W. Bush remarks on HS in New Jersey - 18 Oct 04)*

### 3.b. Diverse and Uncertain Threats to the Homeland

Threats to the Homeland will continue to be diverse, adaptive, and in many cases difficult to predict. Potential adversaries will attempt to surprise the United States as they adopt an array of persistent and emerging traditional, irregular, catastrophic, and disruptive methods and capabilities to threaten the Homeland.

The most dangerous circumstance for the United States will be situations where DOD is confronted with multiple challenges simultaneously. The technical advances of hostile state and non-state actors, the proliferation and diffusion of key technologies, and the continued advancement of weapons and delivery systems will provide destructive mechanisms and the ability to deliver them to an increasing number of adversaries who will continue to threaten US territory,

population, and critical infrastructure. These threats – some known and some unknown – fall into three broad categories:

- ❖ Hostile states using traditional means of attack, including missiles, other advanced technologies, and potentially weapons of mass destruction (WMD);
- ❖ Hostile states employing irregular means of attack such as smuggled WMD or cyber attacks; and
- ❖ Terrorist groups and other non-state actors using primarily irregular means of attack, and to a lesser degree traditional means of attack in a range of ways, potentially including the use of WMD.

Threats to the Homeland will not always be from adversarial challenges. Natural catastrophes such as major hurricanes, earthquakes, or pandemics also must be viewed as threats. These situations can have a tremendous adverse effect on the US economy and can require a significant allocation of federal, state, and local resources to mitigate the effects and manage the consequences of the catastrophe as well as providing for recovery and relief efforts.

Intelligence is at the forefront of identifying adversaries and threats against the US. However, since the United States cannot know with complete confidence which nation, combination of nations, or non-state actor(s) will pose a threat in the future, the focus of intelligence, planning, and operations also must be on how a potential adversary **could** threaten the United States – on the destructive mechanism and delivery means – rather than on a specific adversary or adversaries.

Destructive mechanisms of concern include, but are not limited to: nuclear devices, biological agents, chemical agents, radiological dispersion devices, conventional (perhaps enhanced) weapons or improvised explosives, cyber attacks, and the use of civil equipment and facilities as weapons. Each of these has the potential to cause significant psychological and / or physical damage to US territory, population, and critical infrastructure and could be employed by hostile states or non-state actors. Potential delivery systems include but are not limited to: intercontinental ballistic missiles (ICBMs); sea-launched ballistic missiles (SLBMs); cruise missiles, including air-launched cruise missiles (ALCMs), sea-launched cruise missiles (SLCMs), and ground-launched cruise missiles (GLCMs); unmanned and manned aircraft; shoulder-fired weapons; and various ground and sea vehicles. In addition, a weapon could be acquired overseas and smuggled into the Homeland either fully assembled or in pieces; or it could be built within the Homeland and

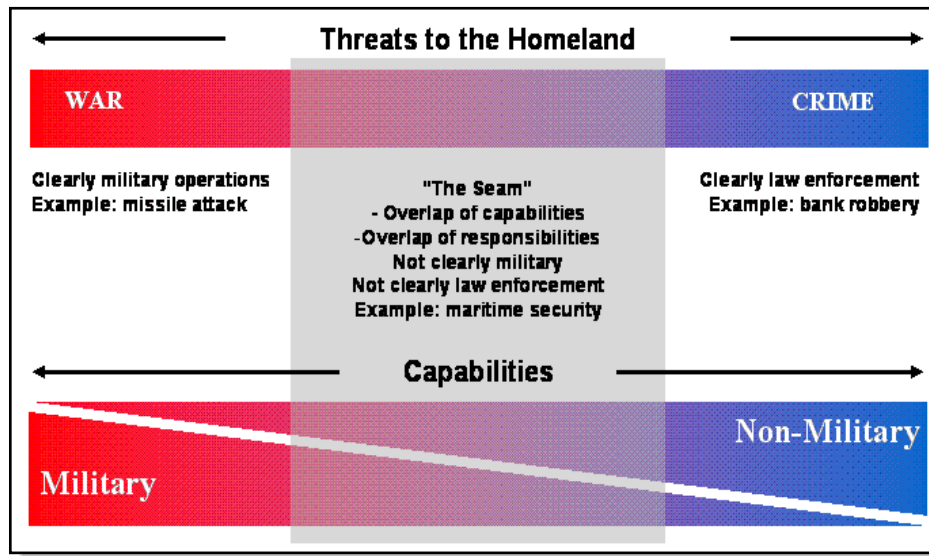


delivered to its target by a variety of methods including any of the means listed above.

Potential adversary objectives include, but are not limited to inflicting large numbers of casualties; destroying significant property; disrupting the US economy; damaging US agriculture; creating psychological shock to reduce public support for specific US policies; and impeding US military deployment, command and control, or other activities. Potential attacks by both hostile states and non-state actors will rely on surprise, deception, and asymmetric warfare and cover the range of activities from acquisition of materiel and know-how to delivery of individual weapons, or coordinated attacks with multiple weapons of the same or different types.

### 3.c. National Challenge

The Homeland is confronted by threats ranging from national security threats (for example, ballistic missile attack) to law enforcement threats (for example, bank robbery) (Figure 4). This is a conceptual spectrum with clear definitions of both ends and less clarity in the



**Figure 4: National Challenge**

middle where the two blend together. In the middle is a “seam” of ambiguity where threats are neither clearly military wartime threats (requiring a military [DOD] response capability) nor clearly criminal type threats (requiring a non-military response capability from DHS, DOJ, or other agency). Within this overlap area are threats such as transnational terrorist groups that challenge the delineation of responsibility between DOD and DHS, DOJ, or other agencies because it is sometimes difficult to label them as either a national security threat or a law enforcement threat.

Determining the best response to a particular threat will depend on circumstances such as the United States Government's (USG) desired outcome for the particular threat, current law, authority to act, magnitude of the threat, response capabilities required, and asset availability. Because of the nature of this threat spectrum, a coordinated, integrated, and coherent national effort will be essential to secure the Homeland. The absence of a clearly defined border between and the overlap of DOD and DHS, DOJ, or other agency capabilities and responsibilities allows latitude in determining which threats are best met by law enforcement and which will require military response.

The NSHS recognizes overlap in military and non-military capabilities by defining HS as a "concerted national effort to prevent terrorist attacks..." where the "concerted national effort" is based on "the principles of shared responsibility and partnership" between various federal, state, and local agencies and with the American people<sup>14</sup>. The overlap of DHS, DOJ, or other federal agencies and DOD's domestic role in the Homeland supports the national strategy by providing the Federal government with military and non-military options to address a specific threat.

The implications of the spectrum of threats between "war" and "crime" will continue to challenge planning efforts for DOD and other agencies to support HD and CS missions. However, on-going efforts to clarify existing and evolving policies, protocols, procedures, statutes, and legal authorities through legislative and / or executive action, and implementation of changes to the same, continue to reduce that challenge and enhance comprehensive and effective planning for DOD and its partners. Even if legislative and executive actions are not complete, DOD must be capable of operating against adversaries in all situations should the President so direct. For example, under existing legislation or the President's constitutional authority, DOD may be directed to take action against any threatened use of a weapon of mass destruction. As the NSS concludes, "To defeat this [terrorist] threat we must make use of every tool in our arsenal - military power, better HD, law enforcement, intelligence, security cooperation, and vigorous efforts to cut off terrorist financing". The national challenge is to use the overlapping responsibilities and capabilities of DOD and its interagency partners effectively to cover and eliminate the seam of uncertainty and provide the President with maximum flexibility to confront adversaries.

---

<sup>14</sup> *National Strategy for Homeland Security* (Government Printing Office, July 2002).

Another aspect of the national challenge is to identify gaps not covered by the overlapping responsibilities and capabilities. This includes gaps in government-wide counter-terrorism or HD and CS integration and / or capabilities.

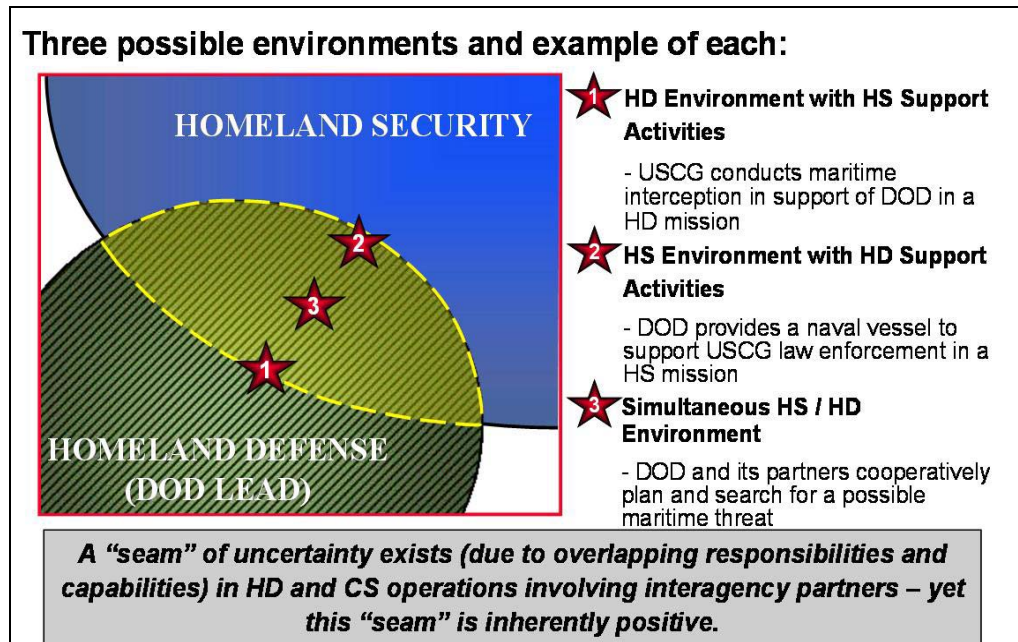
The overlap between military and law enforcement operations complicates planning and execution for DOD in the operational environment. Within the Homeland, DOD must be able to interact at an appropriate level with other government agencies and States and Territories responsible for protecting their citizens. For DOD to operate as an effective military force while performing HD and CS missions or EP planning activities, the role and capabilities of non-federalized National Guard forces must be synchronized and integrated in the overall effort. The National Guard is trained and equipped by DOD and can operate in most traditional DOD missions.

In addition to HD responsibilities, DOD must continue to be prepared to respond quickly and appropriately in the event of overwhelming natural disasters and catastrophic events. DOD contributions may include response, as necessary and appropriate, to both man-made and natural disasters and events.

There is both a challenge and benefit for an operating concept addressing DOD's conduct of HD and CS operations and EP planning in that these activities may occur simultaneously with other efforts to secure the US Homeland. The HD and CS JOC addresses how operations will be conducted in the "seam of uncertainty" between DOD responsibilities and other US and international agencies to transition from an aspect of uncertainty to one of confidence. This "seam of uncertainty" exists (due to overlapping responsibilities and capabilities) in HD and CS operations involving interagency partners – yet this "seam" is inherently positive because it allows National authorities to select the most appropriate response (military or non-military) to achieve the USG's desired outcome.

There are three possible "seam" environments in which DOD may operate; 1) a HD environment with HS support activities; 2) a HS environment with HD support activities; and 3) a simultaneous HS / HD environment. Examples of each are contained in Figure 5.

For each of these environments, DOD and Joint Force Commanders must focus on a clear desired end state for integrating military operations into the broader National Security Campaign context as follows:



**Figure 5: Seam Environments**

- ❖ In the **HD environment with HS support activities** DOD and Joint Force Commanders operate effectively with interagency and international partners at all levels to leverage and integrate non-DOD capabilities in a unified HD effort against threats or hazards.
- ❖ In the **HS environment with HD support activities** DOD and Joint Force Commanders operate effectively with interagency and international partners at all levels to leverage and integrate DOD capabilities in a unified HS effort against threats or hazards.
- ❖ In the **simultaneous HS / HD environment** DOD and Joint Force Commanders operate effectively with interagency and international partners at all levels and synchronize and integrate DOD capabilities in a unified effort until a lead agency is determined through previously-discussed criteria.

The key to effective, successful military operations in all three environments is unified action between DOD and a coalition of interagency and international partners.

## 4.0 SOLUTION

The solution to the military problem described in this JOC is multi-faceted. At the strategic level is an active, layered defense designed to detect, deter, prevent, or, if necessary, defeat threats as far from the Homeland as possible. The solution includes unified action founded on national strategies, 2006 QDR guidance, and CCJO central and supporting ideas required by the Joint Force to accomplish HD and CS missions. Another element of the solution includes development of a NHSP designed to reduce uncertainty by enabling a coordinated national effort in pre-attack national security measures (detect, deter, prevent, or if necessary, defeat external threats<sup>15</sup> and aggression). To reduce uncertainty further, three campaign frameworks linked to three related “seam” environments are presented to illustrate conceptually how DOD may operate with its partners. The final element of the solution is the identification of the desired end state, effects, and at the operational level, Joint Force Commander actions and capabilities. How DOD applies the elements of this multi-faceted solution is essential to unified action between DOD and its partners, especially in the “seam of uncertainty” when roles and responsibilities overlap.

### 4.a. Global, Integrated, Active, and Layered Defense

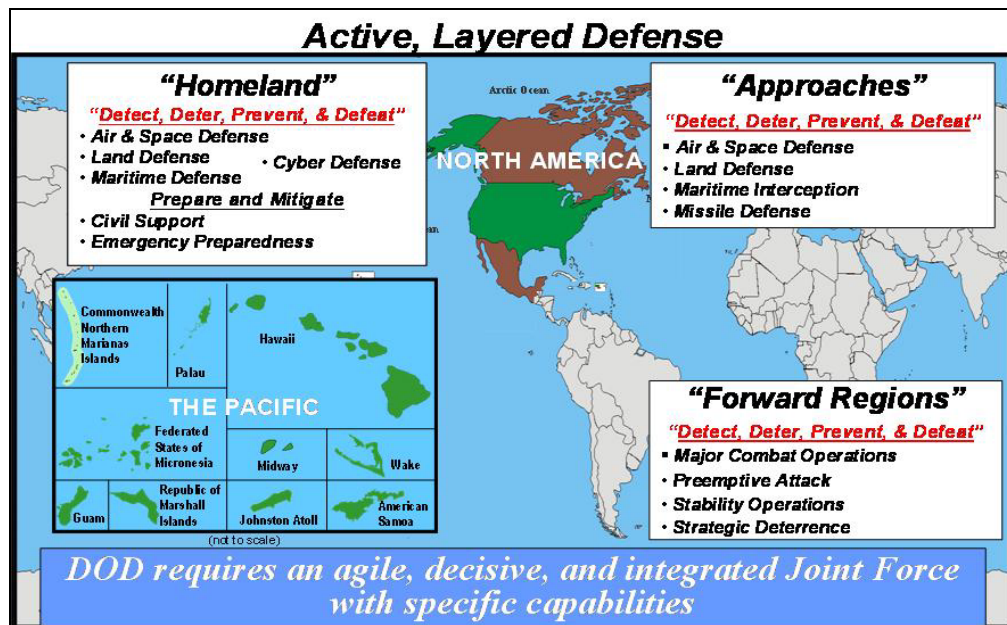
This JOC proposes a solution to the Joint Force Commander’s mission of defending the Homeland against traditional, irregular, disruptive, and catastrophic challenges. It offers a concept for the Joint Force Commander to deny adversary objectives through a global, integrated, active, and layered defense that includes surging capabilities for response to an immediate threat without compromising the defense over time. The overall strategic end state is a secure US homeland, effectively defended from external threats and aggression and capable of managing consequences of attacks by state and non-state actors as well as natural disasters.

**Global** – The interplay of globalization, transnational actors, and the global reach of potential and existing adversaries necessitates a global perspective by Joint Force Commanders. Defense of the

---

<sup>15</sup> As referenced in *Strategy for Homeland Defense and Civil Support* (p. 5), Homeland Defense includes missions such as domestic air defense. DOD recognizes that threats planned or inspired by “external” actors may materialize internally. The reference to “external threats” does not limit where or how attacks could be planned and executed. DOD is prepared to conduct HD missions whenever the President, exercising his constitutional authority as Commander-in-Chief, authorizes military actions.

Homeland involves a global, multi-domain battlespace. Within the context of a global battlespace (Figure 6) the joint operations area (JOA) is a multi-domain space with the Homeland at its core. The JOA expands and contracts in relation to the Joint Force Commander’s ability to acquire and engage the adversary. Since the strategy is to engage adversaries before they gain access to the Homeland, areas of the JOA are often either in the Forward Regions or in the Approaches, or both. The joint area of interest is the multi-domain space beyond the boundary of the JOA that is the source of indirect influence on the Joint Force Commander’s mission.



**Figure 6: DOD Strategic Concept: Active, Layered Defense**

**Integrated** – The Joint Force Commander contributes to unity of effort by taking actions to integrate joint force planning and operations with the full set of HD and CS stakeholders. In the Forward Regions, for example, multiple Joint Force Commanders act in supported and supporting roles to engage adversaries across geographic boundaries. The Joint Force Commander integrates intelligence, surveillance, and reconnaissance (ISR) capabilities with other US government agencies and multi-national partners. In the Homeland, integration efforts shift from multi-national partners to local, state, and federal partners. Managing the transition of responsibilities, particularly within the Approaches, without compromising capability is a critical element of the Joint Force Commander’s operational approach.

**Active** - An active defense includes offensive actions to seize the initiative and dominate the adversary at a spatial and temporal distance. Detect, deter, prevent, or, if necessary, defeat are the operational actions



the Joint Force Commander takes to seize the initiative and dominate adversaries before they gain access to the Homeland. As directed, support actions are taken by the Joint Force Commander to stabilize the environment and enable civil authorities. Five primary lines of operations (based on the actions of detect, deter, prevent, defeat, and support) orient the force in time and space relative to the adversary. They support the synchronization of actions in time and space in order to accomplish the objectives that achieve the overall strategic end state.

The objective of the line of operation associated with the **detect** action is to discover and characterize the intention and capability of an emerging or existing adversary as early as possible. Detection involves discriminating adversaries from legitimate actors and providing assured collection of an elusive target system. Early detection enables the Joint Force Commander to seize the initiative. The objective of the line of operation associated with the **deter** action is to prevent hostile action by imposing costs, denying benefits, and encouraging restraint. The objective of the line of operation associated with the **prevent** action is to preclude the initiation of hostile action against the US through shaping and pre-emptive actions. This objective is achieved primarily by shaping the battlespace to the relative disadvantage of the adversary and taking pre-emptive actions to neutralize adversary capabilities. Prevention constrains adversary actions and removes capabilities while simultaneously assuring allies and partners. The deter and prevent lines are closely linked. They apply similar capabilities in different ways to accomplish the shared objective of stopping hostile action before it is initiated. Should deterrence and prevention fail, the objective of the line of operation associated with the **defeat** action is to dominate the battlespace and the adversary and deny its objectives. The Joint Force denies adversary objectives by destroying capability, undermining the will to attack, blocking access to the Homeland, defeating the enemy strategy, and deception. If the adversary is successful in attacking the Homeland, the objective of the line of operation associated with the **support** action is to enable civil authorities and stabilize the environment while sustaining offensive actions against the adversary. The support line also includes DOD assistance to civil authorities for natural disasters or other activities as directed.

These lines of operations represent the Joint Force Commander's military contribution to unified action and achieving the strategic end state. The objectives and associated operational effects for each are tailored based upon whether the Joint Force Commander is acting in the Forward Regions, Approaches, or the Homeland.

**Layered** - A layered approach arrays defenses in depth so that the Joint Force Commander can trade space for time in order to characterize

and engage the adversary with the most appropriate instrument. Layered defenses provide more options and a greater likelihood of success than non-layered approaches. If the defense fails at one layer, it may succeed at the next. In addition, layered defenses complicate adversary's attack planning and execution and may require adversaries to undertake more complex and visible operations, thereby providing more opportunities to gather intelligence and defeat the threat. The defense in depth entails mutually supporting defense positions designed to absorb and progressively weaken attack, prevent initial observations of the whole position by the enemy, and allow the Joint Force to engage the adversary decisively. Mutually supporting defensive positions exist in multiple domains. Against irregular challenges such as terrorist organizations, key defensive positions are often "manned" by interagency and multi-national partners. The irregular enemy is likely to employ unconventional means to bypass defensive positions (for example, immigration officials) in the Forward Regions, delaying detection by the Joint Force or other HD partners until the enemy is in the Approaches. In these cases, the suspected adversary may be allowed to pass through one or more layers of defenses while characterization is made and appropriate action(s) taken.

Regardless of whether the adversary seeks to penetrate or infiltrate defenses, the Joint Force Commander contributes to the early culmination of the adversary's planning and / or operational tempo. One way to encourage culmination is to generate uncertainty in the adversary's mind by posing access dilemmas in the Approaches, disguising vulnerabilities throughout the JOA, and denying observation of the whole defensive position. Once detection is confirmed, the Joint Force maneuvers in all domains on a global basis in order to engage and defeat the adversary with kinetic and non-kinetic force as necessary and appropriate. Strong points also are incorporated into the defensive array in order to provide an additional layer of defense for US ports, the National Capital Region, Defense Industrial Base (DIB) facilities, and other high-value nodes. Strong points and a responsive infrastructure are essential to continuity of governance and sustaining offensive actions during and after attack. Inherent to the defense is the ability to recover from attack while simultaneously projecting military power. The Joint Force Commander also renders support to civil authorities as directed to mitigate the effects and manage the consequences of catastrophic emergencies.

The central idea of this concept is for DOD to contribute to a national HD / CS system-of-systems that is active and layered. The objective is to deal with threats to the US as early and far forward from the Homeland as possible, and in the event of successful attack or



natural catastrophe, to support an integrated national response that occurs as quickly and effectively as possible.

This central idea has two key supporting ideas. First, HD and CS (including EP) are ***national*** missions to which DOD contributes a perspective with far-reaching consequences for how DOD and others plan, prepare for, and conduct operations. Second, these integrated national HD and CS activities are conducted via an ***active, layered defense*** comprised of a number of overlapping systems-of-systems.

Figure 6, an illustrative depiction of this strategic concept of an active, layered defense, divides the world into three regions and conceptually illustrates DOD missions within each region. A description of the three regions, as well as **how** DOD will conduct operations in each region to ensure an active, layered defense, follows:

- ❖ **Forward Regions** – The Forward Regions are foreign land areas, sovereign airspace, and sovereign waters outside the Homeland. In the Forward Regions, the objective is to detect, deter, prevent, or if necessary defeat threats and aggression against the United States before they can directly threaten the Homeland. This can be achieved through deterrence, security cooperation, preemptive actions (if actionable intelligence is available), major combat operations, and stability operations. DOD will focus its capabilities in the Forward Regions to create an overwhelming first layer of defense and engage emerging threats as far from the Homeland as possible. Military operations in the Forward Regions will require DOD to coordinate, often through established security cooperation programs, with interagency partners and other nations to synergize efforts to protect US interests. Theater security programs are vital to the integrated teamwork required to defeat threats and aggression as far from the Homeland as possible. Military operations will likely occur within the operating areas of multiple combatant commanders and will require coordination among multiple sovereign nations / governments / agencies and militaries in addition to internal DOD coordination.
- ❖ **Approaches** – The Approaches are a conceptual region extending from the limits of the Homeland to the Forward Regions based on situation-specific intelligence. Once intelligence has indicated that a threat is enroute to the Homeland from a foreign point of origin, it is considered to be in the Approaches. Military operations in the Approaches will focus on detecting, deterring, preventing, or, if

necessary, defeating transiting threats as far from the Homeland as possible using the entire DOD portfolio of available capabilities. Military operations focused on active missile, air, and land defenses, as well as maritime interception in the Approaches, in addition to effective surveillance and reconnaissance, will often require DOD to coordinate with other federal agencies and nations, often through established theater security programs, to unify efforts to protect the Homeland.<sup>16</sup>

- ❖ **Homeland** – The Homeland is a physical region that includes the land masses of the Continental United States (CONUS), Alaska, and Hawaii; US territories and possessions in the Caribbean Sea and Pacific Ocean; and the immediate surrounding sovereign waters and airspace. In this region, the DOD objective is to detect, deter, prevent, or ,if necessary, defeat external threats – potentially while simultaneously supporting power projection for decisive military operations in the Approaches and / or Forward Regions. Military operations in the Homeland will usually require DOD to coordinate with local or state governments, other federal agencies, and / or non-government agencies to protect US sovereignty, territory, critical infrastructure and key assets, and domestic population. This requirement to coordinate with interagency partners necessitates enhanced coordination and cooperation initiatives and efforts including forums and organizations such as Joint Interagency Task Forces (JIATFs) and Joint Interagency Coordination Groups (JIACGs), to be fully developed, implemented, and integrated into military commands, organizations, and operations. To achieve HD objectives in the Homeland, DOD will focus on the HD mission sets of Air and Space Defense<sup>17</sup>, Land Defense, Maritime Defense, and Cyber Defense. In addition, to achieve CS and EP objectives, DOD must prepare for, and be able to mitigate the effects and manage the consequences of, catastrophic emergencies, including multiple near-simultaneous CBRNE events, and be prepared to support

---

<sup>16</sup> Definitions for Air Defense and Maritime Interception are included in Appendix B: Glossary and Acronyms.

<sup>17</sup> In accordance with existing agreements NORAD performs air defense of the United States and Canada.

civilian agencies against internal threats or national emergencies if directed by the President.

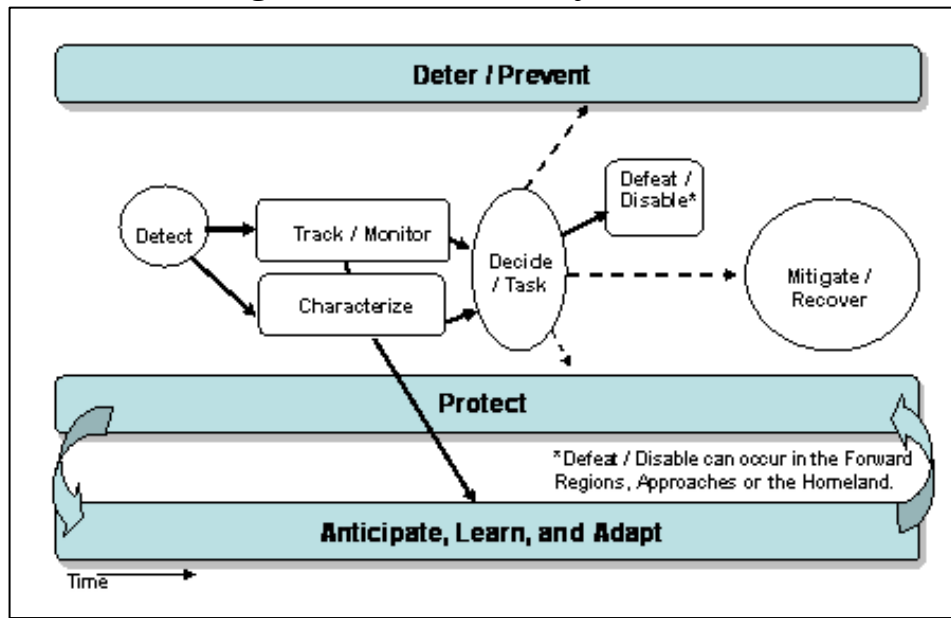
The three regions, as well as the “global commons” of international waters and airspace, space, and cyberspace, define a complex battlespace wherein DOD must maintain superiority through strategic access and control. The boundaries between the three regions, as well as the overarching “global commons”, are not strict and may overlap or change depending on the situation. Additionally, the boundary between the Homeland and the Approaches, America’s **borders**, offers unique challenges for DOD in detecting, deterring, preventing, or, if necessary, defeating threats to the Homeland. This situation requires close cooperation and coordination with neighbors to the north and south of the United States. Regardless of the situation, DOD and its partners will require geographical and functional integration since threats may cross domains or overlap areas of responsibility. The defense must be active, layered, and comprehensive and must encompass the capabilities of DOD, federal, state, and local authorities, and interagency and multi-national partners.

An active, layered defense designed to defeat threats as far from the Homeland as possible requires an adaptive, end-to-end process that operationalizes **how** DOD conducts any HD or CS mission. A generic model<sup>18</sup> depicting such a process is shown in Figure 7. The process applies to any kind of threat, from a conventional attack using military systems, to an irregular or covert attack by non-state adversaries. The specific capabilities required for each of the elements of the process will differ (e.g., detecting a terror plot will require different capabilities from detecting a missile launch), but the overall process is the same. The process model applies both operationally and developmentally. The sequence of activities described in this process can apply to an attack under way with an existing capability, such as inbound missiles, or can apply to a developing threat such as an adversary trying to build a WMD capability.

---

<sup>18</sup> Defense Adaptive Red Team, 16 March 2006.

The process encompasses initial detection through defeat, as well as mitigation / recovery should an attack be successful, or in the case of a large scale natural catastrophe. If an attack is successful, DOD will be responsible for mitigation and recovery of DOD installations and



**Figure 7: End-to-End Process**

personnel, and as directed, will support civil authorities in mitigation and recovery for the rest of the Nation. Although DOD may conduct mitigation and recovery operations at overseas installations and be called on to assist partner nations, for the purposes of this concept mitigation and recovery operations will be conducted in the Homeland. All process actions up to mitigation / recovery are a HD focus for DOD. When directed by the President or the Secretary of Defense, the mitigation / recovery element of the process becomes a CS mission for DOD.

As an example of the end-to-end process, an enemy ICBM launch is detected and tracked; the threat is quickly characterized; a decision is made to neutralize the threat; incoming missiles are destroyed or disabled by anti-missile systems; and local protection and emergency response (mitigation) measures are activated.

#### **4.b. Unity of Effort**

Unity of effort is achieved through agile, integrated intra-US, interagency and multi-national action in order to overcome the seams of uncertainty that challenge the Joint Force Commander’s ability to engage the enemy. **Seams of uncertainty** exist among multiple HD and CS stakeholders in terms of roles, responsibilities, authorities and capabilities. Seams exist: 1) within DOD; 2) within the interagency; 3) within the US among local, state, and federal agencies, as well as with

citizens and the private sector; and 4) between the United States and a wide range of other international actors, including nation-states, inter-governmental organizations (IGOs), and non-governmental organizations (NGOs). Removing seams and / or mitigating their negative effects require national level initiative.

Unity of effort is paramount in how DOD will conduct operations in the “seam of uncertainty”. The Joint Force will apply three strategic principles, as discussed in the NMS, to guide effective operations in the seam. When the principles of agility, decisiveness, and integration are inherently ingrained and integrated in DOD and its partners’ HD, CS, EP, and HS actions, the “seam of uncertainty” between DOD responsibilities and those of other federal, state, and local authorities will be mitigated. Commanders must develop plans that ensure they retain the agility to contend with uncertainty and integrate actions with other government agencies and multi-national partners. Combatant commanders should consider these principles when planning and conducting HD and CS operations.

The principles of agility, decisiveness, and integration fuse US military power with other national and international instruments of power to support simultaneous operations and the application of overmatching power. These principles stress speed, allowing US commanders to exploit an enemy’s vulnerabilities, rapidly seize the initiative, and achieve desired end states. They support the concept of surging capabilities from widely dispersed locations.

These strategic principles can guide the application of military power to protect, prevent, and prevail in ways that contribute to longer-term national goals and objectives. When each of these strategic principles is applied to HD and CS operations, required characteristics and activities of the Joint Force emerge in each strategic principle area as follows:

❖ **Agility**

- This principle is enabled by interagency integration and coordination, communications interoperability, intelligence sharing, integrated operational and training plans, policies, protocols, and procedures for conflict resolution, and entrance and exit strategies for DOD involvement.
- During the course of a HD, CS, or HS operation, lead agency responsibility may change. The timeframe when lead responsibility transitions from one agency to another is especially challenging and requires integration, coordination,

and agility to execute the transition most effectively. DOD policies, procedures, and training should evolve to enable and facilitate continuous and effective operations during this transition.

- During a HD, CS, or HS crisis, potential ambiguity of agency and actor responsibilities requires the effective coordination and use of existing and developing authorities, protocols, plans, and procedures to ensure the ability to recommend and decide appropriate supported-supporting relationships rapidly.
- DOD must proactively collaborate, plan, and otherwise share information with federal, state, and local officials through liaison and interoperable voice and data communications.

❖ **Decisiveness**

- DOD must be prepared to help ensure the security of the Homeland during time-critical situations by rapidly energizing integrated military command, interagency, and international partner linkages to recommend and facilitate decisions.
- During time-critical situations where operations are required to protect the Homeland prior to determination of lead or supporting agencies, DOD and its partners must proceed with situational dependent action as required. DOD and its partners must use existing and developing authorities, policies, protocols, procedures, plans, and training to empower on-scene leaders to take lead responsibility or to provide support to other agencies.
- DOD and its partners must continue to develop, refine, and exercise policies, protocols, plans, procedures, and training to ensure that regardless of which federal agency has responsibility, operations critical to the security of the Nation are coordinated and conducted rapidly, effectively, and achieve the desired outcomes.

❖ **Integration**

- DOD must have the ability to interface directly with interagency partners at the operational level to enhance unified action and must be able to accomplish missions as both a LFA and a supporting federal agency to achieve the desired outcomes.

- These challenging situations require the use of existing and developing authorities, protocols, procedures, plans, capabilities, and training to ensure the ability to communicate and operate effectively with other federal, state, and local agencies. Enablers should include, but not be limited to: interagency integration and coordination, communications interoperability, ability to control operational assets and funding obligations, integrated operational and training plans, entrance and exit criterion, and strategies for DOD involvement.
- DOD must integrate and coordinate policies, procedures, protocols, plans, capabilities, and training that facilitate interagency success, regardless of which federal agency has responsibility. Operations critical to the security of the Nation must be coordinated and conducted rapidly and effectively to achieve the desired outcome.
- DOD must have the ability to engage at the multi-national level through active security cooperation programs to ensure an integrated and active layered defense to detect, deter, prevent, or, if necessary, defeat threats as far from the Homeland as possible.

The three strategic principles guide the Joint Force and facilitate DOD's ability to interface directly with interagency partners to enhance unity of effort and accomplishment of the mission as both lead and supporting federal agency. Agility, decisiveness, and integration in the Joint Force will enable the Joint Force Commander to leverage unified action to reduce and / or mitigate the effects of uncertainty in the "seam" between DOD and other federal, state, and local authorities responsibilities and capabilities.

#### **4.c. Methods to Reduce Uncertainty**

Reducing uncertainty requires use and integration of existing and developing policy and guidance to clarify and codify roles, responsibilities, and an interagency concept of operation between DOD and its partners. A recommended approach is that DOD actively engage its partners using existing and developing policy and guidance to help develop a NHSP similar in concept to the NRP, but addressing detect, deter, prevent, or if necessary defeat versus post-attack roles and responsibilities. Development and implementation of a NHSP would help cover the seam of uncertainty through the integration and coordination of planning, exercising, training, and operations with interagency partners to achieve desired outcomes.

The global war on terrorism (GWOT) requires a greater degree of interagency involvement and coordination than does conventional warfare. A challenge to achieving a wartime footing for DOD in terms of the GWOT is that many of the key “wartime” activities involve coordination and planning with other federal departments and agencies. In Homeland Security Presidential Directive (HSPD)-5, the President directed development of the NRP to align federal coordination structures, capabilities, and resources into a unified, all discipline, and all-hazards approach to domestic incident management. Although preparations and plans for DOD to support civil authorities in the event of an attack are outlined in the NRP, there is no similar overarching national level plan that specifically coordinates the pre-attack actions of the USG.

**“The Defense Department’s capabilities are only one component of a comprehensive national and international effort. Non-military components of this campaign include diplomacy, strategic communications, law enforcement operations and economic sanctions”. (NDS)**

Development of a NHSP that operationalizes the NSS and helps define roles and responsibilities for DOD and its partners would help clarify how operations will be conducted in the “seam” of overlapping responsibilities and capabilities. The NRP and National Incident Management System (NIMS) allow DHS to coordinate authorities, tasks, and procedures for all federal departments and agencies for post attack response measures. A NHSP would enable a coordinated national effort to do the same for pre-attack national security measures to detect, deter, prevent, or, if necessary, defeat external threats and aggression.

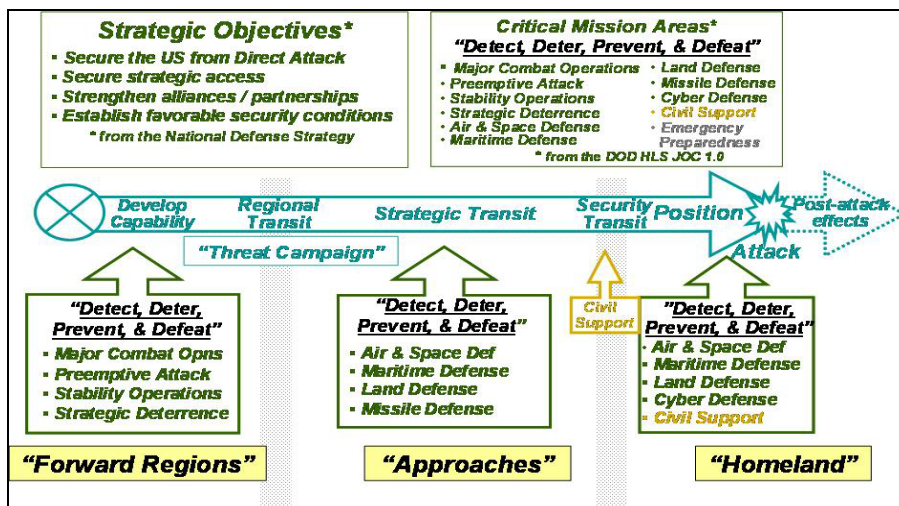
This concept does not specify the details of a NHSP. However, it is likely that in some areas, such as ballistic missile defense, DOD will be the lead and operate more or less autonomously. In other areas, such as maritime defense of the United States, DOD may lead in some geographic areas and functions, while coordinating closely with one or more of the agencies (in this instance the US Coast Guard). In yet other areas, such as the GWOT where the National Counter Terrorism Center is responsible for developing an integrated national strategic-operational plan, DOD will contribute to an integrated national planning effort and may lead in some areas and support in other areas as that plan is implemented.



Three different campaign frameworks<sup>19</sup> are fundamental to the discussion of the NHSP. All three campaign frameworks are founded on the central idea and strategic objective of this concept – dealing with threats to the United States as early and as far forward from the Homeland as possible, and in the event of successful attack or natural catastrophe, to support an integrated national response that occurs as quickly and effectively as possible. DOD plays a vital role in each campaign. The first campaign framework is the “HD and CS Campaign Framework” with DOD missions performed in each of the three regions to produce an active, layered defense of the Homeland. The second campaign framework is the “HS Campaign Framework” wherein DHS, DOJ, or other non-DOD agency is designated as the LFA in conducting HS missions across several critical mission areas. The third campaign framework is the “National Security Campaign Framework” which encompasses the roles, missions, and actions of federal, state and local authorities, and other Government agencies at all levels in addressing threats to the Homeland.

❖ **HD and CS Campaign Framework**

The HD and CS Campaign Framework of an active, layered defense builds upon the NDS strategic objectives and serves to depict conceptually how DOD will accomplish its HD and CS missions, and EP planning activities across the threat spectrum in the Forward Regions,



**Figure 8: HD and CS Campaign Framework**

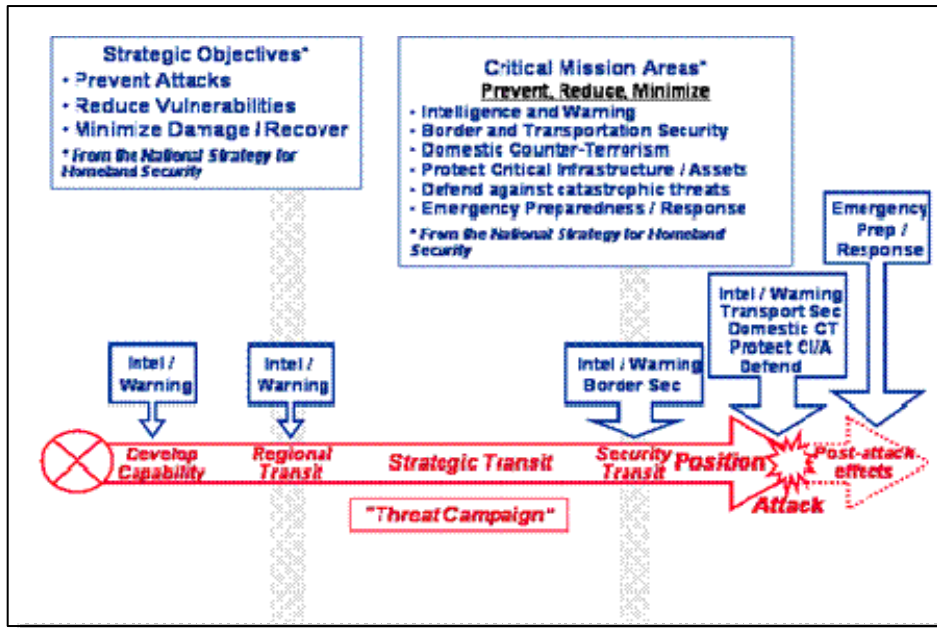
<sup>19</sup> The figures associated with each of the three campaign frameworks are conceptual examples and are not all inclusive of DOD HD and CS actions and the overlap of those actions with non-DOD partners.

Approaches, and the Homeland. This framework (for illustrative purpose only in Figure 8) emphasizes the critical importance of preventing attacks on the Homeland and mitigating and / or managing the consequences of the effects should they occur. To meet this complex challenge, planning and execution of military operations need to be integrated and synchronized within a larger national security strategy construct and conducted in coordination with other government agencies, allies, and international partners in a broader “National Security Campaign”. Integration and synchronization of HD operations and HS activities within the context of the National effort assure maximum and optimum resources against any designated threat.

❖ **HS Campaign Framework**

The purpose of a HS campaign, as expressed in the NSHS, is to mobilize and organize the Nation to secure the US Homeland from terrorist attacks. The NSHS establishes a foundation upon which to organize HS efforts and delineates the strategic objectives of HS as (in order of priority):

- Prevent terrorist attacks within the United States;
- Reduce America’s vulnerability to terrorism; and
- Minimize damage and recover from attacks that do occur



**Figure 9: HS Campaign Framework**

The NSHS also aligns and focuses HS functions into six critical mission areas: intelligence and warning, border and transportation security, domestic counter-terrorism, protecting critical infrastructure, defending against catastrophic threats, and emergency preparedness and response. The first three mission areas focus primarily on preventing terrorist attacks; the next two on reducing the Nation’s vulnerabilities; and the final one on minimizing the damage and recovering from attacks that do occur. In this way, the NSHS provides a conceptual HS campaign framework to align the resources directly to the task of securing the Homeland.

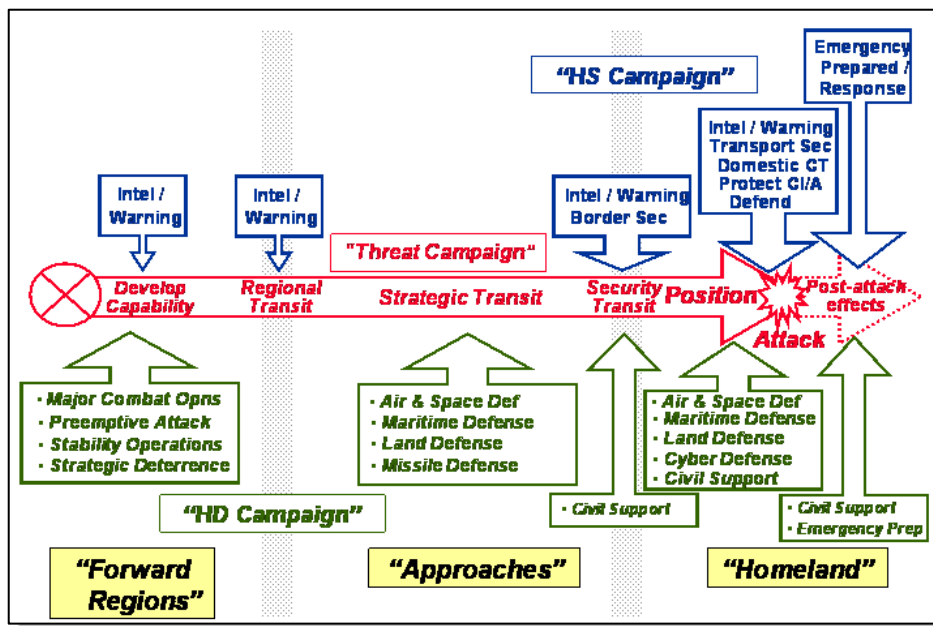
Figure 9 displays, in general terms, a HS Campaign Framework based on the strategic objectives and the critical mission areas defined in the NSHS and imposed upon a generic threat campaign. The critical mission areas are conceptually aligned with the major threat events (threat capability development through post - attack effects). This campaign framework applies when DHS, DOJ, or another non-DOD agency is the designated LFA. Although not the LFA in this campaign, DOD must maintain cognizance of the situation and leverage critical situational intelligence / warning.

❖ **National Security Campaign Framework**

As addressed in the National Challenge section, threats such as transnational terrorist groups challenge the delineation of responsibility between DOD and DHS, DOJ, or other agencies because it is difficult to label them as either a national security threat or a law enforcement

threat. Determining whether a particular threat is one or the other will depend on circumstances such as current law, authority to act, magnitude of the threat, response capabilities required, and asset availability. A coordinated, integrated, and coherent national effort will be essential to secure the Homeland against all threats. The absence of a clearly defined border between and the overlap of DOD and DHS, DOJ, or other agency capabilities and responsibilities allows latitude in determining which threats are best met by law enforcement and which will require military response, and conceptually substantiates the importance of a National Security Campaign Framework.

Figure 10 illustrates how both DOD and non-DOD campaigns would work together to establish unified action against common threats and hazards in the Forward Regions, the Approaches, and the Homeland.



**Figure 10: National Security Campaign Framework**

For DOD conducting HD and CS operations, the strategic and operational context of integrated planning and conducting missions inside a broader National Security Campaign in coordination with US and international partners has significant implications. The first is the acknowledgement of other actors conducting parallel efforts to protect the United States and the challenges and opportunities this national security partnership presents. The main challenge is coordinating and integrating, through formal and informal agreements, the activities of multiple federal, state, and local actors involved and operating in the same battlespace. Because the structure of the government makes unity of command impractical with this coalition of actors, coordination must be accomplished at all levels through formal and informal agreements.

However, this spectrum of actors and capabilities also presents the opportunity for DOD and the Joint Force Commander to leverage cooperation to increase situational awareness, mitigate capability gaps in the Joint Force, and synchronize a more effective response to emerging threats. Interoperability and interagency coordination are key considerations in maximizing these opportunities.

#### **4.d. Desired End State, Effects, and Required Capabilities**

To further define “how” DOD will integrate and conduct HD and CS operations to ensure an active, layered defense, as well as unified action with its partners, the desired end state has been defined, effects identified, and operational-level capabilities required by future Joint Forces listed. These capabilities, closely linked to the strategic objectives and core capabilities in the Strategy for Homeland Defense and Civil Support and the Joint Capability Areas (JCAs), identify and discuss how DOD must be able to integrate effectively with non-DOD partners in order to detect, deter, prevent, or, if necessary, defeat potential threats to the Homeland, or to mitigate the effects of attacks that do occur. The association of desired end state, objectives, and effects to the JCAs is detailed in Appendix C. The operational-level required capabilities associated with HD (detect, deter, prevent, or, if necessary, defeat) are a higher priority for DOD than those associated with CS. The desired end state, effects, and minimum essential operational-level capabilities required to implement the strategic concept include:

### **Desired End State**

**A secure US Homeland, effectively defended from external threats and aggression, and capable of managing consequences of attacks by state and non-state actors, as well as natural disasters.**

#### **Effects:**

- Globally projected and positioned forces capable of conducting decisive Joint operations.
  - Rapid and effective deployment, employment, and sustainment of Joint Forces from multiple locations.

**Required Capability:** Project power to defend the Homeland.

DOD must have the ability to project expeditionary Joint Forces and conduct joint decisive operations globally. To be able to detect, deter, prevent, or, if necessary, defeat threats in the Approaches and / or in the Forward Regions before they reach the

Homeland, DOD must be able to deploy and sustain forces in and from multiple dispersed locations rapidly and effectively to respond to crises, to contribute to deterrence, and to enhance regional stability. Projecting US military power globally and conducting effective theater-level military operations (including major combat or stability operations) are essential contributors to HD because they are visible deterrents to potential adversaries and reduce instability that can incite potential adversaries to act. In addition, forward postured (forward based and forward deployed) forces can be made available to conduct preemptive or interception operations rapidly. The United States must leverage its advantages beyond the scope of forward deployments to assure a responsive, executable, and credible power projection capability. This capability includes US strike options (kinetic and non-kinetic) and space capabilities. These assets amplify US deterrence and provide the options and lethality necessary to deal with potential adversaries. This capability is closely tied to deterrence, as well as major combat and military support to stabilization, security, transition and reconstruction operations.

*(This capability also is addressed by the Forward Presence discussion in the Deterrence Operations JOC and in the Focused Logistics JFC)*

**Effects:**

- A US Homeland secure from external threats and aggression through integrated detection, deterrence, prevention or, if necessary, defeat of attacks in the Forward Regions and the Approaches before they become a threat to the Homeland.
  - Enhanced integration, coordination, shared information, knowledge, and teamwork among US and multi-national agencies on known or suspected threat countries, organizations, and individuals through in-depth and effective theater security cooperation programs.
  - Preemptive action, if required, ranging in size and complexity from a single strike to major combat operations.

**Required Capability:** Detect, deter, prevent (including through preemptive action), or, if necessary, defeat potential threats to the Homeland as they arise in the Forward Regions and / or Approaches.

Sharing of information, knowledge, and teamwork with international partners through theater security cooperation programs will further detection, deterrence, prevention, or if necessary, defeat of threats within the Forward Regions and / or

Approaches. However, the ability to conduct preemptive actions (which can range in size and complexity from a single strike to major combat operations) also must be a viable option for senior decision makers. These strikes could include targeting key development nodes, command and control systems or processes, or the weapon system itself at any point during the development and preparation process before an attack on the Homeland is actually initiated. Illustrative preemptive actions include a strike in the Forward Regions to prevent ballistic missile launch by destroying the delivery systems and / or infrastructure prior to launch or destroying adversary aircraft before takeoff. US military presence in the Forward Regions and / or Approaches, enhanced through information sharing on known or suspected threat countries, organizations, and individuals, also will continue to serve as a deterrent to potential attacks on the Homeland. Detecting, deterring, and preventing attacks before they can be set in motion, or defeating them once initiated is the best way to ensure a secure US Homeland.

*(This capability is also addressed in the Deterrence Operations JOC and the Global Strike JIC)*

**Effects:**

- A US Homeland secure from space attack through space superiority.
  - Negation of adversary space threats and support infrastructure through deception, disruption, denial, degradation, and if necessary destruction.
  - Maintaining and leveraging superiority in global space operations.

**Required Capability:** Detect, deter, prevent, or, if necessary, defeat hostile space systems threatening the Homeland.

In the decades ahead, an increasing number of countries will gain access to space capabilities as a means to upgrade and enable their military applications. As such, the United States must maintain its superiority in space operations, including defense of US space systems. The United States must also be prepared to address and mitigate the threat posed by an adversary's orbital assets, including through preemptive actions if the situation is a direct threat to the safety of the Homeland. Space defense should focus on detecting, identifying, tracking, and preventing / negating adversary space systems supporting attacks on the Homeland. This includes the ability to conduct space negation, whereby adversary space systems are deceived, disrupted, denied,

degraded, and / or destroyed (including attacks against ground-based support and launch infrastructures in the Forward Regions and / or Approaches, possibly in coordination with related or unrelated ongoing military combat operations).

**Effects:**

- A US Homeland secure from ballistic missile attack.
  - Enemy missiles detected, deterred, prevented, or, if necessary, destroyed.
  - Enemy missiles detected and prevented from launching.

**Required Capability:** Detect, deter, prevent, or, if necessary, defeat ballistic missile threats to the Homeland.

The objective of missile defense will remain the protection of the US Homeland, our friends and allies, and US deployed forces. This will be accomplished by a combination of; (a) time sensitive and accurate ISR of ballistic missile threat activities; (b) Joint Force preemptive actions aimed at detecting and preventing imminent missile attacks prior to launch by destroying the delivery systems and disabling associated infrastructure, including command and control (C2) nodes before they can be employed (in the Forward Regions); (c) regionally oriented defenses in the Forward Regions and the Approaches that protect deployed forces (a force protection responsibility); and, (d) a US homeland missile defense system effectively integrated with theater missile defense assets to provide overlapping fields of fire and defense in depth. Dependent on timely, reliable, and accurate early warning information, this capability must provide an active, layered defense that allows multiple engagement opportunities throughout the boost, midcourse, and terminal phases of a missile's flight to negate or defeat an attack as far from the Homeland as possible. Coupled with US force projection, global strike, and nuclear capabilities, missile defense not only provides an active defense against the threat of ballistic missiles, it also strengthens the overall US deterrent posture.

*(This capability also is discussed in the Deterrence Operations JOC and the Integrated Air & Missile Defense JIC)*

**Effects:**

- A secure US Homeland through a secure global maritime domain.
  - Unrestricted freedom of movement, access, and basing within the maritime domain for Joint Force deployment and power projection.



- Domination of oceans and littoral, coastal, and internal waters, as required.
- Enhanced cooperation with US strategic and emerging partners.
- Increased capacity of maritime forces of US strategic and emerging partners.
- Unrestricted freedom of action to conduct maritime commerce and authorized civilian access.
- Reduced vulnerability of the maritime domain to hostile exploitation and / or hostile acts.
- Early detection and interception of maritime threats in the maritime domain as far from the Homeland as possible.

**Required Capability:** Detect, deter, prevent, or, if necessary, defeat maritime threats to the Homeland.

Maritime security must be an integrated and coordinated effort among interagency, international, and domestic partners beginning in the Forward Regions and transitioning through the Approaches to the Homeland. Additionally, the integration, coordination, and interoperability with federal, state, and local law enforcement agencies (particularly the US Coast Guard) are important in this effort due to their regulatory and law enforcement roles, which overlap significantly in the maritime environment with DOD's national security responsibilities.

The United States must use the full range of its operational assets and capabilities to prevent the Maritime Domain<sup>20</sup> from being exploited and used by terrorists and criminals for hostile acts against the US Homeland and its interests. This prevention is a complex task critical to differentiating maritime threats from valid maritime commerce and its positive financial effect. Increased awareness of the global maritime domain enables understanding and action, which will be required to provide an active, layered defense from the Forward Regions to the Homeland. DOD must work closely with interagency and international partners to establish a unified concept for maritime domain awareness (MDA)

---

<sup>20</sup> As defined in *National Security Presidential Directive (NSPD) 41*, "Maritime Domain" means all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances.

and operational threat response. DOD must have the ability to detect, sort, track, evaluate, intercept, and, if necessary, disrupt and defeat any maritime threat. Any operational response must be integrated and coordinated with the appropriate interagency partners to ensure unified action and desired outcome. DOD must have the capability to defend against developing surface and sub-surface vessels, including future threats armed with cruise and theater ballistic missiles. DOD also must defend against continued proliferation of WMD threats via maritime vessels. DOD must maintain forward presence capabilities to increase maritime domain awareness and maritime international partner cooperation, ensure unrestricted freedom of movement, access, basing and power projection for the Joint Force, and enable the ability to shape the environment proactively, and deter, disrupt, and defeat terrorist networks.

**Effects:**

- A Secure US homeland through early detection, prevention, or, if necessary, defeat of airborne threats.
  - Effective surveillance and acquisition of air threats in the Homeland and Approaches regardless of size, speed, or altitude.
  - Uninhibited authorized commercial and civilian Homeland airspace access.

**Required Capability:** Detect, deter, prevent, or, if necessary, defeat airborne threats to the Homeland.

Protecting and maintaining national air sovereignty while concurrently ensuring maximum airspace for commercial and civilian activities are essential to keeping the Homeland safe. Protection begins with actionable intelligence to detect and negate threats before they become airborne. Once airborne, detection of threats is complicated, and such threats may not be easily differentiated from benign air activity. Additionally, weapon proliferation and increased access to key technologies have presented US enemies with asymmetric strike options that will continue to mature in the decades ahead. Cruise missiles, unmanned aerial vehicles / aircraft systems (UAV / UAS), man-portable air defense systems (MANPADS), and independent aircraft represent significant hazards to the Homeland. DOD must have the ability to detect and prevent these and other airborne threats early using all means available (including low altitude surveillance and over-the-horizon acquisition) to determine intent and provide sufficient warning to defeat them before they reach their intended target. This is a complex challenge due to significant overlap

between national security and law enforcement that will require close cooperation, coordination, interoperability, collaboration, and a net-centric approach between DOD and its interagency and international partners.

**Effects:**

- A secure US homeland through early detection and prevention of land threats and attacks.
  - Effective DOD, interagency, and international collaboration and cooperation in detecting, deterring, preventing, or, if necessary, defeating any adversary threatening the Homeland.
  - Established DOD and interagency partner policies and procedures for land defense and protection of the Homeland.

**Required Capability:** Detect, deter, prevent, or, if necessary, defeat land threats to the Homeland.

The future Joint Force must be able to conduct large-scale and sustained military operations throughout the global battlespace, including land defense of the Homeland if required. Protecting the Homeland from national security threats and foreign aggression in the land domain is the foremost responsibility and highest priority of the US Armed Forces. While the likelihood of a land invasion of the Homeland will continue to be remote, the United States must have the ability to counter a range of possibilities – from conventionally equipped militaries to small, elusive adversaries able to employ the most sophisticated technologies. The Joint Force requires the capability to help defend bases, installations, critical infrastructure, national borders, and US sovereignty against national security threats as directed by the President. This capability must provide the ability to detect and prevent threats early, determine intent of threats, and provide sufficient warning to defeat threats before they reach their intended target. This is a complex challenge due to the significant overlap between national security and law enforcement that will require close cooperation, coordination, interoperability, and collaboration between DOD and other federal, state, and local agencies and between the United States and its international partners. This overlap, as discussed in National and DOD strategies, requires a three-tiered response to land threats: local, state, and federal.

Short of a Presidential directed DOD response to an invasion of the Homeland, the land defense mission remains an inherent protection and law enforcement responsibility of DOD's interagency partners. However, if a land threat exceeds local, state, and non-

DOD federal capabilities, the President may direct DOD to take the lead to counter the threat. The President has broad constitutional authority as Commander in Chief to use the Armed Forces to defeat national security threats. The Posse Comitatus Act<sup>21</sup> does not limit the President's authority in this regard. DOD also must be prepared to support other federal agencies in a CS role when approved by the Secretary of Defense based upon the principles of cooperation, partnership, the rule of law, and civilian control of the military. Military involvement will be part of a synchronized strategic approach involving federal, state, local, and sometimes private resources, as directed, to defeat or otherwise respond to any threat to the Homeland.

**Effects:**

- A secure physical and cyber environment for DOD assets in the Homeland.
  - Effective and comprehensive critical defense infrastructure vulnerability assessments.
  - Successful detection, accurate identification, and timely response to physical and cyber threats.
  - Established DOD and interagency policies, procedures, and doctrine for physical and cyber security.

**Required Capability:** Detect, deter, prevent, or, if necessary, defeat physical and cyber threats to DOD assets in the Homeland.

Protecting defense critical infrastructure and assets is vital to DOD's ability to project power, conduct traditional and special military operations, and secure the Homeland. Reliance on multi-national global network capabilities will be essential to ensuring physical and cyber security across the global battlespace, especially in the US Homeland. Although some aspects of this capability will take place during operations, the majority of the actions necessary to achieve this capability must be taken prior to the commencement of operations. To achieve this capability, the Joint Force must determine what infrastructure is critical to the completion of its missions; systematically and comprehensively assess those infrastructures to identify vulnerabilities affecting them; implement physical and electronic barriers, security protocols, and other measures as appropriate to remediate

---

<sup>21</sup> Refer to the 1878 *Posse Comitatus Act*; United States federal law (18 U.S.C. § 1385) for more information.

vulnerabilities; prepare fully coordinated plans to mitigate the effects of specific threats against these critical infrastructures; detect the emergence of threats against these critical infrastructures; and develop and implement consequence management (CM) plans and procedures necessary to preserve mission essential functions supported and enabled by these critical infrastructures. Because an effective infrastructure is crucial to modern warfighting, this capability is intrinsically linked to deterrence, as well as major combat and military support to stabilization, security, transition and reconstruction operations.

*(The capability to protect DOD installations is also discussed in the Protection JFC)*

**Effects:**

- A secure DIB<sup>22</sup> for the Homeland.
  - Clear identification of what constitutes the DIB.
  - Effective and timely identification of attack precursors.
  - Current and accurate critical infrastructure and key resource risk assessments.
  - Established DOD, interagency, and state and local partner policies and procedures for DIB protection.
  - Unified action across multiple tiers in the infrastructure protection framework.

**Required Capability:** Collaborate with other federal, state, and local agencies; conduct or facilitate vulnerability assessments; and encourage risk management strategies to protect against and mitigate the effects of attacks against the DIB.

Exploitation or destruction of the DIB could have a catastrophic effect on not only the Nation's economy and morale, but also on DOD's ability to complete its assigned warfighting missions. DOD must have the capability to work with all relevant federal, state, and local agencies to identify, prioritize, and coordinate the protection of all DIB critical infrastructure and key resources. This unity of effort requires decision superiority to execute necessary

---

<sup>22</sup> Defense Industrial Base is defined in the June 2005 *Strategy for Homeland Defense and Civil Support* (page 18) as "...a world-wide industrial complex, with capabilities to perform research and development and design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements."

protection functions proactively. DOD and its interagency partners must develop vulnerability assessments and risk management strategies designed to prevent and if necessary, reduce the consequences of failures, whether caused by terrorist or non-terrorist acts / events. Sharing information about physical and cyber threats, coupled with direct collaboration between DOD and its interagency partners, will enable mutual understanding and identification of indicators and precursors of an attack and allow for preventive measures to be taken to preserve operational readiness. This capability is intrinsically linked to deterrence, major combat, and military support to stabilization, security, transition, and reconstruction operations.

**Effects:**

- A secure US Homeland enhanced through viable and effective Strategic Communication.
  - DOD is able to convince potential adversaries that courses of action that threaten US national interests will result in undesirable outcomes.
  - DOD is able to convince potential adversaries that the US can deny any benefits to adversaries who attack the Homeland.

**Required Capability:** Support USG Strategic Communication to dissuade and deter adversaries from attacking the Homeland.

Effective deterrence requires capabilities that can deny adversary benefits, impose costs on the adversary, or encourage adversary restraint. Strategic Communication is focused USG processes and efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable to advance national interests and objectives through the use of coordinated information, themes, plans, programs, and actions synchronized with other elements of national power. DOD requires the capability to enable a fully synchronized and coordinated global strategic communication campaign to dissuade and deter adversaries and to inform and influence other desired audiences. DOD will keep the American public apprised of HD and CS actions by its contribution to the USG Strategic Communication campaign through Information Operations related capabilities of public affairs (PA), civil military operations (CMO), and defense support to public diplomacy.

*(This capability is also discussed in the Deterrence Operations JOC and the Force Application JFC)*

**Effects:**

- Rapid and effective mitigation of any CBRNE event.
  - Enhanced and standardized CBRNE training programs and efforts between DOD and its partners.
  - Adequate DOD forces trained, postured, and equipped for CBRNE missions.

**Required Capability:** Prepare for and mitigate the effects of multiple, near-simultaneous CBRNE events.<sup>23</sup>

One of the most severe threats facing the Homeland is the threat of CBRNE attacks or emergencies. These events present not only an extreme danger to the US population, but also could adversely affect the ability of the Joint Force to project power from the Homeland, and ultimately, degrade the Joint Force's capacity to prevent or manage follow-on attacks. DOD will require capabilities and forces uniquely qualified and trained for CBRNE defense and CM events. These forces must be prepared to support DOD requirements on DOD bases and installations, as well as local, state, and federal agencies overwhelmed in an emergency. Warfighting forces with dual capability for CBRNE defense and domestic CBRNE CM operations must be identified, trained, equipped, and exercised as necessary to assist civil authorities. This capability must include forces and assets able to provide agent detection and assessment, agent containment, quarantine, evacuation, force protection, decontamination, medical operations in a contaminated environment, and medical surge capabilities (including mortuary affairs). These forces and assets must be available in a timely and reliable manner and must be able to deploy rapidly and sustain themselves (potentially in an austere or contaminated environment).

*(The capability to mitigate the effects of CBRNE events is also discussed in the Protection JFC)*

**Effects:**

- A secure US Homeland through timely and efficient conduct of HD and CS missions, and EP planning activities in all situations.

---

<sup>23</sup> This capability is inherently linked to capabilities relevant for force protection in major combat or military support to stabilization, security, transition, and reconstruction operations (decontamination or protective gear, for example) that could be employed by Joint Forces wherever they are required.

- Proactive and integrated interagency partner relationships and linkages.
- Effective policies, procedures, and authorities for DOD to operate with non-DOD agencies.
- Enhanced unified action between DOD and interagency partners at the operational level providing rapid responses to HD and CS missions, and EP planning activities.

**Required Capability:** Conduct HD and CS operations, and EP planning activities while operating as the LFA, providing support to another agency, and during transitions of responsibility.

Providing robust and rapid response in coordination with other federal, state, and local agencies is a critical aspect of DOD's ability to provide security to the Homeland. DOD must have the ability to interface directly with interagency partners at the operational level to enhance unified action and must be able to accomplish this mission as both a LFA and a supporting federal agency. DOD must work with its interagency partners to develop the policies, processes, and procedures to ensure that, regardless of which organization has responsibility, operations critical to the security of the Homeland are conducted rapidly, correctly, and in the best interests of the Nation. DOD must be able to respond in a supporting or, as directed, in a supported role. DOD also must be prepared to respond quickly and appropriately in the event of overwhelming natural disasters and catastrophic events, like major hurricanes, floods, and earthquakes.

Interagency synchronization requires proactive / dedicated assets designed to improve communications, interoperability, and liaison through collaborative, rapid crisis planning and intelligence sharing down to and including state and local level to support the appropriate officials in their process of designating lead agency responsibilities. This capability will enhance DOD response times during a crisis and improve multi-agency coordination for HD and CS operations, as well as EP planning activities.

During the course of a HD or CS operation or EP planning activity, lead agency responsibility may change. The period when lead responsibility transitions from one agency to another is especially challenging. Policies and procedures should enable and facilitate continuous and effective operations during this transition. DOD also must ensure DOD HD, CS, and EP capabilities can function during this transition of operational lead agency.



## 5.0 RISKS AND MITIGATION

**5.a. Risks** that could invalidate this concept include:

- ❖ Any significant change in the role or use of the military in America between now and 2012 – 2025 could alter the paradigm by which DOD acts in a lead role for HD and in a supporting role for CS. It also could affect the legal framework (such as the Posse Comitatus Act) that governs DOD support (assessed as low risk).
- ❖ The emergence of a hostile global peer competitor, though unlikely within the specified timeframe, could represent a significant challenge to US freedom of action and the ability to project power overseas, as well as encourage a significant reprioritization of US national security objectives and defense resources (assessed as low risk).
- ❖ Increasing US military transformation and enhanced capabilities could outpace coalition partner efforts resulting in an increasing gap between the way the US military operates and addresses the GWOT and the way even our closest allies operate. This gap could adversely affect the end state or strategic objective of this concept, securing the Homeland from external threats and aggression (assessed as medium risk).

**5.b. Mitigation** of risks to this JOC is accomplished through enablers that span across all capabilities identified in this JOC as follows:

- ❖ Ensure collaborative DOD, interagency, and multi-national partner unified action against threats to the Homeland. This effort should include proactive and participatory planning designed to reduce response times, especially during CM operations. Develop integrated training and exercise programs, communications interoperability, information sharing, and policies / procedures on entrance and exit strategies for DOD involvement.
- ❖ Develop and maintain situational awareness and shared understanding throughout the HD / CS / EP environments.
- ❖ Develop, manage, and employ a robust, secure, distributed, collaborative, and interoperable net-centric operational process.
- ❖ Apply force selectively and precisely to achieve the desired effect wherever and whenever required using the full portfolio of available capabilities.

- ❖ Provide protection for DOD forces, assets, installations, and critical DIB infrastructure.
- ❖ Ensure the delivery of equipment, supplies, and personnel in the right quantities, to the right place, at the right time to support HD, CS, and EP objectives.
- ❖ Develop and acquire transformational technologies through a streamlined cycle for capabilities-based acquisitions.
- ❖ Provide in-depth and sustained training for DOD personnel in all HS related activities.
- ❖ Improve DOD capabilities through sharing of expertise and relevant technology, as appropriate, across military and civilian boundaries.
- ❖ Apply results of Joint experimentation and exercises, as appropriate, with DOD and its partners.

## **6.0 IMPLICATIONS**

HD, CS, and EP are by nature Joint endeavors. No individual Military Department has or will have sufficient resources to fulfill DOD's responsibilities in these areas unilaterally. Consequently, future Joint Force Commanders will require the implementation of a joint construct that provides for subordinate command relationships on a permanent (for example, Standing Joint Force Headquarters (SJFHQ)) and / or temporary (for example, Joint Force Headquarters (JFHQ) / Joint Task Force (JTF)) basis. In addition, to command and control integrated operations of air, land, maritime, and information capabilities effectively, the Joint command and control construct should consider all aspects of the Total Force; active and reserve military, civilian, and contractor support. As a result, changes in Joint concepts, policies, authorities, organizations, and technology may be required to synchronize and integrate efforts of the DOD community with respect to HD and CS operations.

DOD must remain committed to working with its interagency partners. Accordingly, DOD must enhance its secure and non-secure connectivity and interoperability within the interagency organizations involved in HS, particularly DHS and DOJ, to provide a robust and active defense-in-depth. DOD should ensure that the determination and refinement of military force requirements and capabilities necessary to meet HD, CS, and EP responsibilities are congruent with the efforts of the other interagency entities while ensuring its full mission readiness. DOD also must actively seek to enable the readiness of its interagency partners by sharing expertise and relevant technology as appropriate.

Common education and training programs between interagency partners and DOD will improve coordination for HS and HD / CS missions and operations, as well as EP activities.

Problematic international strategic trends, including the proliferation of dangerous technologies and weaponry, exponentially increase the range of potential threats confronting the Homeland. As a result, the US military cannot limit HD activities to the Homeland; rather, DOD efforts should be based on an active, layered, and comprehensive spatial strategy that extends beyond the Approaches and to the Forward Regions (as depicted in Figure 6, Strategic Concept: An Active, Layered Defense). To implement this strategy successfully, DOD should vigorously pursue theater security cooperation activities and continue to place appropriate emphasis upon international security and strategic basing agreements, alliances, coalitions, and bilateral arrangements that serve collective interests and demonstrate a commitment to HS and HD / CS. Additionally, DOD must strive to capitalize on and enable contributions of its foreign partners, and in turn enhance DOD capabilities through continued sharing of relevant technology as appropriate and warranted.

**Essential Characteristics for HD, CS, and EP:**

- Fully Integrated
- Expeditionary
- Networked
- Decentralized
- Adaptable
- Decision Superiority
- Effective

### 6.a. Essential Characteristics

To accomplish the missions and objectives associated with each of the three campaign frameworks presented in this JOC successfully, the Joint Force must possess a number of essential characteristics. Each characteristic was derived from and builds upon the attributes and key characteristics identified by the NMS, CCJO, and other strategic guidance:

- ❖ **Fully Integrated** – All DOD component capabilities are created inherently capable of integration into a focused effort with a unified purpose. Forces employed for HD and CS operations must be able to work not only with every Service and Service auxiliary (Army, Navy, Air Force, Marines, and Coast Guard), including Reserve Component forces regardless of whether they are under federal or state control, but also interagency elements (for example, the Bureau of Customs and Border Protection), and forces employed by multi-national partners (for example, Canadian or Mexican forces). In addition, DOD must be able to work toward a common objective with any of

these forces in any domain (for example, air-based forces able to coordinate with maritime forces).

- ❖ **Expeditionary** – Rapidly deployable, employable, and sustainable throughout the global battlespace and independent of existing infrastructure. Being expeditionary allows the Joint Force, along with partners and allies, to seize and maintain the initiative required to accomplish its mission. It will enable operational forces to conduct prompt HD and CS missions in response to directives with variable degrees of urgency (from time-critical or fleeting to predictable) and to respond with the operational or global reach required to deal with a threat wherever necessary.
- ❖ **Networked** – Physically connected and synchronized in time and purpose – allowing dispersed forces to communicate, collaborate, maneuver, and share knowledge and a common operating picture securely. Being networked implies technical interoperability; procedural interoperability allows disparate DOD, coalition, non-government organizations, and interagency partners to coordinate to achieve a desired end state. Networking is further enhanced by facilitating communications between national and strategic leaders to combatant commanders and from combatant commanders through operational commanders to tactical warfighters, as well as interagency and multi-national partners. It includes both technical linkages, as well as relationships built on training and working with each other over time. A net-centric Joint Force is able to maintain an accurate presentation of the battlespace built through the integration of ISR, blue force situational awareness, geospatial mapping, and related database elements. This integrated picture allows the Joint Force Commander to make timely, accurate decisions to employ the right capabilities, at the right place and time more effectively.
- ❖ **Decentralized** – DOD use of collaborative planning and shared knowledge and understanding to empower subordinate commanders to compress decision cycles. Based on common real-time situational awareness and a clear understanding of Secretary of Defense directions, strategic objectives, and commander's intent, a decentralized Joint Force can conduct operations at lower echelons, thereby allowing greater autonomy and freedom of action (in accordance with objectives and intent) to permit subordinate commanders to seize the initiative and exploit fleeting opportunities. Decentralized

execution is a critical characteristic for Joint Forces conducting HD and CS operations.

- ❖ **Adaptable** – Trained and ready forces that can be tailored, scaled, and prepared to respond to any contingency quickly. Adaptability ensures that the Joint Force (or elements thereof) can shift rapidly from one mission to another (for example from HD to CS) and can adapt to changing situations, especially during periods of transition between missions. It ensures that forces can be committed to one mission in a steady-state environment (for example, HD), yet remain trained and ready to be committed to another mission (for example, major combat operations) that could occur in another region or operational area. Adaptable forces also have the flexibility to offer commanders a spectrum of means to achieve an objective (for example, kinetic or non-kinetic means).
- ❖ **Decision Superiority** – Gain and maintain information superiority to allow the force to shape the situation or react to changes. Information superiority allows Joint Force Commanders, supplied and informed with a common situational awareness fed by all-source information sharing, to assess and plan multiple options and to make timely and accurate decisions to achieve the desired effect and outcome. Superior decision making involves working at the leading edge of visionary, predictive intelligence fusion and analysis; staying ahead of adaptive, evolving threats; and facilitating information sharing with partner organizations. These actions are critical for HD and CS missions to be able to direct forces in a complex dynamic environment, apply force against fleeting targets or changing situations, and rapidly provide DOD forces to civil authorities in potentially time-critical situations.
- ❖ **Effective**<sup>24</sup> – DOD use of a portfolio of capabilities (including kinetic or non-kinetic means to create lethal or non-lethal

---

<sup>24</sup> Effective is based on the *CCJO* Joint Force characteristic “Lethal”, defined as the ability to destroy an adversary and / or his systems in all conditions and environments when required. It includes the use of kinetic and / or non-kinetic means, while leveraging technological advances in greater precision and more devastating target effects at both longer ranges and in close combat. For the purposes of the DOD HD and CS JOC, “Lethal” was determined as not broad enough in connotation to address all potential force application variations that DOD could be called upon to provide (for example, Visit, Board, Search, and Seizure (VBSS), Information Operations, Military Presence, Decontamination, and Security Augmentation).

effects, information operations, military presence, and decontamination) in a timely manner to detect, deter, prevent, defeat, or, if necessary, mitigate the effects of an attack. Effective Joint Forces provide commanders with the ability to apply force precisely and selectively in proportion to the nature of the threat for any HD or CS mission while minimizing collateral effects.

### **6.b. Relationship to Other Concepts**

In addition to the DOD HD and CS JOC, the Chairman of the Joint Chiefs of Staff and the TPG identified three additional initial JOCs for concurrent development. These other JOCs (Strategic Deterrence – now referred to as Deterrence Operations, Major Combat Operations, and Stability Operations – now referred to as Military Support to Stabilization, Security, Transition and Reconstruction Operations) are closely interrelated and linked with the ideas and concepts presented in this document. Additionally, in fulfilling its responsibilities across the range of HD, CS, and EP, DOD applies several standardized functions – each embodied in a JFC. Each of these functions (battlespace awareness, command and control, force application, focused logistics, protection, net-centric, force management, and training) has unique applications with respect to DOD’s responsibilities associated with HD, CS, and EP. Although these other concepts are addressed in a number of areas within this document, the relationships between this JOC and the other three JOCs, as well as the JFCs, warrant further discussion and clarification.

#### **❖ Major Combat / Military Support to Stabilization, Security, Transition and Reconstruction Operations**

Major combat and military support to stabilization, security, transition, and reconstruction operations are linked with the DOD HD and CS JOC in several key ways. In the most basic sense, a secure US Homeland is a prerequisite for undertaking major combat and / or military support to stabilization, security, transition and reconstruction operations in that it ensures and protects DOD’s ability to deploy forces overseas to project power and conduct these operations. Potential adversaries could target attacks against “rear areas” in the Homeland (for example, military units’ home bases or major deployment centers) in an attempt to forestall US deployment for overseas operations. This JOC is also related to major combat and military support to stabilization, security, transition and reconstruction operations in that an attack on the Homeland may provoke major combat and / or military support to stabilization, security, transition, and reconstruction operations in response (for example, the Afghanistan campaign to the 11 September 2001 terrorist attacks). However, a key distinction exists between the

DOD HD and CS JOC and those JOCs addressing major combat and military support to stabilization, security, transition and reconstruction operations. Specifically, although the strategic objective presented in the DOD HD and CS JOC is the protection of the Homeland from external threats and aggression using integrated operational and tactical offensive and defensive measures, the military art required to conduct those measures or operations successfully is not addressed.

### ❖ **Deterrence Operations**

Deterrence operations and DOD's efforts to secure the Homeland are intrinsically linked. Deterrence operations is the prevention of aggression or coercion by adversaries that could threaten vital interests of the US and / or its national survival. Deterrence prevents an adversary from choosing hostile courses of action affecting the United States by means of decisive influence over their decision making. The objective of deterrence is to convince potential adversaries that courses of action that threaten US national interests will result in outcomes that are decisively worse than they could achieve through alternative courses of action. Effective deterrence operations requires strategic forces and capabilities that provide the President with a wider range of military options to (a) deny an adversary the benefits of his actions, (b) impose costs on the adversary, or (c) encourage adversary restraint. Specific capabilities required for deterrence operations will vary significantly from adversary to adversary, but include force projection, active and passive defenses, global strike, and strategic communication and information operations. These efforts are enabled by global situational awareness, command and control, forward presence, security cooperation, and military integration and interoperability. Deterrence is a continuous activity that provides global influence. Thus, HS, HD, and deterrence operations have the same goal – preventing attacks against the Homeland – but although deterrence operations is focused on influencing an adversary's decision to attack the Homeland, HS and HD are focused on active and passive prevention and deterrence of attacks.

### ❖ **Battlespace Awareness**

Battlespace awareness is the ability of the Joint Force Commander to understand the operational environment, the full array of interagency and international capabilities, and the adversary. To ensure DOD can detect, deter, prevent, or if necessary defeat threats to the Homeland and assist in mitigating the effects of attacks that do occur, the Joint Force Commander must have a comprehensive understanding of the battlespace (within the limits set by law). This includes the capability to detect the full range of threats enabled through an interlocking field of sensors with deep reach and remote surveillance capability, fused with

national-level intelligence collection and analysis to provide common situational awareness across the spectrum of participants for all domains in the operating environment (air, space, land, maritime, and cyber). For HD and CS, this includes shared awareness (including non-intelligence sources) between numerous government and non-government participants.

#### ❖ **Command and Control**

Command and control is the exercise of authority and direction by a properly designated commander over assigned and attached forces and equipment in the accomplishment of the mission. To ensure DOD can meet its responsibilities for HD, CS, and EP, the Joint Force Commander, leveraging battlespace awareness, develops multiple courses of action, recommends the best course of action, and directs force employment using the net-centric operational environment (NCOE) that facilitates rapid command decision making and information sharing with all applicable mission partners.

#### ❖ **Force Application**

Force application is the sum of all actions taken to cause a desired effect on an adversary. To ensure DOD can detect, deter, prevent, or if necessary defeat threats to the Homeland early in their development, the Joint Force Commander must be able to employ the full range of military capabilities, in coordination with other elements of national power, necessary to create the desired effect on an adversary. Such capabilities include the ability to defeat both conventional and unconventional (for example, CBRNE) attacks across the entire operating environment (air, space, land, maritime, and cyber). In most instances, DOD will be required to respond quickly (potentially in a time-sensitive situation) and will need to apply force selectively and with precision. Just as important is a targeting process facilitated by rules of engagement that ensures the correct target is identified and engaged with a level of force commensurate to the threat posed. DOD forces must be capable of precisely and selectively targeting hostile threats covered or concealed by civilian assets while avoiding collateral damage. The Joint Force Commander requires the capability to apply the appropriate means against threats to the Homeland, in coordination with the Interagency effort, in a manner that is proactive / offensive in nature, externally focused, and conducted in depth by layering integrated military and interagency capabilities, beginning at the source of the threat.



### ❖ **Focused Logistics**

Focused logistics is the ability to provide the Joint Force Commander the right personnel, equipment, supplies, and support in the right place at the right time, and in the right quantities, across the entire ROMO. To ensure DOD can conduct HD operations, or if directed, conduct CS missions, the Joint Force Commander must be able to deploy rapidly and sustain capabilities in area-denial or contaminated environments independent of existing infrastructure. Joint Force logistical capabilities are, in some instances, particularly relevant for CS missions (for example, medical supplies, airlift, and logistical assistance). All forces employed in CS missions should be self-sustaining without creating a large logistics footprint, either through deployment of critical supplies or drawing upon existing DOD infrastructure in the area of operation. In some cases, civilian infrastructure may be capable of providing the required level of support. All forces for HD and CS should have ready access to the Defense Transportation System to deploy within directed timelines. They also should be capable of operating throughout the strategic context of HD (Forward Regions, Approaches, and the Homeland) and in CS missions with little warning and in any operational environment.

### ❖ **Protection**

Protection is a process, a set of activities and capabilities by which the Joint Force protects personnel (combatant / non-combatant), information, and physical assets against the full spectrum of threats. To ensure DOD can perform its responsibilities associated with securing the Homeland and ensure the US ability to project power, the Joint Force Commander should protect all critical bases of operation, the forces that may be required, and other essential critical infrastructure as directed. To provide continuous and effective protection, the Joint Force should be capable of timely threat detection, assessment, and warning to prepare and employ decisive counter-measures. Because CBRNE weapons pose a unique and catastrophic threat, special measures must be taken to prevent or mitigate the effects of their use. Key components of protection include, but are not limited to: counter-proliferation, an effective defensive umbrella against missile attack, and the capability to assist civilian authorities, if so directed, in managing the consequences of natural and man-made hazards (including incidents involving CBRNE weapons or materials).

### ❖ **Net-Centric**

Net-centric is the enabling capability wherein the Joint Force exploits the human and technical connectivity and interoperability fully

to achieve unprecedented levels of operational effectiveness and efficiency across the ROMO. For DOD to operate within the net-centric operational environment effectively while performing its roles and responsibilities associated with securing the Homeland, it must exploit all human and technical networking capabilities. These capabilities are facilitated by information transport, network management, enterprise services, mission applications, and knowledge management, all protected through information assurance measures. Of vital importance in the net-centric operational environment is the need for the effective integration of varied, non-standard, dynamic, and often unanticipated communications capabilities between DOD and its mission partners, throughout all phases of the operation.

### ❖ **Force Management**

Force Management is the capability to integrate new and existing human and technical assets from across the Joint Force and its mission partners to make the right capabilities available at the right time and place in support of the NDS. This is especially important for DOD in determining the proper Active and Reserve Component mix required not only to conduct Forward Region missions, but also to ensure that the missions in the Approaches and the Homeland can be effectively conducted and supported. DOD must consider, as part of its Total Force management plan, the roles and contributions that its non-DOD interagency and coalition partners make to the Total Force effort in detecting, deterring, preventing, or, if necessary, defeating external threats and aggression, as well as direct attacks against the Homeland.

### ❖ **Training**

Training is a vital element of DOD's overall ability to provide protection and the level of security required to ensure the continued safety of the Homeland, its citizens, and their property. Training of the DOD Joint Force in not only traditional warfighting skills, but also in skills designed to address the ever increasing asymmetrical threat is paramount. To ensure DOD can effectively conduct its HD and CS missions, the future Joint Force must be trained to be flexible and versatile when confronting future threats that continue to move from traditional challenges to the more catastrophic and disruptive. Future Joint Force training must also include wargames and exercises with interagency and multi-national partners designed to enhance interoperability through standardized training procedures and programs.

## **6.c. Related Issues**

Securing the Homeland is a complex challenge. There are issues related to that challenge that are important and distinct enough to merit clarification of how they relate to security of the Homeland and to the concepts covered in this JOC. These issues include:

### **❖ Critical Infrastructure Protection (CIP)**

For DOD, CIP is an overarching term that has HD, CS, and EP implications. According to the current DOD definition<sup>25</sup>, CIP includes actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. The Defense Critical Infrastructure Program (DCIP) is a DOD risk management program that seeks to ensure the availability of networked assets critical to DOD missions. Activities include the identification, assessment, and security enhancement of assets essential for executing the NMS. CIP is concerned with the assurance of assets that provide services or products that DOD requires to enable it to accomplish missions to deter aggression, project forces, and conduct operations. Physical protection is one of many possible risk mitigation activities that could be considered. Direction to protect critical assets outside of DOD ownership or control, but that have an effect on DOD missions, originates from senior leaders (for example, the President or Secretary of Defense) and, for purposes of this JOC are considered core functions carried out by relevant installation commanders or DOD asset owners (as a complement to Force Protection / COOP functions). However, DOD also may be called upon to protect civilian critical infrastructure (for example, bridges and power plants) unrelated (or only tangentially so) to DOD's military missions. In these cases, CIP could be a HD mission with DOD in the lead, or take on a CS connotation. This is a critical distinction for two reasons: (1) use of force policy may differ between the HD and CS CIP paradigms, and (2) Although the HD CIP functions are part of DOD's core mission, the CS CIP functions are undertaken only if approved by the Secretary of Defense consistent with existing legal constraints and only if they do not negatively affect DOD's primary warfighting mission.

### **❖ Force Protection**

"Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. Force protection does not include

---

<sup>25</sup> DODD 3020.40, 19 August 2005

actions to defeat the enemy or protect against accidents, weather, or disease.”<sup>26</sup> These measures conserve the force’s fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the Joint Force while degrading opportunities for the enemy. HD and force protection are closely related. Force protection is a key enabling function carried out continuously in the conduct of DOD missions. Accomplishment of HD protects DOD installations and facilities, as well as the general population and territory of the Homeland. DOD has a specific responsibility to defend military installations and DOD-owned or leased facilities against CBRNE attacks. This responsibility is closely related to the HD mission in that carrying out HD tasks protects DOD installations and facilities in CONUS, Alaska, Hawaii, and US territories and possessions, as well as the general population of the Homeland. A crucial element of that responsibility involves collecting and evaluating non-validated threat information for DOD installation defense. Prevention of many potential attacks involves the combined efforts of the Intelligence Community, DHS, law enforcement, and DOD. DOD may perform in support of these civil authorities as described previously in this concept. For example, DOD might support or enable DHS in the event a state or non-state actor has introduced into or found within the United States the components and materiel to manufacture a weapon. However, regardless of DOD’s role at any given time, DOD is responsible for protection of its installations and facilities. DOD also is responsible for protecting personnel from CBRNE attacks, responding to such attacks with trained and equipped emergency responders, and ensuring that installations are able to continue critical operations during an attack and resume essential operations after an attack.

#### ❖ **Information Operations (IO)**

IO is the integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with the specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own. In the 2012 – 2025 timeframe, IO abilities, including computer network attack, will be among the portfolio of capabilities available to commanders and may provide a less lethal, less destructive means of preventing or defeating threats.

---

<sup>26</sup> *Joint Publication 1-02.*

## ❖ **Active and Reserve Components**

The Reserve Component is an integral element of the Total Force<sup>27</sup> and plays a key role in DOD responsibilities associated with HD, CS, and EP. The specialized low density / high demand skill sets in the National Guard – coupled with their unique relationship with civil authorities at the local and state level – often translates into deployment locally within the first 24 hours of an event. Additionally, some Reserve Component forces possess specialized HD and / or CS skills that are limited in the Active Component. This provides the capability to execute a synchronized military response. The National Guard is organized, trained, and equipped by DOD, and can operate in most traditional DOD missions within the spectrum of Title 10, Title 32, or State active duty status. Additionally, the National Guard in State or Title 32 status possesses many of the characteristics required of an effective Joint Force, yet remains responsive to State sovereign authorities free of many of the limitations that constrain federal forces. The Secretary of Defense has discretionary authority to approve proposed HD activities for the National Guard with each proposed activity considered on the merits of the nature of the threat, criticality of the mission to national security, mission appropriateness, and finally the effect of military preparedness on the Total Force. Whether built into operational and contingency plans as friendly forces available for coalition-style, cooperative operations, or addressed directly as assigned forces under specified command arrangements such as JTF augmentation, the use of National Guard and Reserve Component forces, as an integral part of the Total Force package, helps bridge the gap and ensures that those forces remain an essential partner in the defense of the Homeland.

---

<sup>27</sup> For a more detailed description of the Total Force, refer to Section V of the June 2005 *Strategy for Homeland Defense and Civil Support* and the 19 September 2005 *Congressional Research Service Report* for Congress on DOD's disaster response to Hurricane Katrina.

## **CONCLUSION**

This JOC scopes the depth and breadth of HD, CS, and EP responsibilities confronting DOD. It identifies the most prevailing problem facing DOD in the 2012 - 2025 timeframe; how DOD will fulfill responsibilities of securing the Homeland including detecting, deterring, preventing, or, if necessary, defeating external threats or aggression to the Homeland, how to be prepared to respond to catastrophic incidents as appropriate or as directed, and how to integrate and operate with non-DOD and international partners to achieve unity of effort for HD and CS. This JOC proposes a multi-faceted solution with an active, layered defense, unified action to achieve unity of effort, methods to reduce uncertainty (including the proposal for a NHSP), and the desired end state, effects, and capabilities that the future Joint Force Commander will require.

This JOC will guide development and foster integration of DOD's JFCs and JICs with ancillary HD and CS applications to provide the foundation for development and acquisition of new capabilities through changes in Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF). Similarly, this JOC provides other concept developers with a strategic concept and operational context, including how DOD will operate in the overlap of responsibilities with other federal, state, and local authorities, from which those developers may derive or amplify particular military functions across the range of HD, CS, and EP mission sets.

This JOC discusses Joint Force, interagency, and multi-national implications of DOD's role in HD and CS, and highlights the need for DOD to mature its relationships with interagency and international partners to ensure geographical and functional integration necessary for DOD to perform its responsibilities to secure the Homeland. The intent at the national level is to have adequately resourced and exercised national plans, and integrated national command and control, which provide the basis for effective and timely HD and CS operations across the full range of potential threats. The intent for DOD is to implement fully its roles and responsibilities in planning and executing national HD and CS operations.

## 7.0 APPENDICES

### APPENDIX A: References

- a. 2010 Theater Air and Missile Defense Concepts (Pamphlet), Undated
- b. Battlespace Awareness Joint Functional Concept, 31 December 2003
- c. Capstone Concept for Joint Operations (CCJO), 3 August 2005
- d. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3010.02B, Joint Operations Concepts Development Process (JOpsC-DP), 27 January 2006
- e. CJCSI 3170.01E, Joint Capabilities Integration and Development System (JCIDS), 11 May 2005
- f. Command and Control Joint Functional Concept, December 2003
- g. Congressional Research Service Report for Congress, Hurricane Katrina: DOD Disaster Response, 19 September 2005
- h. Defense Adaptive Red Team (DART) Working Paper # 02-4, A Practical Guide for Developing and Writing Military Concepts, December 2002
- i. Defense Planning Guidance (DPG) 2004-2009 (U), May 2002, SECRET
- j. Defense Planning Scenario: Homeland Defense, 2010-2012 (U), 21 November 2003, SECRET//NOFORN
- k. Department of Defense Directive (DODD) 3025.dd, 1 January 2006
- l. Department of Defense Directive (DODD) 3020.40, Defense Critical Infrastructure Program (DCIP), 19 August 2005
- m. Executive Order (EO) 12656, Assignment of Emergency Preparedness Responsibilities (as amended by: EO 13074, 9 February 1998; EO 13228, 8 October 2001; and EO 13286, 28 February 2003)
- n. Fifth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (Gilmore Commission), Forging America's New Normalcy--Securing our Homeland, Protecting Our Liberty, 15 December 2003
- o. Focused Logistics Joint Functional Concept, December 2003

- p. Force Application Joint Functional Concept, February 2004
- q. Homeland Security Joint Operating Concept Version 1.0, February 2004
- r. Homeland Security Presidential Directive (HSPD) 5, Management of Domestic Incidents, 28 February 2003
- s. Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection, 17 December 2003
- t. Joint Operations Concepts (JOpsC), November 2003
- u. Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 12 April 2001 (as amended through 9 November 2006)
- v. Joint Publication 3-01.1, Aerospace Defense of North America, 4 November 1996
- w. Joint Publication 3-03, Joint Interdiction Operations, 10 April 1997
- x. Joint Publication 3-13, Information Operations, 13 February 2006
- y. Joint Publication 3-14, Joint Doctrine for Space Operations, 9 August 2002
- z. Joint Publication 3-26, Homeland Security, 2 August 2005
- aa. JROC Memorandum (JROCM) 022-03, An Evolving Joint Perspective: US Joint Warfare and Crisis Resolution in the 21<sup>st</sup> Century (JW&CR), 28 January 2003
- bb. JROCM 023-03, Interim Range of Military Operations (ROMO), 28 January 2003
- cc. Major Combat Operations Joint Operating Concept, Version 2.0, December 2006
- dd. National Incident Management System , 1 March 2004
- ee. National Military Strategy, 13 May 2004
- ff. National Military Strategic Plan for the War on Terrorism, 4 March 2005 and 1 February 2006
- gg. National Response Plan (NRP), December 2004
- hh. National Security Strategy of the United States of America, 16 March 2006
- ii. National Security Presidential Directive NSPD-41, 21 December 2004
- jj. National Strategy for Maritime Security, September 2005



- kk. National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, February 2003
- ll. National Strategy for Combating Terrorism (NSCbT), September 2006
- mm. National Strategy for Homeland Security, July 2002
- nn. National Strategy to Combat Weapons of Mass Destruction, December 2002
- oo. National Military Strategy to Combat Weapons of Mass Destruction, 13 February 2006
- pp. National Strategy to Secure Cyberspace, February 2003
- qq. Net-Centric Environment Joint Functional Concept Version 1.0, 7 April 2005
- rr. Net-Centric Operational Environment Joint Integrating Concept Version 1.0, 31 October 2005
- ss. Presidential Decision Directive (PDD) 67, Enduring Constitutional Government and Continuity of Government Operations (U), 21 October 1998, SECRET
- tt. Protection Joint Functional Concept, 31 December 2003
- uu. Quadrennial Defense Review Report (QDR), 30 September 2001
- vv. Quadrennial Defense Review Report (QDR), 6 February 2006
- ww. Security Cooperation Guidance (U), 22 November 2005, SECRET//NOFORN
- xx. Military Support to Stabilization, Security, Transition, and Reconstruction Operations Joint Operating Concept, Version 2.0, August 2006
- yy. Deterrence Operations Joint Operating Concept, Version 2.0, December 2006
- zz. Strategic Planning Guidance (U), 22 March 2006, SECRET
- aaa. Strategy for Homeland Defense and Civil Support, 24 June 2005
- bbb. The Joint Operational Environment: Into the Future, USJFCOM, Living Draft, 5 August 2005
- ccc. The National Defense Strategy of The United States of America, 1 March 2005
- ddd. Transformational Planning Guidance, April 2003

THIS PAGE INTENTIONALLY LEFT BLANK

## APPENDIX B: Glossary and Acronyms

### Glossary:

**Air Defense:** All defensive measures designed to destroy attacking enemy aircraft or missiles in the Earth's envelope of atmosphere, or to nullify or reduce the effectiveness of such attack. (JP 1-02)

**Air & Space Defense:** All measures of Homeland Defense taken to detect, deter, prevent, defeat, or nullify hostile air, missile, and space threats, against US territory, domestic population, and critical infrastructure. (Joint Staff J7 working definition, modified. JP 1-02 definition of aerospace defense)

**Capability:** The ability to achieve a desired effect under specified standards and conditions through combinations of means and ways to perform a set of tasks. (CJCSI 3170.01E)

**Catastrophic Challenges:** Challenges involving the acquisition, possession, and use of WMD or methods producing WMD-like effects. (NDS)

**Characteristic:** A desirable trait, quality, or property that distinguishes how the future Joint Force should conduct military operations. (CJCSI 3010.02B)

### **Civil Support (CS):**

- Department of Defense (DOD) support to US civil authorities for domestic emergencies and for designated law enforcement and other activities. (JP 3-26)
- Civil Support, also referred to as Defense Support of Civil Authorities (DSCA)), missions are undertaken by the Department when its involvement is appropriate and when a clear end state for the Department's role is defined. (Strategy for HD and CS)

**Consequence Management:** Actions taken to maintain or restore essential services and manage and mitigate problems resulting from disasters and catastrophes, including natural, manmade, or terrorist incidents. Also called CM. (JP 1-02)

**Continuity of Government (COG):** A coordinated effort within each branch of government ensuring the capability to continue branch minimum essential responsibilities in a catastrophic crisis. COG is dependent on effective continuity of operations, plans, and capabilities. DOD COG activities involve ensuring continuity of delegations of authority (where permissible, and in accordance

with applicable law); the safekeeping of vital resources, facilities, and records; the improvisation or emergency acquisition of vital resources necessary for the performance of Mission Essential Functions (MEF); and the capability to relocate essential personnel and functions to, and sustain performance of MEF at, alternate work sites(s) until normal operations can be resumed. (DODD 3020.26)

**Continuity of Operations (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. COOP 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)
- An internal effort within individual components of the Executive, Legislative, and Judicial branches of government ensuring the capability exists to continue uninterrupted essential component functions across a wide range of potential emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies. COOP involves plans and capabilities covering the same functional objectives of COG, must be maintained at a high level of readiness, and be capable of implementation both with and without warning. COOP is not only an integral part of COG and Enduring Constitutional Government (ECG), but is simply “good business practice” – part of the Department of Defense’s fundamental mission as a responsible and reliable public institution. (DODD 3020.26)

**Critical Infrastructure Protection:** Actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on the risk, these actions could include: changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding, etc. (DODD 3020.40)

**Cyber Defense:** All *defensive* measures (particularly computer network defense (CND)) taken to detect, deter, prevent, or if necessary defeat hostile cyber threats against DOD assets and the DIB. (DOD HLS JOC [Version 1.0] definition)

**Defense Support of Civil Authorities (DSCA):** DOD support, including Federal military forces, the Department’s career civilian

and contractor personnel, and DOD agency and component assets, for domestic emergencies and for designated law enforcement and other activities. The Department of Defense provides defense support of civil authorities when directed to do so by the President or Secretary of Defense. (Strategy for HD and CS)

**Disruptive Challenges:** Challenges that may come from adversaries who develop and use break-through technologies to negate current US advantages in key operational domains. (NDS)

**Effects:** The outcomes of actions taken to change unacceptable conditions, behaviors, or freedom of action to achieve desired objectives. (CCJO)

**Emergency Preparedness (EP):** Measures taken in advance of an emergency to reduce the loss of life and property and to protect a nation's institutions from all types of hazards through a comprehensive emergency management program of preparedness, mitigation, response, and recovery. (JP 3-26)

**End State:** The set of conditions, behaviors, and freedoms that defines achievement of the commander's mission. (CJCSI 3010.02B)

**Homeland Defense (HD):** The protection of US sovereignty, territory, domestic population and critical defense infrastructure against external threats and aggression, or other threats as directed by the President. The DOD is responsible for HD. (Strategy for HD and CS)

**Homeland Security (HS):** A concerted national effort to prevent terrorist attacks within the US, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. (National Strategy for Homeland Security)

**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 the specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own. Also called "IO". (JP 3-13)

**Irregular Challenges:** Challenges from those employing "unconventional" methods to counter the traditional advantages of stronger opponents. (NDS)

**Joint Functional Concept (JFC):** A JFC applies elements of the CCJO solution to describe how the joint force, 8 to 20 years into the future, will perform an enduring military function across the

full range of military operations. It identifies the operational-level capabilities required to support ROMO operations and the key attributes necessary to compare capability or solution alternatives. JFCs also determine any additional capabilities required to create effects identified in JOCs. (CJCSI 3010.02B)

**Joint Integrating Concept (JIC):** A JIC is an operational-level description of how a Joint Force Commander, 8 to 20 years into the future, will perform a specific operation or function derived from a JOC and / or JFC. JICs are narrowly scoped to identify, describe and apply specific capabilities, decomposing them into fundamental tasks, conditions, and standards for use in capability based assessments. Additionally, a JIC contains illustrative vignettes to facilitate understanding of the concept. (CJCSI 3010.02B)

**Joint Interagency Coordination Group (JIACG):** An interagency organization that establishes and / or enhances regular, timely, and collaborative working relationships between civilian and military operational planners. Composed of USG civilian and military experts accredited to the combatant commander and tailored to meet the requirements of the supported combatant commander, the JIACG provides the combatant commander with the capability to collaborate at the operational level with other USG civilian agencies and departments. (JP 3-08)

**Joint Interagency Task Force (JIATF):** A JIATF constituted and so designated by the Secretary of Defense and other Cabinet Secretaries who have provided forces, equipment, and / or personnel to build / establish an interagency task force to facilitate and accomplish a specified USG mission(s) and / or objectives. (JP 3-07.4)

**Joint Operating Concept (JOC):** A JOC applies the CCJO solution in greater detail to a specified mission area. It describes how a Joint Force Commander, 8 to 20 years in the future, is expected to conduct operations within a military campaign, linking end states and effects. It identifies effects and the broad capabilities considered essential for creating those effects. A JOC contains illustrative vignettes to facilitate understanding of the concept. Additionally, JOCs provide the operational context for JFC and JIC development. (CJCSI 3010.02B)

**Land Defense:** All measures of Homeland Defense taken to detect, deter, prevent, or defeat hostile land threats against US territory, domestic population, and critical infrastructure. (Joint Staff J7 working definition)

**Maritime Defense:** All measures of Homeland Defense taken to detect, deter, prevent, or defeat hostile maritime threats against US territory, domestic population, and critical infrastructure. (Joint Staff J7 working definition)

**Maritime Interception:** The detection, localization, evaluation, sorting, and possible stopping and boarding, by force if necessary, of commercial and noncommercial maritime traffic to deter, destroy, or seize contraband cargo, persons, or flagged vessels. These operations are carried out under the authority provided by international law, treaty, agreement, or United Nations resolution and sanction. (Joint Staff J-5 working definition)

**Military Assistance for Civil Disturbances (MACDIS):** A mission set of civil support involving DOD support, normally based on the direction of the President, to suppress insurrections, rebellions, and domestic violence, and provide federal supplemental assistance to the States to maintain law and order. (JP 1-02)

**Military Assistance to Civil Authorities (MACA):** The broad mission of civil support consisting of the three mission subsets of military support to civil authorities, military support to civil law enforcement agencies, and military assistance for civil disturbances. (JP 1-02)

**Military Support to Civilian Law Enforcement Agencies (MSCLEA):** A mission of civil support that includes support to civilian law enforcement agencies. This includes, but is not limited to: combating terrorism, counter-drug operations, national security special events, and national critical infrastructure protection and key asset protection. (JP 1-02)

**Net-Centric Operational Environment (NCOE):** The coherent application of seamless, integrated net-centric capabilities to the forward edge of the battlespace enabling full spectrum dominance. (Net-Centric Operational Environment JIC)

**Traditional Challenges:** Challenges posed by states employing recognized military capabilities and forces in well-understood forms of military competition and conflict. (NDS)

**Acronyms:**

ALCM.....	Air-Launched Cruise Missile
AOR.....	Area of Responsibility
BMD.....	Ballistic Missile Defense
BMDS.....	Ballistic Missile Defense System
CBRNE .....	Chemical, Biological, Radiological, Nuclear, or High Yield Explosives
CCJO.....	Capstone Concept for Joint Operations
CIP .....	Critical Infrastructure Protection
CJCS .....	Chairman of the Joint Chiefs of Staff
CJCSI.....	Chairman of the Joint Chiefs of Staff instruction
CJCSM .....	Chairman of the Joint Chiefs of Staff manual
C2 .....	Command and Control
CM.....	Consequence Management
CND.....	Computer Network Defense
COG .....	Continuity of Government
CONUS .....	Continental United States
COOP .....	Continuity of Operations
CS .....	Civil Support
DART .....	Defense Adaptive Red Team
DCIP.....	Defense Critical Infrastructure Program
DSCA.....	Defense Support of Civil Authorities
DHS.....	Department of Homeland Security
DIB.....	Defense Industrial Base
DOD .....	Department of Defense
DOJ.....	Department of Justice
DOTMLPF .....	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities
DPG.....	Defense Planning Guidance
ECG.....	Enduring Constitutional Government
EO .....	Executive Order
EP.....	Emergency Preparedness
GLCM .....	Ground-Launched Cruise Missile
GWOT.....	Global War on Terrorism
HD.....	Homeland Defense
HS .....	Homeland Security
HSPD.....	Homeland Security Presidential Directive
ICBM .....	Intercontinental Ballistic Missile
IRBM .....	Intermediate Range Ballistic Missile
IGO.....	Inter-Governmental Organization
IO .....	Information Operations
ISR .....	Intelligence, Surveillance, and Reconnaissance
JCA .....	Joint Capability Area



JCIDS..... Joint Capabilities Integration and Development System  
 JFC..... Joint Functional Concept  
 JFHQ..... Joint Force Headquarters  
 JIACG..... Joint Interagency Coordination Group  
 JIATF..... Joint Interagency Task Force  
 JIC ..... Joint Integrating Concept  
 JOA ..... Joint Operations Area  
 JOC ..... Joint Operating Concept  
 JOE ..... Joint Operational Environment  
 JOpsC ..... Joint Operations Concepts  
 JROC..... Joint Requirements Oversight Council  
 JROCM..... Joint Requirements Oversight Council Memorandum  
 JTF ..... Joint Task Force  
 JW&CR..... Joint Warfare and Crisis Resolution  
 LFA..... Lead Federal Agency  
 LEO ..... Low Earth Orbit  
 MACA ..... Military Assistance to Civil Authorities  
 MACDIS..... Military Assistance for Civil Disturbances  
 MANPADS..... Man-portable air defense system  
 MDA ..... Maritime Domain Awareness  
 MEF..... Mission Essential Functions  
 MSCLEA ..... Military Support to Civilian Law Enforcement Agencies  
 NCOE ..... Net-Centric Operational Environment  
 NDS..... National Defense Strategy  
 NGO ..... Non-governmental Organization  
 NHSP..... National Homeland Security Plan  
 NMS ..... National Military Strategy  
 NORAD ..... North American Aerospace Defense Command  
 NRP ..... National Response Plan  
 NSCbT..... National Strategy for Combating Terrorism  
 NSHS..... National Strategy for Homeland Security  
 NSPD..... National Security Presidential Directive  
 NSS ..... National Security Strategy  
 OSD..... Office of the Secretary of Defense  
 PA..... Public Affairs  
 PD ..... Public Diplomacy  
 PDD..... Presidential Decision Directive  
 QDR ..... Quadrennial Defense Review  
 RFA ..... Request for Assistance  
 ROMO..... Range of Military Operations  
 SJFHQ..... Standing Joint Force Headquarters  
 SLBM..... Submarine-Launched Ballistic Missile  
 SLCM..... Sea-Launched Cruise Missile

SPG ..... Strategic Planning Guidance  
TPG ..... Transformation Planning Guidance  
TSA..... Transportation Security Administration  
TTP..... Tactics, Techniques, and Procedures  
UAS ..... Unmanned Aircraft System  
UAV ..... Unmanned Aerial Vehicle  
US ..... United States  
USCENTCOM..... United States Central Command  
USEUCOM ..... United States European Command  
USG..... United States Government  
USJFCOM..... United States Joint Forces Command  
USNORTHCOM ... United States Northern Command  
USPACOM ..... United States Pacific Command  
USSOCOM..... United States Special Operations Command  
USSOUTHCOM ... United States Southern Command  
USSTRATCOM .... United States Strategic Command  
USTRANSCOM... United States Transportation Command  
VBSS ..... Visit, Board, Search, and Seizure  
WMD.....Weapon of Mass Destruction

**APPENDIX C: Operational Level Effects and Associated Joint Capability Areas**

This appendix summarizes the operational-level desired effects considered essential for achieving the end state envisioned by the DOD HD and CS JOC. The appendix links each of these effects to the associated JCA necessary to create them. The table defines the JOC end state and the five objectives derived from the actions of detect, deter, prevent, defeat, and support. Each objective contains the effects / broad capabilities. The applicable mission set is also noted (e.g. Airborne Threats). These effects are mapped to primary Tier 1 JCAs and each of these Tier 1 JCAs to applicable Tier 2 JCAs to further DOD’s continued evolution of the JCIDS.

<b>END STATE</b>			
<b>A secure US Homeland, effectively defended from external threats and aggression, and capable of managing consequences of attacks by state or non-state actors, as well as natural disasters.</b>			
<b>OBJECTIVE</b>			
<b>DETECT: Discover and characterize the intention and capability of an emerging or existing adversary as early as possible.</b>			
<b>EFFECTS</b>		<b>JOINT CAPABILITY AREAS</b>	
		<b>TIER 1</b>	<b>TIER 2</b>
Airborne Threat	Legitimate air activity distinguished from hostile air activity.	Command and Control	Develop Shared SA and Understanding
		Net-Centric Operations	All
		Interagency Coord	USG Integration
		Homeland Defense	Air and Space Defense
	Hostile aircraft / UAVs located and tracked.	Homeland Defense	Air and Space Defense
Battlespace Awareness		All	

Airborne Threat		Command and Control	Develop Shared SA and Understanding
	Intelligence coordinated / shared among interagency, inter-governmental, and international partners.	Interagency Coord	USG Integration; Intergovernmental Coordination
		Command and Control	Develop Shared SA and Understanding
		Public Affairs Operations	Public Info; Command / Internal Info
		Battlespace Awareness	Observation and Collection; Analysis and Production
	Adversary missile sites / platforms located (before launch).	Net-Centric Operations	All
		Spec Ops & Irregular Ops	Special Recon
		Battlespace Awareness	All
	Adversary missile launch detected and tracked.	Homeland Defense	Air and Space Defense
		Air Operations	Air Interdiction
		Battlespace Awareness	All
	Effective and timely identification of airborne attack precursors (positioning, shipment, or acquisition of required delivery systems / equipment).	Interagency Coord	USG Integration; Intergovernmental Coord
		Command and Control	Develop Shared SA and Understanding
		Spec Ops & Irregular Operations	Special Recon
		Net-Centric Operations	All
Maritime Threat	Legitimate maritime activity distinguished from hostile maritime activity.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
		Interagency Coord	USG Integration
		Homeland Defense	Maritime Defense

Maritime Threat		Maritime / Littoral Operations	Maritime Interception and Interdiction
	Hostile maritime activity (surface and sub-surface vessels) located and tracked.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
		Homeland Defense	Maritime Defense
		Maritime / Littoral Operations	Maritime Interception and Interdiction
	Intelligence coordinated / shared among interagency, inter-governmental, and international partners.	Interagency Coord	USG Integration; Intergovernmental Coordination
		Command and Control	Develop Shared SA and Understanding
		IA/IGO/MN/NGO Coordination	All
		Public Affairs Operations	Public Info; Command / Internal Info
	Exploitation or disruption to free flow of maritime commerce detected.	Interagency Coord	USG Integration; Intergovernmental Coordination
		Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
	Contents of maritime vessels identified.	Battlespace Awareness	Observation and Collection; Analysis and Production
		Maritime / Littoral Operations	Maritime Interception and Interdiction
	Land Threat	Legitimate land activity distinguished from hostile land activity.	Battlespace Awareness
Command and Control			Develop Shared SA and Understanding
Homeland Defense			Land Defense

Land Threat	Hostile land activity / movement located and tracked.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
		Net-Centric Operations	All
	Intelligence coordinated / shared among interagency, inter-governmental, and international partners.	Interagency Coord	USG Integration; Intergovernmental Coordination
		IA/IGO/MN/NGO Coordination	All
		Command and Control	Develop Shared SA and Understanding
		Public Affairs Operations	Public Info; Command/Internal Info
	Military installations and critical infrastructure compromises detected.	Interagency Coord	USG Integration; Intergovernmental Coordination
		Command and Control	Develop Shared SA and Understanding
		Public Affairs Operations	Public Info; Command/Internal Info
	Infiltration through land borders with Mexico and Canada identified.	Battlespace Awareness	Observation and Collection; Analysis and Production
		Interagency Coord	USG Integration; Intergovernmental Coordination
		Public Affairs Operations	Public Info; Command/Internal Info
Space Threat	Legitimate space activity distinguished from hostile space activity.	Net-Centric Operations	All
		Interagency Coord	USG Integration; Intergovernmental Coordination

Space Threat		Homeland Defense	Air and Space Defense
		Command and Control	All (Space Situational Awareness)
		Battlespace Awareness	All (Space Situational Awareness)
	Hostile space and infrastructure activity located and tracked.	Battlespace Awareness	All (Space Situational Awareness)
		Net-Centric Operations	All
		Interagency Coord	USG Integration; Intergovernmental Coordination
		Command and Control	All (Space Situational Awareness)
		Space Operations	Space Control
	Intelligence coordinated / shared among interagency, inter-governmental, and international partners.	Interagency Coord	USG Integration; Intergovernmental Coordination
		Command and Control	Develop Shared SA and Understanding
		IA/IGO/MN/NGO Coordination	All
		Public Affairs Operations	Public Info; Command/Internal Info
	Exploitation of use of commercial space information for hostile intent identified.	Space Operations	Space Control
Interagency Coord		USG Integration; Intergovernmental Coordination	
Public Affairs Operations		Public Info	
Cyber Threat	Legitimate cyber activity distinguished from illegal / hostile cyber activity.	Net-Centric Operations	All
		Interagency Coord	USG Integration

Cyber Threat	Illegal / hostile cyber activity located and tracked.	Net-Centric Operations	All
		Interagency Coord	USG Integration
	Intelligence coordinated / shared among interagency, inter-governmental and international partners.	Net-Centric Operations	All
		IA/IGO/MN/NGO Coordination	All
		Interagency Coord	USG Integration
	Adversary's cyber capacity / capability identified.	Net-Centric Operations	All
		Interagency Coord	USG Integration

**OBJECTIVE**

**DETER: Prevent hostile action by imposing costs, denying benefits, and encouraging restraint.**

<b>EFFECTS</b>		<b>JOINT CAPABILITY AREAS</b>	
		<b>TIER 1</b>	<b>TIER 2</b>
Airborne Threat	Legitimate air activity distinguished from hostile air activity.	Battlespace Awareness	All
		Interagency Coord	USG Integration
		Command and Control	Develop Shared SA and Understanding
		Homeland Defense	Air and Space Defense
	Rapid and effective deployment and sustainment of air assets from multiple dispersed locations.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
		Net-Centric Operations	All
		Interagency Coord	USG Integration
		Homeland Defense	Air and Space Defense
		Air Operations	Air Interdiction



Airborne Threat	Effective air operations conducted that are essential to deter threats from the Homeland.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
		Net-Centric Operations	All
		Interagency Coord	USG Integration
		Homeland Defense	Air and Space Defense
		Air Operations	Air Interdiction
	Visible deterrent through projected US airpower into the Forward Regions and / or Approaches.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
		Air Operations	Air Interdiction
	Dissuaded adversary action through robust integration, coordination, and shared information with international partners.	Net-Centric Operations	All
		Interagency Coord	USG Integration
	Projected air power to negate ground-based support and launch infrastructure.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
		Net-Centric Operations	All
		Interagency Coord	USG Integration
		Homeland Defense	Air and Space Defense
	Rapid conduct of preemptive or interception operations in the Forward Regions and / or Approaches to reduce the threat to the Homeland.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
		Net-Centric Operations	All
		Homeland Defense	Air and Space Defense
Air Operations		Air Interdiction	

Airborne Threat	Operationalized ballistic missile defense to deter international community from producing / manufacturing ICBMs / SLBMS / and short range missiles.	Battlespace Awareness	All
		Interagency Coord	USG Integration
		Protection	IAMD
		Homeland Defense	Air and Space Defense
	Legitimate air activity distinguished from hostile air activity.	Battlespace Awareness	All
		Interagency Coord	USG Integration
		Homeland Defense	Air and Space Defense
		Command and Control	Develop Shared SA and Understanding
		Air Operations	Air Interdiction
	Maritime Threat	Conduct effective maritime operations to deter threats to the Homeland.	Battlespace Awareness
Command and Control			Develop Shared SA and Understanding
Global Deterrence			Force Projection
Interagency Coord			USG Integration
Maritime and Littoral Operations			Maritime Intercept Operations
Homeland Defense			Maritime Defense
Rapid and effective deployment and sustainment of maritime forces in and from multiple dispersed locations.		Battlespace Awareness	All
		Command and Control	All
		Homeland Defense	Maritime Defense
		Logistics	Agile Sustainment and Joint Deployment/Rapid Distribution
US military presence in the Forward Regions		Maritime / Littoral Operations	All
	Battlespace Awareness	All	

Maritime Threat	/ Approaches.	Global Deterrence	Force Projection
		Interagency Coord	USG Integration
		Shaping	Presence
		Command and Control	Develop Shared SA and Understanding
		Maritime / Littoral Operations	Maritime Interception and Interdiction
		Net-Centric Operations	All
		Logistics	Joint Deployment/Rapid Distribution
	Strong forward presence to protect freedom of movement in littoral, coastal, and international waters.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
		Maritime / Littoral Operations	Maritime Interception and Interdiction
		Net-Centric Operations	All
		Access and Access Denial	Freedom of Navigation
		Global Deterrence	Force Projection
		Interagency Coord	USG Integration
		Shaping	Presence
	Logistics	Joint Deployment/Rapid Distribution	
	Early detection and interception of maritime threats as far from the Homeland as possible.	Battlespace Awareness	All
		Net-Centric Operations	All
Maritime / Littoral Operations		Maritime Interception and Interdiction	
Global Deterrence		Force Projection	

Maritime Threat		Logistics	Joint Deployment/Rapid Distribution
		Interagency Coord	USG Integration
	An active, layered defense in the maritime domain in the Forward Regions and / or Approaches.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
		Maritime / Littoral Operations	Maritime Interception and Interdiction
		Net-Centric Operations	All
	Globally projected expeditionary joint forces and conduct of joint operations in the Forward Regions and Approaches.	Logistics	Joint Deployment/Rapid Distribution
		Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
		Maritime / Littoral Operations	All
Global Deterrence		Force Projection	
Net-Centric Operations		All	
Land Threat	Conduct of effective military operations to dissuade adversary action.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
	Threat of preemptive military action by land forces to deter countries from assembling and operationalizing ballistic missiles.	Battlespace Awareness	All
		Protection	IAMD
		Homeland Defense	Air and Space Defense
	Maintenance of the ability to use US and coalition partner land forces to counter	Battlespace Awareness	All

Land Threat	conventional and asymmetric adversary forces that employ all types of warfare.	Command and Control	Develop Shared SA and Understanding
		Homeland Defense	Land Defense
	Collaboration with federal, state, and local officials to ensure interoperability in the land domain.	Command and Control	Develop Shared SA and Understanding
		Net-Centric Operations	All
		Interagency Coord	USG Integration
		Homeland Defense	Air and Space Defense
	Deterrence of attacks against critical infrastructure, bases, national borders and installations in the Homeland.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
		Homeland Defense	All
		Protection	All
Air Operations		Air Interdiction	
Space Threat	Use of space assets (ISR) to deter an adversary from launching a preemptive attack.	Battlespace Awareness	All
		Net-Centric Operations	All
	Negate threats in the Forward Regions, Approaches, and Homeland posed by adversary's orbital assets.	Battlespace Awareness	All
		Space Operations	All
		Net-Centric Operations	All
	Deterrence of adversary space assets from being used to attack the Homeland.	Battlespace Awareness	All
		Net-Centric Operations	All
		Space Operations	All
Homeland Defense		Air and Space Defense	

Space Threat	Negate adversary space threats and support infrastructure.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
		Space Operations	All
		Net-Centric Operations	All
	Leverage space superiority in global space operations.	Battlespace Awareness	All
		Net-Centric Operations	All
		Space Operations	All
		Air Operations	Air Interdiction
	Provision of time sensitive and accurate ISR of ballistic missile threats.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
		Net-Centric Operations	All
	Enhanced Homeland missile defense system integrated with theater-wide ballistic missile system to negate an adversary's attempt to launch ballistic missiles.	Battlespace Awareness	All
		Protection	IAMD
		Homeland Defense	Air and Space Defense
Accurate prediction of boost, midcourse, and terminal phases of missiles flight.	Battlespace Awareness	All	
	Net-Centric Operations	All	
	Homeland Defense	Air and Space Defense	
Shared information with theater security cooperation programs to deter adversary actions.	Net-Centric Operations	All	
	IA/IGO/MN/NGO Coordination	All	
	Interagency Coord	USG Integration	
Cyber Threat	Integrated command, control, and computer systems to enhance preemptive actions by US and coalition forces.	Battlespace Awareness	All
		Net-Centric Operations	All

Cyber Threat	Implemented global security protocol cyber systems to remediate potential vulnerabilities.	Net-Centric Operations	All
	Deterrence of the exploitation or destruction of the Defense Industrial Cyber Base.	Interagency Coord	USG Integration
	Mutual sharing and collaboration of communication, control and computer information to deter threats to the DIB.	Net-Centric Operations	All
		Interagency Coord	USG Integration
	Fully synchronize and coordinate a global communication strategy to deter an adversary from conducting a threatening act.	Net-Centric Operations	All
Interagency Coord		USG Integration	
<b>OBJECTIVE</b>			
<b>PREVENT: Preclude the initiation of hostile action against the US through shaping and preemptive actions.</b>			
<b>EFFECTS</b>		<b>JOINT CAPABILITY AREAS</b>	
		<b>TIER 1</b>	<b>TIER 2</b>
Airborne Threat	Leveraged deployments to protect the Homeland by assuring a responsive, executable, and legitimate power projection capability.	Battlespace Awareness	All
		Global Deterrence	Force Projection
		Shaping	Presence
		Logistics	Joint Deployment/Rapid Distribution
		Command and Control	Develop Shared SA and Understanding
	Preemptive airborne action in the Forward Regions and / or Approaches to prevent an	Battlespace Awareness	All

Airborne Threat	attack on the Homeland.	Homeland Defense	Air and Space Defense
		Air Operations	Air Interdiction
	Leveraged US and coalition air assets to prevent launch of ballistic missile(s) against the Homeland.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
	Protected and maintained air sovereignty in the Forward Regions, Approaches, and / or Homeland.	Battlespace Awareness	All
		Homeland Defense	Air and Space Defense
		Air Operations	Air Interdiction
	Low altitude surveillance and over the horizon acquisition to determine threat and possible target.	Battlespace Awareness	All
		Net-Centric Operations	All
		Homeland Defense	Air and Space Defense
Maritime Threat	Leveraged deployments to protect the Homeland by assuring a responsive, executable, and legitimate maritime power projection capability.	Homeland Defense	Maritime Defense
		Global Deterrence	Force Projection
		Shaping	Presence
		Logistics	Joint Deployment/Rapid Distribution
		Maritime / Littoral Ops	Maritime Interception and Interdiction
	Preemptive maritime action in the Forward Regions and / or Approaches to prevent an attack on the Homeland.	Battlespace Awareness	All
		Global Deterrence	Force Projection
		Shaping	Presence
		Logistics	Joint Deployment/Rapid Distribution
		Command and Control	Develop Shared SA and



Maritime Threat			Understanding
		Net-Centric Operations	All
	Leveraged US naval assets to prevent launch of ballistic missile(s) against the Homeland.	Battlespace Awareness	All
		Protection	IAMD
		Homeland Defense	Air and Space Defense
	Prevent hostile action(s) against US maritime and coalition maritime partners in the littoral, coastal, and international waters.	Battlespace Awareness	All
		Interagency Coord	USG Integration
		Global Deterrence	Force Projection
		Shaping	Presence
		Logistics	Joint Deployment/Rapid Distribution
		Maritime and Littoral Operations	All
		IA/IGO/MN/NGO Coordination	All
	Prevented use of the maritime domain from exploitation by terrorists.	Homeland Defense	Air and Space Defense
		Battlespace Awareness	All
		Maritime and Littoral Operations	All
Land Threat	Preemptive land action to prevent an imminent missile attack prior to launch by destroying critical infrastructure and command and control nodes.	Net-Centric Operations	All
		Battlespace Awareness	All
		Battlespace Awareness	All
	Homeland Defense	Land Defense	
	Battlespace Awareness	All	

Land Threat	Preemptive land action in the Forward Regions and / or Approaches to prevent an attack on the Homeland.	Air Operations	Air Interdiction
	Enhanced US military presence in the Forward Regions and / or Approaches to prevent potential attacks on the Homeland.	Battlespace Awareness	All
	Potential threats identified before they reach their intended targets.	Battlespace Awareness	All
		Net-Centric Operations	All
	Integrated efforts with national law enforcement agencies, as well as other federal, state, and local law officials to prevent an attack on the Homeland.	Net-Centric Operations	All
Interagency Coord		USG Integration	
Space Threat	Projected space power to prevent adversary forces from being deployed, employed or sustained in the Homeland, Forward Regions and / or Approaches.	Battlespace Awareness	All
		Net-Centric Operations	All
		Homeland Defense	Air and Space Defense
		Space Operations	All
	Defensive space action in the Forward Regions and / or Approaches to prevent an attack on the Homeland.	Battlespace Awareness	All
		Space Operations	All
		Net-Centric Operations	All
	Offensive space action in the Forward Regions and / or Approaches to prevent an attack on the Homeland.	Battlespace Awareness	All
		Net-Centric Operations	All
		Space Operations	All
		Homeland Defense	Air and Space Defense
	Integrated space-borne missile defense system(s) to prevent a missile attack(s) on the Homeland.	Homeland Defense	Air and Space Defense
		Protection	IAMD

Cyber Threat	Cyber attacks prevented from affecting the ability to deploy, employ, and sustain forces.	Battlespace Awareness	All
		Net-Centric Operations	All
		Homeland Defense	Air and Space Defense
	Cyber defensive action in the Forward Regions and / or Approaches to prevent an attack on the Homeland.	Battlespace Awareness	All
		Net-Centric Operations	All
	Established DOD and interagency policies, procedures, and doctrine for physical and cyber security.	Net-Centric Operations	All
		Interagency Coord	USG Integration
	Development and implementation of CM plans and procedures.	Homeland Defense	All
	Shared information, identification of key indicators, key resource, and risk assessments to mitigate and negate cyber threats to the DIB.	Battlespace Awareness	All
		Net-Centric Operations	All
		Interagency Coord	USG Integration
		Homeland Defense	Air and Space Defense
	Potential adversaries convinced that courses of action that threaten US national interests will result in undesirable outcomes.	Net-Centric Operations	All
		Interagency Coord	USG Integration
		Homeland Defense	Air and Space Defense
<b>OBJECTIVE</b>			
<b>DEFEAT: Deny the adversary's objective by dominating the Battlespace and the adversary.</b>			
<b>EFFECTS</b>		<b>JOINT CAPABILITY AREAS</b>	
		<b>TIER 1</b>	<b>TIER 2</b>
	Adversaries defeated in the Forward Region and / or Approaches before they reach the	Battlespace Awareness	All

Airborne Threat	Homeland.	Homeland Defense	Air and Space Defense
		Air Operations	Air Interdiction
	Adversaries defeated by enhancing regional stability.	Interagency Coord	USG Integration
		Homeland Defense	Air and Space Defense
	Adversaries defeated through a preemptive air strike.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
		Net-Centric Operations	All
		Interagency Coord	USG Integration
		Homeland Defense	Air and Space Defense
		Air Operations	Strategic Attack
		Global Deterrence	Global Strike
	Accurate identification and destruction of adversary missile support systems and critical infrastructure.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
		Net-Centric Operations	All
		Interagency Coord	USG Integration
		Homeland Defense	Air and Space Defense
		Protection	IAMD
		Air Operations	Strategic Attack
	Negated airborne threats in the Forward Regions, Approaches, and / or the Homeland before they reach the intended target.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
Net-Centric Operations		All	
Interagency Coord		USG Integration	
Homeland Defense		Air and Space Defense	

		Air Operations	Air Interdiction
Maritime Threat	Adversaries defeated in the Forward Regions and / or Approaches before they reach the Homeland.	Battlespace Awareness	All
		Global Deterrence	Force Projection
		Logistics	Joint Deployment/Rapid Distribution
		Command and Control	Develop Shared SA and Understanding
		Net-Centric Operations	All
		Homeland Defense	Maritime Defense
		Maritime / Littoral Ops	All
	Adversaries defeated by destroying delivery systems or critical infrastructure prior to takeoff.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
		Net-Centric Operations	All
		Air Operations	Strategic Attack
		Global Deterrence	Global Strike
		Interagency Coord	USG Integration
	Accurate identification and destruction of adversary missile support systems and critical infrastructure.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
		Net-Centric Operations	All
Defeat maritime threats in the Forward Regions and / or Approaches.	Battlespace Awareness	All	
	Global Deterrence	Force Projection	
	Logistics	Joint Deployment and Rapid Distribution	
	Command and Control	Develop Shared SA and Understanding	

Maritime Threat		Net-Centric Operations	All
		Interagency Coord	USG Integration
		Homeland Defense	Air and Space Defense
	Identified, tracked, intercepted, and defeated maritime threats that pose a threat to the Homeland by transporting WMD.	Battlespace Awareness	All
		Protection	WMD Threat, Elimination, Interdiction Operations
		Command and Control	Develop Shared SA and Understanding
		Net-Centric Operations	All
		Interagency Coord	USG Integration
		Homeland Defense	Maritime Defense
		Maritime and Littoral Operations	Maritime Interception and Interdiction
Land Threat	Key command and control nodes or weapon systems targeted prior to an attack on the Homeland.	Battlespace Awareness	All
		Net-Centric Operations	All
	Accurate identification and destruction of adversary missile support systems and critical infrastructure.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
		Net-Centric Operations	All
		Global Deterrence	Global Strike
		Air Operations	Strategic Attack
		Interagency Coord	USG Integration
	Defeated manned systems (for example, MANPADS) that pose a hazard in the Forward Regions, Approaches, and / or the Homeland.	Battlespace Awareness	All
		Homeland Defense	Land, Air and Space Defense
		Air Operations	Air Interdiction

Land Threat	Established and implemented procedures with interagency partners to defeat a land threat directed at the Homeland.	Interagency Coord	USG Integration	
		Defense Support to Civil Authorities	All	
	Retained ability to defeat conventional and asymmetric land threats to the Homeland.	Battlespace Awareness	All	
		Homeland Defense	Air and Space Defense	
Space Threat	Effective use of space capabilities to defeat adversaries in the Forward Regions and / or Approaches.	Battlespace Awareness	All	
		Net-Centric Operations	All	
		Homeland Defense	Air and Space Defense	
		Space Operations	All	
	Space assets leveraged to defeat and / or destroy command and control nodes and weapon systems in the Forward Regions and / or Approaches.	Battlespace Awareness	All	
		Net-Centric Operations	All	
		Space Operations	All	
		Homeland Defense	Air and Space Defense	
	ISR assets leveraged to be able to defeat an adversary's ballistic missile critical infrastructure and command and control nodes.	Battlespace Awareness	All	
		Space Operations	Space Control	
		ISR leveraged to defeat ballistic missile(s) in boost, midcourse, or terminal phase.	Battlespace Awareness	All
			Space Operations	Space Control
Cyber Threat	Leveraged computer networks to help defeat an adversary in the Forward Regions and / or Approaches.	Net-Centric Operations	All	
		Information Operations	Computer Network Operations	
	Adversary command and control nodes defeated.	Battlespace Awareness	All	
		Command and Control	Develop Shared SA and	

Cyber Threat			Understanding
		Net-Centric Operations	All
		Interagency Coord	USG Integration
		Global Deterrence	Global Strike
		Information Operations	Computer Network Attack
		Air Operations	Strategic Attack
	Shared information with theater security partners to permit preemptive actions.	Battlespace Awareness	All
		IA/IGO/MN/NGO Coordination	All
		Command and Control	Develop Shared SA and Understanding
		Net-Centric Operations	All
		Interagency Coord	USG Integration
	Adversary attempts to render the sharing of information with international partners defeated.	Battlespace Awareness	All
		Command and Control	Develop Shared SA and Understanding
		Information Operations	Computer Network Defense
		Net-Centric Operations	All
		Interagency Coord	USG Integration
	Systems leveraged to be able to render adversary cyber infrastructure harmless.	Battlespace Awareness	All
		Information Operations	Computer Network Operations
		Net-Centric Operations	All
	Established DOD and interagency policies, procedures, and doctrine for physical and cyber security.	Interagency Coord	USG Integration



Cyber Threat	Defeated cyber threats in the Forward Regions, Approaches, and/or the Homeland.	Net-Centric Operations	All
		Information Operations	Computer Network Operations
		Interagency Coord	USG Integration
<b>OBJECTIVE</b>			
<b>SUPPORT: Aiding, protecting, complementing, or sustaining another force in accordance with a directive requiring such actions.</b>			
<b>EFFECTS</b>		<b>JOINT CAPABILITY AREAS</b>	
		<b>TIER 1</b>	<b>TIER 2</b>
CBRNE Event	Properly trained and equipped forces for CBRNE defense and CM.	Defense Support to Civil Authorities	All
		Protection	WMD Threat
	Land forces properly organized, trained, and equipped for CBRNE defense and domestic CM.	Defense Support to Civil Authorities	All
		Protection	WMD Threat
	Organized, trained, and equipped forces able to detect, assess, contain, quarantine, evacuate, and provide force protection and medical surge capabilities.	Battlespace Awareness	All
		Interagency Coord	USG Integration
		Defense Support to Civil Authorities	All
		Logistics	Force Health Protection, Theater Logistics, Joint Deployment/Rapid Distribution
		Protection	WMD Threat, Terrorist Threat
	Robust and rapid response in coordination with other federal, state, and local agencies.	Battlespace Awareness	All
Interagency Coord		USG Integration	

CBRNE Event		Net-Centric Operations	All	
	Established DOD, interagency, and state and local partner policies and procedures for DIB protection.	Battlespace Awareness	All	
		Command and Control	All	
		Net-Centric Operations	All	
		Interagency Coord	USG Integration	
	DOD forces available in a timely and reliable manner and able to deploy rapidly and sustain themselves.	Logistics	Joint Deployment and Rapid Distribution	
		Command and Control	All	
		Interagency Coord	USG Integration	
	Standardized CBRNE training programs between DOD and non-DOD partners.	Command and Control	Develop Shared SA and Understanding	
		Interagency Coord	USG Integration	
	DIB	Effective and timely identification of natural and manmade threats to the Homeland to protect the DIB.	Battlespace Awareness	All
			Interagency Coord	USG Integration; Intergovernmental Coordination
Established DOD, interagency, state, and local partner policies and procedures for DIB protection.		Net-Centric Operations	All	
		Interagency Coord	USG Integration	
Accurate development of vulnerability assessments and risk management strategies designed to prevent, and if necessary, reduce the consequences of failures, whether caused by natural or man-made disasters.		Net-Centric Operations	All	
		Defense Support of Civil Authorities	Emergency Preparedness	
		Protection	Physical Security, Threat Reduction and Cooperation	
		Interagency Coord	USG Integration	
Successful detection, accurate identification, and timely response to physical and cyber		Battlespace Awareness	All	
	Information Operations	Computer Network		

Cyber Support	threats.		Operations	
		Command and Control	Develop Shared SA and Understanding	
		Net-Centric Operations	All	
		Interagency Coord	USG Integration	
		Homeland Defense	Air and Space Defense	
	Established DOD and interagency policies, procedures, and doctrine for physical and cyber security.	Net-Centric Operations	All	
		Interagency Coord	USG Integration	
		Shared information on cyber threats to protect DIB and critical infrastructure.	Net-Centric Operations	All
			Interagency Coord	USG Integration
EP	Rapid crisis planning at the federal, state, and local level.	Command and Control	Develop Shared SA and Understanding	
		Defense Support to Civil Authorities	Emergency Preparedness	
		Net-Centric Operations	All	
		Interagency Coord	USG Integration	
	Shared intelligence at the federal, state, and local level.	Net-Centric Operations	All	
		Battlespace Awareness	All	
		Interagency Coord	USG Integration	
	Established policies and procedures to enable and facilitate continuous and effective operations during transition between LFAs.	Command and Control	Develop Shared SA and Understanding	
		Net-Centric Operations	All	
		Defense Support to Civil Authorities	Emergency Preparedness	
		Interagency Coord	USG Integration	
	Natural Disasters and	DOD forces and assets prepared to respond	Command and Control	All

Catastrophic Events	quickly and appropriately in the event of overwhelming natural disasters and catastrophic events in a supporting or supported role.	Defense Support to Civil Authorities	All
		Net-Centric Operations	All
		Logistics	All
		Interagency Coord	USG Integration
Inter-agency Partners	Enhanced unified action between DOD and Interagency partners at the operational level providing rapid response to HD, CS, and EP planning activities.	Command and Control	All
		Defense Support to Civil Authorities	All
		Net-Centric Operations	All
		Interagency Coord	USG Integration
Strategic Communication	DOD prepared to operate in a supporting, or as directed, a supported role.	Command and Control	All
		Shaping	Strategic Communications
		Public Affairs Operations	All
		Net-Centric Operations	All
		Interagency Coord	USG Integration
	Dedicated assets designed to improve communications, interoperability, and liaison through collaborative planning.	Command and Control	All
		Net-Centric Operations	All
		Interagency Coord	USG Integration

## **APPENDIX D: Concept Assessment and Experimentation**

Experimentation and assessment provide a disciplined, analytical, and iterative process to identify, explore and assess capabilities and proposed solutions. Experimentation remains a key component of DOD strategy for transformation. Active experimentation is critical to efforts to solve the significant challenges (near, mid, and far-term) faced by agencies and organizations conducting HD and CS operations.

Experimentation for HD and CS covers a range of activities and approaches. The range varies from discovery or concept development efforts to explore new issues, to controlled hypothesis testing studies, to demonstrations and testing of capabilities. Common throughout this range is the requirement to collect and examine data within a disciplined framework that supports generating insights or conclusions that are meaningful and valid. The range of efforts includes studies, table tops, exercises, wargames, modeling and simulation, Military Department and Joint advanced warfighting experiments, symposiums, seminars, and workshops, science and technology programs, and fielding of proven prototypes.

The ability to apply experimentation and assessment results to more than a narrow, specific issue or problem area requires use of accepted scenarios and conditions. Accordingly, the DOD HD and CS JOC experimentation program supports the DOD Joint Experimentation Campaign Plan and uses the campaign environments detailed in the JOC as the defining framework. In general, Defense Planning Scenarios are the basis for deriving specific scenarios to support Joint experimentation.

Experimentation activities throughout DOD have informed the development of the DOD HD and CS JOC by exploring how the USG and DOD develop strategy, prepare plans, and conduct operations to meet the challenge of securing the Homeland. Study findings of the Center for Strategic and International Studies on Beyond Goldwater-Nichols and Unified Quests 05 and 06 experimentation contributed to the development of a National Security Campaign Framework and ultimately the concept of a National Homeland Security Plan. The Joint Urban Warrior 2005 and 2006 wargames, co-sponsored by the US Marine Corps and USJFCOM, explored operational, organizational, and command relationship approaches to the conduct of Joint, Combined, and Interagency operations in an urban environment in the Forward Regions. These wargames reaffirmed the necessity for an active, layered defense of the Homeland where interagency and multi-national unity of effort are critical to detecting, deterring, preventing, or if necessary defeating threats in the Forward Regions. The 2012 Multi-Service Force Deployment for Homeland Defense used the DOD HLS JOC (Version 1.0)

as its primary source document providing analysts with a basis from which to perform analysis on HD and CS issues. Maritime Homeland Security and Homeland Defense Wargames reinforced the importance of multi-national coordination in both the Approaches and the Homeland to enhance plans and operations, specifically Strategic Communication Plans. Additionally, the DOD HD and CS JOC has drawn from multiple table top exercises, interagency exercises, and symposiums on topics such as HD, HS, maritime interception, missile defense, bioterrorism, and information sharing.

Since approval of the DOD HLS JOC (Version 1.0), efforts to secure the Homeland have led to increased appreciation of the levels of complexity and difficulty inherent in the mission. Experimentation is a tool for understanding and addressing that challenge. Some areas requiring focused attention are clear. For example, “interagency” experimentation may help DOD and the USG identify and eliminate unforeseen capability gaps in securing the Homeland. Other areas include the need to examine relationships, capabilities, and responsibilities within DOD, between combatant commands, and with and between supporting agencies. The DOD HD and CS JOC underscores the need to go beyond Joint experimentation and expand to the Interagency environment to include local, tribal, and state actor involvement. The desired end state, effects, and required capabilities will continue to be validated through experimentation and assessment.

## **APPENDIX E: HD and CS Illustrative Vignettes**

### **Purpose**

These illustrative vignettes demonstrate potential traditional, irregular, catastrophic, and disruptive threats to the security of the US Homeland in the 2012 - 2025 timeframe. The intent is not to reach a natural conclusion to any of the threat actions or events portrayed but to demonstrate key implications for the Joint Force, especially with regard to future capabilities DOD should possess. These vignettes also highlight challenges discussed in the DOD HD and CS JOC and illustrate the criticality of an active, layered defense that ensures DOD's mission of detecting, deterring, preventing, or if necessary defeating attacks as far from the Homeland as possible. The vignettes also relate the desired end state and effects identified in this concept to possible threat scenarios.

### **Vignette 1**

#### **Setting**

This illustrative vignette begins in the Forward Regions with a country in Central Asia that recently experienced an insurrection wherein religious fundamentalists, with minor support from elements in the armed forces, gain state control. This country possesses both Intermediate Range Ballistic Missiles (IRBMs) and nuclear weapons (Note: Intelligence indicates they only possess IRBMs and are incapable of directly targeting the US). Within 72 hours the newly established fundamentalist council obtains full access to these capabilities. This country has been known to support several terrorist organizations in the region openly. Additionally, both this country and these terrorist organizations are extremely belligerent toward the United States and its policies, allies, and regional presence. The fundamentalists initially concern themselves with the coalescence of power within the state and refrain from bellicose or antagonistic statements directed at the United States or the international community in response to their preliminary protests.

#### **Actions / Events**

Without warning, (24 hours after radical fundamentalists gain complete control of the nuclear weapons and their associated delivery vehicles) they launch a single IRBM. Initial US early warning capabilities instantly relay this information to USSTRATCOM to determine the trajectory and proposed impact. Geographic Combatant Commanders assess if their AOR is under attack (NORAD makes the assessment for North America) and prepare for a possible missile defense response. The

USSTRATCOM commander, prepares potential strategic response options.

As the missile exits the atmosphere a nuclear explosion is detected at 900 kilometers altitude in Low Earth Orbit (LEO). The blast disperses X-rays, gamma rays, and high-energy neutrons which disable satellites within the explosion's line-of-sight if they were not previously hardened against ionized radiation. After the blast, residual high-energy radiation particles propagate in LEO, encircling the Earth's magnetic field with additional radiation belts capable of disabling additional non-hardened satellites within LEO in a matter of weeks. Unstable nuclear fission fragments decay, emitting electrons that are trapped in earth's magnetic field. This greatly increases ambient radiation in LEO and could cause it to remain contaminated for up to two years. Exacerbating the situation is the US military's continued heavy reliance on space-based assets which, coupled with fiscal restraints, has forced the Joint Force to supplement their capability with commercial space-based assets. The high cost associated with payload orbital launches has dissuaded most commercial entities from embracing additional tonnage in the form of radiation hardening. Subsequently, these commercial satellites will be increasingly unavailable to the Joint Force as they continue to degrade.

The United States is unable to determine the missile's projected target and is uncertain whether the nuclear detonation was a premature malfunction or a direct attack. The United States requires additional information before it can assess and respond appropriately.

A communiqué is received by the US Department of State from the fundamentalists stating that the nuclear detonation was a demonstration to show their capability to attack. They assert that they are capable of launching similar attacks against US bases of operation in the Middle East, US allies in the region, and against specific oil production centers. They demand that the United States completely withdraw its military presence from the region, discontinue its support of local allies, and disengage itself from diplomatic and economic endeavors in the Middle East. The radical fundamentalists stress that if the United States fails to comply, or more importantly, employs a military response to this ultimatum, then the United States would be subjected to pervasive measures against its Homeland in addition to the execution of the threats levied above.



## Vignette 2

### Setting

A country in East Asia possesses both a limited ICBM arsenal and nuclear weapons capability. It also possesses an undetermined number of tactical nuclear weapons. In addition to these formidable weapons, it boasts a large, yet antiquated, conventional force. This country has been a destabilizing force in the region for decades but has not sought to upend the status quo due in large part to a sizable US military contingent located in an adjacent state and the backing of other regional allies by the United States. The country has continually sought leverage to eject US forces from such close proximity and re-establish national homogeneity, including the annexation of adjacent country territory. It is capable of launching an initial assault with only a few days preparation, but sustained operations will require the employment of a sizeable logistics system.

### Actions / Events

Leaders of the East Asian country identify an opportunity to realize their regional prerogatives. They quickly launch a large military assault across the border into adjacent country territory. They enjoy a sizeable advantage in heavy weaponry, special operations forces, and the number of personnel it employs in its armed forces. The adjacent country's defenses are quickly overrun at the border, although a defensive perimeter begins to solidify once US units are employed.

Leaders of the country recognize the inevitability of a loss if the United States is allowed to reinforce and direct its assets toward the fight. They have attacked at a point when the United States is dealing with a major crisis with another rogue state in Central Asia, and while the United States is experiencing a systematic failure of a large portion of the space-based assets upon which it has grown reliant. In addition to capitalizing on the current situation and events, they deliver a staunch warning to the United States that they will respond to any attempts at escalation with nuclear weapons. This country is capable of delivering 15 nuclear warheads via ICBMs to urban centers in the Western United States. Although the US Ballistic Missile Defense System (BMDS) has been operational for more than a decade, defeating 15 ICBMs would potentially be beyond the BMDS' capability, especially considering the possible degradation of early warning by a LEO nuclear detonation. These 15 ICBMs are housed in hardened silos dispersed throughout a mountainous region. Furthermore, leaders of this country have

threatened to widen the conventional war by using tactical nuclear weapons against the Joint Force and its allies if the United States attempts to target and destroy its ICBM silos.

The belligerents will attempt to overrun US and adjacent country positions, degrade interior infrastructure via Special Operations Forces insertion, and seek adjacent country capitulation before adequate missile defense assets can be focused in the “forward” and “approach zones”. They fully comprehend that ability to hold US population centers hostage via ballistic missiles is pivotal to realizing ambitions in the region. They will issue both general and overt threats against regional states that host US forward bases in an attempt to stymie US support to its besieged forces in adjacent countries. Additionally, they have instigated cybernetic attacks geared toward the distribution of false information to the American public. Their hackers gained access to several federal websites and inserted misinformation into sites dedicated to public information consumption. This has precipitated broad-spectrum confusion and increased public pressure on the administration.

### **Vignette 3**

#### **Setting**

A terrorist group has become exceedingly proficient in its sleeper cell placement within the United States and Europe. These cells constitute an ethnically diverse composition different from their singularly Arab predecessors. Though the group’s methods and character have necessarily changed, it still adheres to the ideological concepts associated with radical religious fundamentalism. The group has operated terrorist training outposts in the sparsely populated areas of an adjacent country sympathetic to their ideals. The group benefited from direct materiel and financial assistance from that country. With prior knowledge of an impending insurrection attempt by another country in the region, the group will use its established assets located in the United States and abroad to facilitate US acquiescence to their demands. It is suspected that they possess both the propensity and capability to use biological weapons. They seek to perpetrate a demonstrative attack on the US Homeland while reserving the capability to carry out additional, escalatory assaults.

#### **Actions / Events**

The terrorist group, exploiting a pre-positioned sleeper cell, initiates a biological attack on commuter trains in Washington, DC. They use a non-contagious biological pathogen that will shut down the transportation system in the Nation’s capital and significantly tax the

city's first-response, medical, and law enforcement assets. Responders find themselves wearing full protective gear for days, not hours. It is possible that in excess of a thousand people have been infected and the metro system will remain contaminated for quite some time. MSCLEA will likely be necessary in the National Capital Region to assist with CM and preclude possible civil disturbances stemming from population panic.

The terrorist group also owns and operates two large vessels off the US West Coast, and over the course of the last few years, they have concealed the vessels' intent and ownership by engaging them in legitimate commerce. During the last several weeks the group has successfully deployed a single land attack cruise missile and the necessary launch equipment onto each of these vessels without being detected by US intelligence or maritime forces. The cruise missiles are relatively low-technology weapons in comparison to those employed in military arsenals in the 2012 - 2025 timeframe. The terrorists plan to launch two land attack cruise missiles equipped with spray tanks to disseminate a particular biological pathogen (one at San Francisco and one at Los Angeles). The two vessels are loitering several miles off the coastline awaiting instruction. If no command is received within 5 days, the vessels will launch their payloads. Loitering any longer would likely subject them to scrutiny by US maritime patrols, which could compromise their intended attack. The cruise missile attacks will be launched under the most favorable weather and time of day conditions possible within the timeframe provided in order to maximize the effectiveness of the biological pathogens being used.

#### **Vignette 4**

##### **Setting**

A terrorist group has established a sleeper cell in the US Midwest. Members of this cell have integrated themselves into the central Illinois agricultural community. Consequently, they have gained access to small crop-dusting airplanes capable of disseminating pathogens by aerosol. If the United States does not acquiesce to their demands, they will use two planes to enter St. Louis airspace and spray an extremely contagious pathogen on the general downtown population during lunchtime.

##### **Actions / Events**

The planes will approach close to the ground to avoid initial radar detection, and they will approach from different vectors in order to increase their chance for success. The attacks will be launched under the most favorable weather and time of day conditions possible within

the timeframe provided in order to maximize the effectiveness of the biological pathogens being used. An attack with this particular pathogen would be difficult to quarantine, would likely cause significant casualties, and would certainly cause panic and potential population flight from St. Louis and other cities. MSCLEA will likely be necessary in the region to maintain quarantine zones to prevent a possible nation-wide pandemic, assist with CM, and preclude possible civil disturbances stemming from population panic.

An additional scenario that could require DOD support to civil authorities includes threats to the Homeland from natural disasters such as major Category 5 hurricanes or earthquakes. In these situations, DOD must be prepared to provide support to local and state authorities if the situation exceeds or overwhelms local and state assets or, if so directed, assume lead responsibilities. Adversaries may capitalize on these natural catastrophes within the Homeland to further their ambitions and goals.

### **Implications by Operational Capability**

As depicted in these illustrative vignettes, effective implementation of the active, layered defense strategy presented in this JOC could require DOD assets to address threats and aggression in not only the Forward Regions and Approaches, but also in support of civilian authorities in the Homeland. This commitment of DOD assets in multiple regions could occur simultaneously. To illustrate further the possible implications for DOD, this JOC will now address additional circumstances (by required capability) that could affect DOD's HD and CS missions. This section is designed to facilitate a better understanding of the desired end state and effects identified in this concept and their linkage with the associated broad operational capabilities needed for the Joint Force in ensuring a concerted national effort to detect, deter, prevent, or, if necessary, defeat attacks on the Homeland.

**Capability:** Project power to defend the Homeland.

- The Joint Force's ability to project power may be affected if enemy actors threaten to use CBRNE either against regional targets or the Homeland itself.
- Anti-access efforts by would-be aggressors could limit the Joint Force's ability to project power to the degree necessary to safeguard the Homeland.
- Disruptions to United States space assets, either by direct attack, jamming, or cyber attack, could reduce the Joint Force's ability to project power or degrade certain enabling capabilities.

- Dispersed terrorist organizations could present a predicament for the US in that these organizations are difficult to defend against, particularly by normal conventional methods. The persistent application of focused preventive and preemptive measures will remain the primary means of countering these foes.

**Capability:** Detect, deter, prevent (including through preemptive attack), or, if necessary, defeat potential threats to the Homeland as they arise in the Forward Regions and / or Approaches.

- Upper atmospheric nuclear blasts could hinder Joint Force communications and remote sensing capabilities in forward regions either from the initial blast, the electro-magnetic pulse, or the mid-term effects of residual radiation.
- Direct WMD threats or attacks against the Joint Force itself could hinder its ability to act.
- The Joint Force could be overly stretched if a sudden major conflict erupts. Defeating that adversary will require the reallocation of resources, personnel, and materiel from other engagements.
- Multiple events abroad could compromise the Joint Force's ability to respond effectively and cause the United States to prioritize threats incorrectly based on limited information and intelligence.
- Regime change could lead to extreme ideological state actors, which would increase the threshold for deterrence operations for the Joint Force.

**Capability:** Detect, deter, prevent, or, if necessary, defeat hostile space systems threatening the Homeland.

- The aggressors do not possess space-based weapon systems, but they do use space assets that both support and enable their existing capabilities (such space-based assets include GPS, communications, and imaging). It is likely that these space assets are not singularly owned and operated by the aggressors. Most countries will engage in joint space endeavors. As a result, the United States must be selective when attempting to jam, disrupt, or destroy enemy space systems that may be owned or operated by other states or international organizations.

**Capability:** Detect, deter, prevent, or, if necessary, defeat ballistic missile threats to the Homeland.

- The initial nuclear blast in LEO could have an adverse effect on both space-based early warning and tracking systems for missile defense applications. This could also hinder US tracking of mobile launchers.

- A missile defense system for the Homeland could be overwhelmed if an aggressor has the capability to launch 15 ICBMs at US Homeland targets.
- Theater missile defenses will be important in the face of threats by aggressors who possess WMD-armed ballistic missiles. Multiple military engagements around the world could reduce the number of theater missile defense assets available to each region.
- Overt ballistic missile threats against the United States could take the form of a deterrent umbrella under which the enemy can execute conventional military actions.

**Capability:** Detect, deter, prevent, or, if necessary, defeat maritime threats to the Homeland.

- Responding to maritime threats will require considerable interaction and coordination between DOD assets and law enforcement maritime capabilities, particularly the US Coast Guard. The water that surrounds the United States provides a plethora of routes for potential aggressors. DOD and law enforcement agencies must work together to secure not only the US Homeland against maritime threats but its commercial interests as well.
- Degraded space-based capabilities could affect communications and other tools necessary for cohesive defense.
- Increased global conflicts could require a greater operational tempo for warships outside US regional waters. As a consequence, additional responsibilities will fall on law enforcement maritime assets to secure US littoral waters (normal scrutiny and interception activities performed by the US Navy in the Approaches could be reduced).

**Capability:** Detect, deter, prevent, or, if necessary, defeat airborne threats to the Homeland.

- Early warning systems will have little time to react to cruise missile threats originating from the Approaches. Identifying potential cruise missile platforms at sea will continue to be a difficult undertaking.
- Degraded or insufficient sensor capabilities to provide surveillance of the Homeland, particularly detection of low radar cross section or low altitude airborne objects, coupled with less than 100% reliability in assessing intent of airborne tracks could affect DOD's ability to detect, deter, prevent, or, if necessary, defeat airborne threats to the Homeland.

- Responsibility for assessing and addressing vessels close to the US shoreline will require considerable interaction and coordination between DOD assets and law enforcement maritime capabilities.
- Small civilian aircraft in the United States are a potential problem due to the large numbers within the US airspace. Identifying two small aggressors among all in-air contacts could be problematic. Close cooperation and coordination with the Federal Aviation Agency will be necessary. Commercial and civilian airspace radars and monitors must be able to relay suspicious aircraft information to DOD's attention quickly in order to allow the necessary time for analysis and reaction.
- Degraded space-based capabilities could affect communications and other tools necessary for cohesive defense.
- The Joint Force must be responsive to emerging developments and maintain the ability to synchronize all assets against potential airborne threats. An integrated air picture will be necessary, including civilian and DOD assets.

**Capability:** Detect, deter, prevent, or, if necessary, defeat land threats to the Homeland.

- Cooperation among several intelligence assets is imperative to prevent further attacks on the Homeland.
- Increased border control may need to be pursued. This endeavor would require significant interaction, coordination, and cooperation among law enforcement and DOD assets.
- Responders could find themselves ill prepared to operate in a contaminated environment for long periods of time. Immediate medical care for attack victims may require medical facilities (including DOD medical units) to be established in close proximity to the contamination zone.
- DOD is able to provide certain capabilities, such as biological and chemical detection and reaction assets, which may be in short supply to civilian counterparts. Positioning and posturing of CBRNE equipment, supplies, and units are key considerations in a DOD response.
- The pending landfall of the major hurricane could further tax DOD forces and assets, if required in support of state and local efforts, and affect DOD's ability to conduct concurrent actions to address military threats in the Forward Regions and the Homeland.

**Capability:** Detect, deter, prevent, or if necessary defeat physical and cyber threats to DOD assets in the Homeland.

- The intentional distribution of misinformation by aggressors via DOD cyber access could compound problems in the Homeland

during times of threat. Managing accurate information to the public and other agencies is a fundamental need during a crisis. A disruption to the flow of accurate information could incite panic, cause the misdirection of vital resources, and potentially compound the effectiveness of an aggressor's attack.

- Degraded space-based capabilities could affect communications and other tools necessary for cohesive defense. A direct attack on DOD computer networks could hamper DOD and its interagency partner efforts to communicate and coordinate defensive / and or offensive activities effectively. The effects of the LEO nuclear blast could further exacerbate this situation.

**Capability:** Collaborate with other federal, state, and local agencies; conduct or facilitate vulnerability assessments; and encourage risk management strategies to protect against and mitigate the effects of attacks against the DIB.

- Any serious terrorist threat to critical DIB capabilities will be of great concern to DOD, especially the loss or degradation of those that could directly affect/influence Joint Force warfighting capabilities. Immediate collaboration among DOD, DHS, DOJ, local and state authorities, as well as private industry will be required. The threat situation depicted in this example will automatically cause DOD to review current vulnerability assessments and risk management strategies and consider preserving any capability deemed to be at risk, especially those deemed vital to meeting current or planned national security requirements.
- Any successful attack against a critical DIB asset/capability could require not only actions to mitigate the effects of such an attack, but also DOD action to identify all potential alternative actions required to ensure national security requirements continue to be met.

**Capability:** Support USG strategic communication to dissuade and deter adversaries from attacking the Homeland.

- Effective DOD strategic communication will be crucial to informing adversaries of the effect and the cost of threat actions against the US, its allies, or other vital US interests. Strategic DOD communication also may prove to be instrumental in influencing non-adversarial countries. The United States must have secondary means, as well as policies, and procedures in place to ensure strategic communication is not hampered or interrupted by adversary actions.



**Capability:** Prepare for and mitigate the effects of multiple near-simultaneous CBRNE events.

- Threats or attacks against the Homeland, particularly biological attacks, will require considerable coordination among national and local law enforcement, first-responders, and DOD assets.
- DOD medical assets will need to be coordinated with local and state authorities to maximize their effectiveness in areas where CBRNE attacks have taken place.
- Biological attacks require an executable plan to quarantine both the area of attack and possibly the population within a certain radius due to the prospect of a spreading epidemic. It is unlikely that first-responders will be able to determine the pathogen type used. As a result, all precautions must be implemented. In large urban areas it may be necessary for the President to direct DOD to assist or take the lead in quarantining and decontaminating the affected zones.
- Responders could find themselves ill prepared to operate in a contaminated environment for extended periods. Likewise, immediate medical care for attack victims could be lacking requiring makeshift medical facilities (including DOD medical units) to be established in close proximity to the contamination zone.
- Depending on an attack's severity and scope, DOD could be directed to support a LFA with capabilities unique to DOD that can be used to mitigate and manage the consequences of a CBRNE attack.
- Additionally, if the scope of an attack proves to be too complex or devastating for federal, state, and / or local government efforts, then DOD could be tasked to provide the majority of the assets for the response in accordance with the appropriate Presidential directive.

**Capability:** Conduct HD and CS operations, and EP planning activities while operating as the LFA, providing support to another agency, and during transitions of responsibility.

- As the LFA for HD, DOD may need to assist with maritime security, mobile, redundant command centers, and CBRNE CM.
- The President, as Commander in Chief, could direct DOD to act as LFA in the case of overt aggression against the Homeland or to provide to majority of the assets for the response in the wake of a major catastrophic event where local and state assets are overwhelmed and citizen lives are in jeopardy. The on-site leadership must be empowered to take whatever actions are

deemed necessary and appropriate to ensure security of the Homeland, protect lives, and assist in CM activities.

- Communications could be hampered by a LEO nuclear detonation. Law enforcement, DHS, and DOD will have to coordinate their actions in order to mitigate the effects of attacks to the Homeland, prevent additional follow-on assaults, and maintain the ability to transition responsibility during crisis situations.
- Any terrorist attack on the Homeland could quickly exceed first responder, state, and federal capabilities, thus requiring immediate action by DOD. In these situations exceeding DHS capabilities, DHS and DOD will rely on established agreements, and overall policy and doctrine to facilitate and streamline rapid decisions and coordinate actions and supported / supporting roles and responsibilities among agencies.
- In clear cases of foreign aggression such as the threat of an incoming ICBM and other direct threats to national security, DOD will be directed to conduct HD operations necessary to defeat an attack.
- In the case of a biological attack, the formally designated LFA could be compromised resulting in DOD assuming temporary leadership responsibilities on-site.

THIS PAGE INTENTIONALLY LEFT BLANK



**Office of Primary Responsibility:**

Chief, USNORTHCOM Strategy and Policy Division  
Headquarters, US Northern Command  
250 Vandenberg Street, Suite B016  
Peterson AFB, Colorado 80914-3820

**Available at [www.dtic.mil/futurejointwarfare](http://www.dtic.mil/futurejointwarfare)**