HEADQUARTERS

UNITED STATES

STRATEGIC COMMAND

CDRUSSTRATCOM CONPLAN 8039-08 (U)

~~Classified By: Multiple Sources~~
~~Reason: 1.4 (a), (c), and (g)~~
~~Declassify On: Feb 2032~~

(INTENTIONALLY BLANK)

HEADQUARTERS, U.S. STRATEGIC COMMAND
OFFUTT AIR FORCE BASE NE 68113-6500
28 February 2008

USSTRATCOM CONPLAN 8039-08 (U)
Table of Contents (U)

55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75 (INTENTIONALLY BLANK)
76
77

HEADQUARTERS, U.S. STRATEGIC COMMAND
OFFUTT AIR FORCE BASE NE 68113-6500
28 February 2008

USSTRATCOM CONPLAN 8039-08 (U)
Letter of Transmittal (U)

SEE DISTRIBUTION (Annex Z)

1. (U) CDRUSSTRATCOM CONPLAN 8039-08, which provides for Cyberspace Operations, is attached.

2. (U) CONPLAN 8039-08 accomplishes the following:

(~~S//REL USA, AUS, GBR~~) Fulfills the (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(U) Establishes a common context providing linkages among operations in and through cyberspace and operations in all environments.
(U) Identifies threats and prioritizes planning efforts.
(U) (b)(1) Sec 1.7(e) it provides a methodology for
(b)(1) Sec 1.7(e)
(U) Provides a framework for structuring pre-planned authorities to execute tasks that generate desired effects in support of national objectives.

3. (U) Elements of this plan were coordinated with Service Components, Functional Components, and supporting agencies during preparation.

4. (U) Upon approval, CDRUSSTRATCOM CONPLAN 8039-08 supersedes previous versions of CDRUSSTRATCOM CONPLAN 8039.

5. (U) File this letter in front of the plan.

FOR THE COMMANDER:

//signed//

MARK H. OWEN
Brigadier General, USAF
Director, Plans and Policy

120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140 (INTENTIONALLY BLANK)
141

HEADQUARTERS, U.S. STRATEGIC COMMAND
OFFUTT AIR FORCE BASE NE 68113-6500
28 February 2008

USSTRATCOM CONPLAN 8039-08 (U)
Security Instructions & Record of Changes (U)

(U) Plan Title:

1. (U) The long title of this plan is CDRUSSTRATCOM CONPLAN 8039-08 CYBERSPACE OPERATIONS (U).

2. (U) The short title of this plan is CDRUSSTRATCOM CONPLAN 8039-08 (U).

3. (U) This document is classified SECRET//REL TO USA, AUS and GBR to protect information revealing operational plans of US military forces. CDRUSSTRATCOM CONPLAN 8039-08 must be disseminated only to those agencies and personnel whose official duties specifically require knowledge of the plan, including those required to develop supporting plans.

4. (U) This document contains information affecting the national defense of the United States within the meaning of the Espionage Laws, title 18, United States Code, sections 793 and 794. The transmission or revelation of information contained herein, in any manner, to an unauthorized person is prohibited by law.

5. (U) Reproduction of this document is authorized for official use only, in accordance with guidelines for reproduction of classified material outlined in Department of Defense (DOD) 5200.1-R, Information Security Program

RECORD OF CHANGES

Change Number	Copy Number	Date of Change	Date Posted	Posted By

178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198 (INTENTIONALLY BLANK)
199

HEADQUARTERS, U.S. STRATEGIC COMMAND
OFFUTT AIR FORCE BASE NE 68113-6500
28 February 2008

USSTRATCOM CONPLAN 8039-08 (U)
Classification Guidance (U)

SUBJECT REQUIRING PROTECTION:	**PROTECTION REQUIRED DURING:**			
	COA DEVELOP-MENT	EXEC-UTION PLANNING	IMPLEMEN-TATION	POST IMPLEMEN-TATION
(U) Plan Short Title	U	U	U	U
(U) Plan Long Title	U	U	U	U
(U) Cyberspace Terminology	S//REL	S//REL	S//REL	S//REL
(U) Threat Information	S//REL	S//REL	S//REL	S//REL
(U) Concept of Operations	S	S	S	S
(U) Classification Guide	S//REL	S//REL	U	U
(U) Communications effectiveness, sustainability, and limitations	S//REL	S//REL	U	U
(U) Command Arrangements and agreements	S//REL	S//REL	S//REL	S//REL
(U) Rules of Engagement (ROE)	S	S	S	S
(U) Assigned Areas of Operation and boundaries	S	S	S	S
(U) Key planning assumptions	S//REL	S//REL	S//REL	S//REL
(U) Operational constraints	S//REL	S//REL	S//REL	U

(INTENTIONALLY BLANK)

HEADQUARTERS U.S. STRATEGIC COMMAND
OFFUTT AFB NE 68113-6500
28 February 2008

USSTRATCOM CONPLAN 8039-08 (U)
Executive Summary (U)

1. (~~S~~) Situation.

a. (~~S~~) General. Commander, US Strategic Command (CDRUSSTRATCOM) CONPLAN 8039 CYBERSPACE OPERATIONS responds to Contingency Planning Guidance FY 05 and CJCSI 3110.01E (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (CONPLAN 8039 also responds to draft Guidance for Employment of the Forces 08 (GEF) and draft Joint Strategic Capabilities Plan FY 08.) The plan provides a concept for (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Further, CONPLAN 8039 provides cyberspace planners with a basis for (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) The plan's success hinges on close coordination among all Combatant Commanders, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) operations. To facilitate and expedite planning, the plan consolidates existing roles, responsibilities, authorities, and rules of engagement from existing policy and guidance, which require CDRUSSTRATCOM coordinate with affected DOD components. In short the plan (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Finally, a close working relationship with the interagency is critical throughout all phases of planning and execution, as the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

b. (~~S~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

The prosperity and security of our nation rely on (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) In short (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) security environment, CONPLAN 8039 supports the National Defense Strategy by providing (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

c. (~~S~~) Area of Concern. CDRUSSTRATCOM has no geographic area of responsibility (AOR) for normal operations (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) CDRUSSTRATCOM's area of interest (AOI) for military operations is global, particularly involving operations that transcend GCC boundaries. CDRUSSTRATCOM will work in full partnership with geographic combatant commanders (GCCs) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) CDRUSSTRATCOM must be prepared to support operations as directed by the President and Secretary of Defense (SECDEF) as well as to support other combatant commanders (CCDRs). Forces under CONPLAN 8039 (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

d. (~~S~~) Scope. CONPLAN 8039 is (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) When CONPLAN 8039 (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) For (b)(1) Sec 1.4(a) not currently covered in (b)(1) Sec 1.4(a) CONPLAN 8039 provides a framework for planning (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) This CONPLAN (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) effort among USSTRATCOM components. Since (b)(1) Sec 1.4(a) is collaboratively developed with

the GCCs, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) ensures unity of purpose with all (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(1) (U) (b)(1) Sec 1.7(e)

(a) (~~S~~) The purpose of (b)(1) Sec 1.4(a) is to provide national leadership (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Department of Defense (DOD) and US Government (USG) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b) (~~S~~) Comprehensive and tailored (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) combatant commands and interagency partners.

(c) (~~S~~) (b)(1) Sec 1.4(a) encompass a (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) USG policy, and reflects combatant command collaboration. These appendices translate (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) They also translate (b)(1) Sec 1.4(a)

(d) (~~S~~) Depending on the level of planning, each (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) requirements, tasks, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) and assessments of risk and effects.

e. (U) Friendly Forces.

(1) (U) Center of Gravity. For the purposes of CONPLAN 8039, COG analysis will cover CDRUSSTRATCOM's ability to conduct

operations in and through cyberspace. The US utilizes (b)(1) Sec 1.7(e)

(2) (U) Strength and Composition. CDRUSSTRATCOM has Combatant Command (Command Authority) (COCOM) for forces delineated in Forces for Unified Commands (FY 2006) and Global Force management Guidance (FY 2005). CDRUSSTRATCOM will plan with all forces reasonably deemed essential to meet objectives.

f. (~~S//Rel to USA, AUS, GBR~~) Legal Considerations. CONPLAN 8039 contemplates military actions (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) of US law, including the US Constitution, applicable US statutes, executive orders and regulations, the Law of Armed Conflict (LOAC), and applicable ROE. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

2. (~~S//Rel to USA, AUS, GBR~~) Mission.

a. (~~S//Rel to USA, AUS, GBR~~) Purpose. This concept plan provides a (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) In order to accomplish this, CONPLAN 8039 will perform the following four functions:

(1) (U) Provide context for a common planning structure by establishing linkages among cyberspace operations and operations in all environments.

(2) (~~S//Rel to USA, AUS, GBR~~) Provide methods to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(3) (~~S//Rel to USA, AUS, GBR~~) Clarify (b)(1) Sec 1.4(a) roles and responsibilities from existing guidance to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(4) (U) Describe operations and defense of the Global Information Grid

b. (~~S//Rel to USA, AUS, GBR~~) Mission Statement Commander, US Strategic Command (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) support of national and military objectives, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

*(U) Note: (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

c. (U) (b)(1) Sec 1.7(e) CONPLAN 8039 is designed to support (b)(1) Sec 1.7(e) derived from (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) in CONPLAN 8039. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) CONPLAN 8039 (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) CONPLAN 8039 also develops a structure for pre-planned authorities for (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(1) (S) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(2) (S) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(3) (S) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

3. (~~S~~) Execution.

a. (U) Commander's Intent. USSTRATCOM (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) three scenarios:

(1) (U) When CDRUSSTRATCOM is the supported commander for planning within the context of other STRATCOM plans (e.g. (b)(1) Sec 1.7(e) In this case, (b)(1) Sec 1.7(e)

(2) (U) When CDRUSSTRATCOM is a supporting commander for another combatant commander, effects and supporting activities in support of other plans will be derived via the applicable combatant commander plan. For timing and tempo of operations, USSTRATCOM's assigned forces will follow the phasing or planned construct resident in that plan.

(3) (U) When CDRUSSTRATCOM is the supported commander, CONPLAN 8039 (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

b. (~~S~~) Concept of Operations. This CONPLAN employs the JP 5-0 (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) in and through cyberspace. As necessary, and when required, USSTRATCOM will modify the (b)(1) Sec 1.4(a) reflect the concept of operations. The following paragraphs describe general activities that relate to (b)(1) Sec 1.4(a) These descriptions are general in nature and may or may not apply to all (b)(1) Sec 1.4(a) CONPLAN 8039 describes the (b)(1) Sec 1.4(a)

(~~S~~) It is essential that CONPLAN 8039 (b)(1) Sec 1.4(a) be utilized in concert with Geographic Combatant Commander (GCC) campaign plans. CONPLAN 8039 provides planning structure and context, but is not intended to address (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) CONPLAN 8039 is intended to serve as a tool for developing executable OPLANs and EXORDs. For planning purposes, the (b)(1) Sec 1.4(a) construct below allows for the systematic

arrangement of activities and tasks in a logical and anticipated sequence. Some activities from a given (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(1) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) When CONPLAN 8039 (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(2) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) When CONPLAN 8039 (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) both cyber and non-cyber, are available for planners to quickly bundle into COAs to present to decision makers.

(3) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Baseline (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Planning and options for (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) are developed and fielded as directed. (b)(1) Sec 1.4(a)

(4) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) achieve specified objectives. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(5) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(6) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

4. (U) Administration & Logistics.

a. (U) Concept of Support. Security, logistics, personnel and administrative support will be furnished by supporting commands in accordance with service directives, command arrangement agreements (CAAs), memoranda of understanding (MOU), Task Force (TF) operating instructions and the logistics concept for support operations outlined in CDRUSSTRATCOM plans and directives.

5. (U) Command & Control: Service cyberspace operations Command & Control (C2) structure, as it applies to USSTRATCOM and its components, (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
differently. See Annex J for C2 specifics regarding organizational structure expected (b)(1) Sec 1.7(e)
for command relationships by scenario.

HEADQUARTERS U.S. STRATEGIC COMMAND
OFFUTT AFB NE 68113-6500
28 February 2008

Terms of Reference
(U) CDR USSTRATCOM CONPLAN 8039-08

1. (U) Terms of Reference: Because of the relative newness of this warfare area, and due to a lack of consensus regarding terminology, failures in communication regarding cyberspace are common. The terms, phrases and figures below are intended to provide a usable, readily available and common vocabulary for the cyberspace planner. This listing is not intended to be all-inclusive or doctrinal, but rather to identify and reference doctrine where available, and to provide an explanation and common context for other terms used throughout this document.

- (U) Access: Sufficient level (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

- (U//~~FOUO~~) (b)(1) Sec 1.7(e) For the purposes of CONPLAN 8039, attacks (b)(1) Sec 1.7(e)

  - (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

  - (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

- (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

  - (b)(1) Sec 1.7(e)
  combination of such effects.
  - (b)(1) Sec 1.7(e)
  - (b)(1) Sec 1.7(e)
  - (b)(1) Sec 1.7(e)
  adversely affected.

- (U) Computer Network Defense Response Actions (CND-RAs, or RAs): RAs are deliberate, authorized measures or activities that protect and defend DOD computer systems and networks under attack or targeted for attack by adversary computer systems/networks. RAs extend DOD's layered defense-in-depth capabilities and increase DOD's ability to withstand adversary attacks. Objectives for using RAs include:

  - (b)(1) Sec 1.7(e)
  - (b)(1) Sec 1.7(e)
  - (b)(1) Sec 1.7(e)

  (b)(1) Sec 1.7(e)

- (U) Computer Network Operations (CNO): Comprised of computer network attack (CNA), computer network defense (CND), and related computer network exploitation enabling operations (CNE). (JP 3-13). Note that for the purposes of CONPLAN 8039, Computer Network Operations and its subcategories are considered as (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

- (U) Computer Network Attack (CNA): Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (JP 3-13)

- (U) Computer Network Defense (CND): Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks. (JP 6-0)

- (U) Computer Network Exploitation (CNE): Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. (JP 3-13)

– (U) Cross Domain Solution: An information assurance solution that provides the ability to manually and/or automatically access and/or transfer between two or more differing security domains. (CJCSI 6211.02b, DISN Policy, Responsibilities and Processes)

– (U) Cyber: Adjective form of cyberspace. Used as a modifier to create appropriate cyberspace related terms (cyber attack, cyber defense, cyber weapon, etc.)

– (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

- (b)(1) Sec 1.7(e)
-
-

– (U) Cyber Attack Weapon Characterization: The process of determining and documenting the effect producing mechanisms and assurance factors of cyber attack weapons. Characterization

includes aspects of CNA technical assurance evaluation, Operational Test and Evaluation (OT&E), risk/protection assessments, and other screening processes. The operational risk assessment of employing or releasing an offensive or defensive cyber weapon shall include risk factors addressing safety (which can also be global and public) and security (loss of a weapon or exposure of a leading edge capability). Answers the question: "What do I need to know about this weapon before I can use it?"

(b)(1) Sec 1.7(e)

- (S) (b)(1) Sec 1.4(a)
  (b)(1) Sec 1.4(a)

- (U) (b)(1) Sec 1.7(e) The extent to which the cyber
  (b)(1) Sec 1.7(e)

- (U) (b)(1) Sec 1.7(e) The manner in which a
  (b)(1) Sec 1.7(e)

- (U) (b)(1) Sec 1.7(e) A combination of one or more
  (b)(1) Sec 1.7(e)

- (U) (b)(1) Sec 1.7(e)
  (b)(1) Sec 1.7(e)

  - (b)(1) Sec 1.7(e)
  -

- (b)(1) Sec 1.7(e)

- (U) (b)(1) Sec 1.7(e) The process of taking an (b)(1) Sec 1.7(e)

- (U) Cyber Capability: A capability (e.g., device, weapon, tool, computer program, or technique), including any combination of software, firmware, and hardware designed specifically to create an effect in or through cyberspace. Not all cyber capabilities are weapons or potential weapons.

- (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

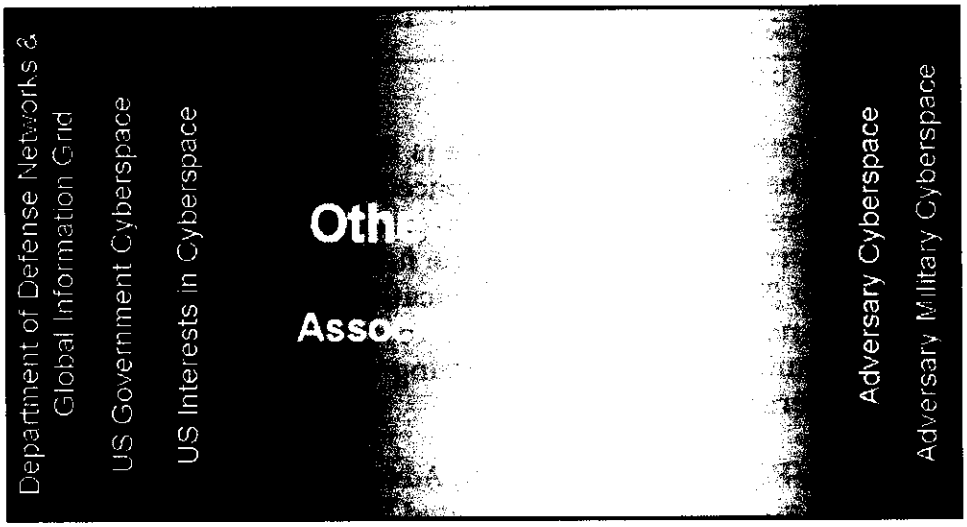
- (b)(1) Sec 1.4(a)

- (b)(1) Sec 1.4(a)

- (U) Cyberspace (working definition): A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. (working definition from NMS-CO)

- (U//~~FOUO~~) Cyberspace Defense: The goal of cyberspace defensive operations is to preserve the intended purpose and operating capabilities of a given network or system. Cyberspace defense is accomplished by a layered, defense-in-depth posture with mutually supporting elements of digital, electronic and physical protection. Critical infrastructure protection, Information Assurance and Computer Network Defense efforts all contribute to a robust defensive posture. Because of the extensive interconnections amongst networked systems, this variety of efforts supports protection of mission critical hardware and software, switching nodes, communications pathways and data integrity not only for critical Department of Defense networks, but also for portions of US, allied and civilian networks.

- (U) Cyberspace Domain: For the purposes of CONPLAN 8039, cyberspace is a domain using electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. (Per the NMS CO working definition of cyberspace)



(U) Figure 1: Cyberspace domain - Terrain

- (U) US Military Cyberspace: This is the area in Figure 1 delineated by the label "Department of Defense Networks & Global Information Grid". The GIG is as defined in Joint Publication (JP) 1-02. The GIG supports all DOD, national security, and related intelligence activities missions and functions (strategic, operational, and tactical), in war and in peace. DOD Networks span the full range from tactical battlefield data networks to networked strategic control systems.

- (U) US Cyberspace: This is the area in Figure 1 delineated by the label "US Government Cyberspace". Per the 2004 National Response Plan, all nationally owned cyberspace that resides outside of the DOD GIG is in this category and falls under the Department of Homeland Security (DHS) for protection. DHS responsibilities are detailed in the National Response Plan (NRP), 2004. This includes both U.S. owned and other U.S. government networks, across the full range of the interagency.

- (U) US Interests in Cyberspace: This is the area in Figure 1 delineated by the label "US Interests in Cyberspace". Networks and systems within this area are owned and operated by a variety of commercial, civil and other entities, however, the impact of their operation is of specific interest for the maintenance of national business operations. This category includes systems such as; (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) financial, commerce and utility networks.

- (U) Other Cyberspace: This is the area in Figure 1 delineated by the label "Other Cyberspace and Associated Infrastructure". The vast majority of cyberspace lies within this region. Included are the full spectrum of World Wide Web (WWW) accessible applications and services, as well as the necessary global infrastructure to support communication and processing of the data flow that enables cyberspace.

- (~~S//Rel to USA, AUS, GBR~~) Adversary Cyberspace: This is the area in Figure 1 delineated by the label "Adversary Cyberspace". Included are those portions of cyberspace (b)(1) Sec 1.4(a)

- (U) Adversary Military Cyberspace: This is the area in Figure 1 delineated by the label "Adversary Military Cyberspace". (b)(1) Sec 1.7(e)

– (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) 8039 characterizes (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

  - (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Comprised of:
    - (b)(1) Sec 1.4(a)
    -

  - (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) May require (b)(1) Sec 1.4(a) Comprised of:
    - (b)(1) Sec 1.4(a)
    -

  - (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) May require (b)(1) Sec 1.4(a) Comprised of:

- (b)(1) Sec 1.4(a)
-
-

Unclassified

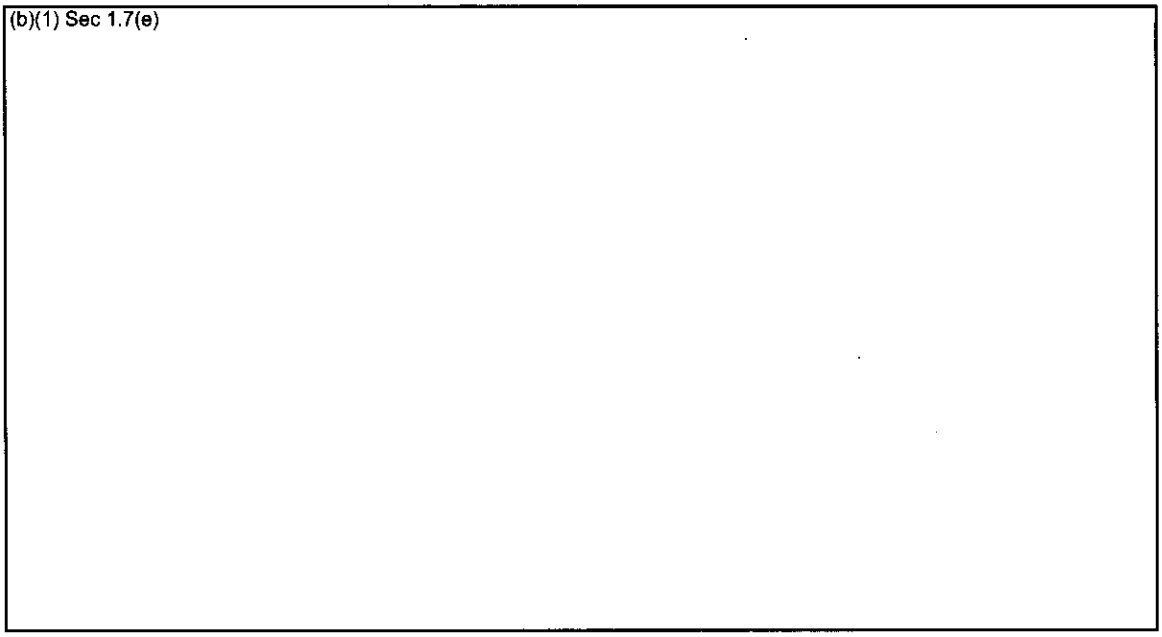


Figure 2: (U) Cyberspace (b)(1) Sec 1.7(e)

– (U) Cyberspace elements: For the purpose of CONPLAN 8039, there are four elements that comprise military use of cyberspace – Purpose, Infrastructure, Electromagnetic Spectrum, and Data. Arranging the elements of cyberspace into a cyber triangle (see Figure 3, below) helps to clarify the four separate, but related, aspects of cyberspace systems. After determining the desired objectives, effects, and actions, planners can use the triangle as a (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) Analysis of the cyber triangle can also guide the search for critical vulnerabilities.

UNCLASSIFIED

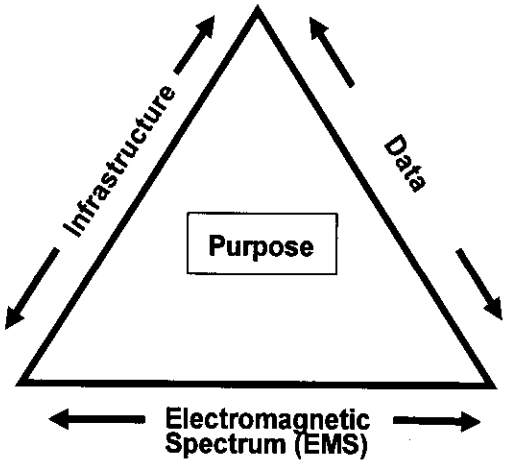


Figure 3: (U) Cyberspace Elements
The Cyber Triangle

- (U) Purpose. This central element represents the reason that an actor uses cyberspace to further his objectives. If an adversary doesn't see the value in using cyberspace to further his objectives hostile to the United States, his cyberspace capability (the rest of the cyber triangle) is not relevant. (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

- (U) Infrastructure. For the purposes of this plan, infrastructure includes the "global information infrastructure" as defined in JP 1-02 (see below) as well as

(b)(1) Sec 1.7(e)

- (U) Electromagnetic Spectrum (EMS). EMS refers to the range of frequencies of electromagnetic radiation from zero to infinity. It can be measured in cycles per second or wavelength in centimeters and includes radio waves, microwaves, and all forms of radiated energy.

- (U) Data: Representation of facts, concepts or instructions in a formalized manner suitable for communication, interpretation or processing by humans or automatic means. (JP 1-02) For the purposes of this plan, data refers to any such information that can be created, stored, modified, or exchanged via networked systems and associated infrastructure, as given in the NMS-CO.

– (U) Cyberspace Operations: Actions taken in, and extending through cyberspace, transcending Computer Network Operations (CNO). Cyberspace Operations broadly include the following objectives:

- (S) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)
- (S) (b)(1) Sec 1.4(a)
- (S) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

– (U) Cyberspace Superiority: The degree of dominance in cyberspace of one force over another that permits the conduct of operations by the former, and its related air, land, sea and space forces at a given time and place without prohibitive interference by the opposing force. (Adapted from: JP 3-13, 3-14, 3-30, Information, Space and Air Superiority)

– (U) Cyber Warfare: Direct creation of effects in and through cyberspace in support of a combatant commander's military objectives. Comprises operations conducted to guarantee friendly forces freedom of action in cyberspace while denying opposing forces effective use of cyberspace.

– (U) Data: Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned. (JP 1-02)

- For the purposes of CONPLAN 8039, data refers to any information, consistent with the above definition, which can be created, stored, modified, or exchanged via networked systems and associated infrastructure.

- (U) Deny: To degrade, disrupt, or destroy access to, operation of, or availability of a target by a specified level for a specified time. Denial is concerned with preventing adversary use of resources.

- (U) Degrade: (a function of amount) To deny access to or operation of a target to a level represented as a percentage of capacity. Level of degradation must be specified. If a specific time is required, it can be specified, otherwise start and stop-time are assumed to be indeterminate.

- (U) Destroy: To permanently, completely, and irreparably deny access to, or operation of, a target. Destruction is the denial effect where time and amount are both maximized.

- (U) Digital Protection: Actions taken in cyberspace to protect, defend, monitor, analyze, detect and respond to unauthorized network activity. It encompasses the concepts of Computer Network Defense (CND), Information Assurance (IA), and Response Actions (RAs).

- (U) Disrupt: (a function of time) To completely but temporarily deny access to or operation of a target for a period represented as a function of time. A desired start and stop time are normally specified. Disruption can be considered a special case of degradation where the degradation level selected is 100%.

- (U) Effects Assessment: The timely and accurate evaluation of effects resulting from the application of lethal or nonlethal force against a military objective. Effect assessment can be applied to the employment of all types of weapon systems (air, ground, naval, special forces, and cyber weapon systems) throughout the range of military operations. (b)(1) Sec 1.7(e) responsibility with required inputs and coordination from the operators. Effects assessment is composed of physical effect assessment, functional effect assessment, and target system assessment. Note: Battle Damage Assessment (BDA) is a specific type of effects assessment for damage effects. (Adapted from the JP 1-02 definition of BDA.)

- (U) Electronic Protection: Division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effect of friendly or enemy use of the electromagnetic spectrum that degrades, neutralizes, or destroys friendly combat capability. (JP 3-13.1)

- (U) Friendly Cyberspace: Those portions of cyberspace used, controlled, and/or maintained by entities understood to be non-hostile to the US, its allies, or coalition partners. For instance, the GIG, our military data links, and critical US cyber infrastructure are examples of friendly cyberspace.

- (U) Global Information Grid (GIG): The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems. Also called GIG. (JP 6-0)

- (U) Global Information Infrastructure (GII): The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure. Also called GII. (JP 3-13)

- (U) HVAC: Heating, Ventilation and Air Conditioning. An acronym used to describe equipment used to control the temperature and humidity of an enclosed space. HVAC systems are critical for the efficient operation of computer and network equipment to maintain their operating environment within required specifications.

- (U) Infrastructure: For the purposes of CONPLAN 8039, infrastructure is the superset of systems including the GII (see above) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

- (U) Intended Cyber Effect: A sorting of cyber capabilities into broad operational categories based on the outcomes they were designed to create. These categories are used to guide capability

selection decisions. Answers the question: "What kind of capability is this?" Specifically:

- Denial: degrade, disrupt, or destroy access to, operation, quality of service, or availability of target resources, processes, and/or data.
- (b)(1) Sec 1.7(e)
- Command and Control: provide operator control of deployed cyber capabilities.
- Information/Data Collection: obtain targeting information about targets or target environments.
- Access: establish unauthorized access to a target.
- Enabling: provide resources or create conditions that support the use of other capabilities.

– (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

– (U) Lethal: Causing death or permanent injuries to personnel.

– (U) Malware: Software designed to infiltrate or damage a computer system without the owner's informed consent. It is a combination of the words "malicious" and "software". The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

– (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

– (U) Misfire: The failure of a weapon to take its designed action; failure of a primer, propelling charge, transmitter, emitter, computer software, or other munitions component to properly function, wholly or in part. (Note: adapted from the JP 1-02 definition of misfire.)

- (U) Nonkinetic: Refers to actions which do not use forces of dynamic motion and/or energy upon material bodies. See (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

- (U) Nonlethal: Neutralizing or incapacitating a target without causing death or permanent injury to personnel. Nonlethal refers to being relatively reversible and is not required to have zero probability of causing fatalities or permanent injuries.

- (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

- (U) Physical protection: Preservation of the effectiveness and survivability of mission-related military and nonmilitary equipment, facilities, and infrastructure deployed or located within or outside the boundaries of a given area. (Adapted from JP 3-0)

- (U) Probability of Effect (PE): The chance of a specific functional or behavioral impact on a target given a weapon action.

- (U) Response Actions (RA): See "Computer Network Defense Response Actions" above.

- (U) (b)(1) Sec 1.7(e) acronym used to describe (b)(1) Sec 1.7(e) which are used to

(b)(1) Sec 1.7(e)

accessible internet.

- (U) Target State: The condition of a target described with respect to a military objective or set of objectives.

- (U) Targeted Vulnerability: An exploitable weakness in the target required by a specific weapon.

    - Objective Vulnerability: A vulnerability whose exploitation directly accomplishes part or all of an actual military objective.

    - Access Vulnerability: A vulnerability whose exploitation allows access to an objective vulnerability.

- (U) Weapon Action: The effect-producing mechanisms or functions initiated by a weapon when triggered. (e.g., the weapon actions of a kinetic weapon are blast, heat, fragmentation; (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

- (U) Weapon Effect: A direct or indirect (intended or unintended) outcome of a weapon action. In warfare, the actions of a weapon are employed to create intended effects, typically to the functional capabilities of a material or personnel target or to the behavior of individuals.

    - Direct Effect: An outcome that is immediately caused by the weapon's action. Also known as a first order effect.

    - Indirect Effect: An outcome that cascades from one or more direct effects; the outcome may be several degrees away from the direct effect but the direct effect must be the proximate cause of the eventual outcome. Also known as second order effects, third order effects, etc.

HEADQUARTERS, U.S. STRATEGIC COMMAND
OFFUTT AIR FORCE BASE NE 68113-6500
28 February 2008

USSTRATCOM CONPLAN 8039-08 (U)
Base Plan (U)

1. References:

a. U) CJCSM 3122.03C, Joint Operation Planning and Execution System (JOPES) Volume II, Planning Formats and Guidance, (Current as of 17 August 2007)

b. (U) CJCSM 3122.01, Joint Operation Planning and Execution System (JOPES) Volume I (Planning Policies and Procedures), 29 Sep 06 (Current as of 6 December 2007)

c. (U) CJCSI 3110.01F, Joint Strategic Capabilities Plan (TS), 1 Sep 06

d. (U) Joint Pub 1, Doctrine for the Armed Forces of the United States, 14 May 2007

e. (U) SM-712-89 Unified Command Plan (UCP) (S), 5 May 06

f. (U) Defense Planning Guidance (DPG), FY 2004-2009 (S), May 02

g. (U) CDRUSSTRATCOM Implementation Plan (IPLAN) for assuming the Computer Network Defense (CND) Mission, 14 May 99

h. (U) Draft Strategic Guidance Statement for Computer Network Operations (S), 24 Apr 06

i. (U) Computer Network Attack Implementation Plan (S//NF), 26 Jan 00

j. (U) Computer Network Attack Concept of Operations (S//NF), 30 Jun 00

k. (U) Delegation of Disclosure Authority Letter, National Disclosure Policy Committee Case No. 6005-00 – Multiple Countries (S), 7 Jun 00

l. (U) National Intelligence Estimate NIE 2004-01HC/I, Cyber Threats to the United States Information Infrastructure (S//NF), 15 Mar 04

m. (U) DODD 0-8530.1, Computer Network Defense (CND), 8 Jan 01

n. (U) CJCSM 3113.01A Series, "Theater Engagement Planning," 31 May 00 (current as of 25 May 05)

o. (U) CJCSI 3121.01B, Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces (S), 13 Jun 05 (Current as of 5 July 2007)

p. (U) APPENDIX 12 TO ANNEX C (OPERATIONS) TO JTF GNO OPORD 05-01 (Global Network Operations) INFORMATION OPERATIONS CONDITION (INFOCON) EXECUTION PROCEDURES (C//Rel USA, AUS, CAN, NZL), 22 May 06

q. (U) DODD O-8530.02, Support to Computer Network Defense, 9 Mar 01

r. (U) CJCS Homeland Security (HLS) Standing Execution Order (S//Rel USA, CAN) 161950Z OCT 01

s. (U) CJCS Strategic Plan, National Military Strategy Plan for the War on Terrorism, Revision 3 (TS), 032000Z Jan 2002

t. (U) Computer Network Defense (CND) Response Actions (RA) Concept of Operations (S), Draft as of 6 May 04

u. (U) Guidance for Computer Network Defense (CND) Response Actions (RA) Memorandum. Signed by (b)(6) (U//FOUO), 26 Feb 03

v. (U) Contingency Planning Guidance (CPG) 2005 (TS)

w. (U) National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996

x. (U) National Military Strategy for Cyberspace Operations (S), 11 Dec 06

y. (U) Quadrennial Defense Review (S), 6 Feb 2006

z. (U) SECDEF Memorandum, Assignment and Delegation of Authority to Director, Defense Information Systems Agency (DISA) (U//FOUO), 18 Jun 04

aa. (U) ASD 3CI Memorandum, DOD Guidance for Computer Network Defense Response Actions (U//FOUO), 26 Feb 03

bb. (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

cc. (U) Horizontal Command and Control (C2) Integration (HC2I) Concept of Operations (CONOPS) (S//Rel USA, AUS, CAN, NZL), 20 Dec 05

dd. (U) JTF-GNO OPORD 03-02 Reconnaissance and Surveillance and Computer Network Defense (U//FOUO), 25 Mar 04

ee. (U) CJCSM 6510.01, Defense in Depth: Information Assurance (IA) and Computer Network Defense (CND) (U//FOUO), 25 Mar 03. Including Ch 2, 26 Jan 06, Ch 3, 8 Mar 06, (Current as of 14 Aug 2006)

ff. (U) JTF-GNO OPORD 05-01, Global Network Operations (U//FOUO)

gg. (U) USSTRATCOM Planning Order (PLANORD) for Ongoing Computer Network Intrusion Activities (S//Rel USA, AUS, GBR), 17 Oct 2005

hh. (U) Amplification to JFCC NW PLANORD (S//Rel USA, AUS, GBR), 09 Mar 06

ii. (U) USSTRATCOM Joint Concept of Operations for Global Information Grid NETOPS, 4 Aug 06

jj. (U) Forces for Unified Commands Memorandum, FY06 (S), 13 Jan 06

kk. (U) Trilateral Memorandum of Agreement among the Department of Defense, the Justice Department and the Intelligence Community Regarding Computer Network Attack and Computer Network Exploitation Activities (DOD-JD-IC MOA) (S//NFS//NF), 9 May 07

ll. (U) Joint Task Force – Global Network Operations Implementing Directive, 5 Aug 05

mm. (U) Joint Functional Component Command – Network Warfare Implementing Directive, 20 Jan 05

nn. (U) USSTRATCOM Network Warfare CONOP (S/Rel USA, AUS, GBR), May 2006

oo. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (S), 7 Jul 04

pp. (U) 2003 National Strategy for Securing Cyberspace (NS-SC)

qq. (U) 2003 National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, Feb 03

rr. (U) 2004 National Response Plan (NRP) Dec 04

ss. (U) Joint Publication 3-13, Information Operations, 13 Feb 06

tt. (U) Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 12 April 2001 (As Amended Through 20 March 2006)

uu. (U) The Law of Armed Conflict, composed of International Agreements to which the United States is a party and Customary International Law binding on the United States

vv. (U) United States Code, Title 10, Armed Forces

ww. (U) United States Code, Title 18, Crimes and Criminal Procedure

xx. (U) United States Code, Title 50, War and National Defense

yy. (U) United States Code, Title 32, National Defense

zz. (U) SECDEF Delegation of Authority to Appoint the Person Serving as Director, National Security Agency, (DIRNSA) as Commander, Joint Functional Component Command for Network Warfare (JFCC NW) (S), 20 Jan 05

aaa. (U) Designation of the Director, Defense Information Systems Agency (DISA), as Commander, Joint Task Force-Global Network Operations (JTF-GNO), 17 Nov 05

bbb. (U) JFCC for Space Implementation Directive (U//FOUO), 19 Jul 06

ccc. (U) JFCC for Global Strike Integration (GSI) Implementation Directive (U//FOUO), 19 Jul 06

ddd. (U) JFCC IMD Implementation Directive (U//FOUO), 22 Jan 05

eee. (U) JFCC ISR Implementation Directive (U//FOUO), 24 Jan 05

fff. (U) Strategic Command Directive 527-1, DOD Information Operations Condition (INFOCON) System Procedures (U//FOUO), 27 Jan 06

ggg. (U) (U) CJCSM 3122.07A, IJSTO Supplement to Joint Operation Planning and Execution System (JOPES) (S//Rel USA, AUS, CAN GBR), 20 Oct 06

hhh. (U) Information Operations Roadmap (S//NF), 30 Oct 03

iii. (U) Doctrine for Joint Operation Planning, JP 5-0, 26 Dec 06

jjj. (U) (U) (b)(1) Sec 1.7(e) for CONPLAN 8039), updated semiannually (S//SI//NF)

kkk. (U) Joint Publication 3-0, Joint Operations, 17 Sep 06

lll. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) Sep 06

mmm. (U) 61JTCG/ME-1-8, Rev 1, Draft 2007, Requirements for Generating, Documentation, Reviewing, and Approving JTCG/ME Vulnerability Data.

nnn. (U) Deterrence Operations Joint Operating Concept, v 1.9, Jul 06

ooo. (U) Joint Publication 6-0, Joint Communications System, 20 Mar 06

ppp. (U) CJCSI 5810.01C Implementation of the DOD Law of War Program, 31 Jan 07

qqq. (U) USSTRATCOM Operational Concept for Cyberspace (OCC) (DRAFT 2008)

rrr. (S) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

1. (U) Situation

a. (U) General

(1) (U) This is the United States Strategic Command (USSTRATCOM) Concept Plan (CONPLAN) 8039 for Cyberspace Operations (CO). The strategic goal of CONPLAN 8039 is to ensure US military freedom of action in cyberspace and to be able to deny adversary freedom of action in cyberspace. To achieve this goal, (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) cyberspace, when directed. Additionally, the plan calls on (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) This plan is prepared and submitted in accordance with requirements detailed in references a and b, and supports the national interests outlined in references c through bq.

(2) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) The prosperity and security of our nation rely on cyberspace to achieve and maintain strategic advantage and strengthen the instruments of national power.

(3) (U) The scope of CONPLAN 8039 spans from peacetime through war fighting in and through cyberspace. It does not direct but must be able to (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

b. (U) Areas of Concern. For the purposes of CONPLAN 8039, cyberspace is a domain using electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures, per reference x. Treating cyberspace as a domain (see Terms of Reference) provides the "cyber-terrain" where 8039 operations will take place. Areas of concern per reference c are:

(1) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) this plan is considered to be (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) as described in the Terms of Reference (see Figure 1, Terms of Reference) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) by operations in cyberspace (see the Terms of Reference for more detailed discussion on the elements of cyberspace).

(2) (U) Operational Area (OA). The potential operational area for this plan is the entire cyberspace domain. The transregional, global nature of cyberspace (b)(1) Sec 1.7(e) operational area can (b)(1) Sec 1.7(e) and wherever the Commander is directed to advance and defend US interests in and through cyberspace. The operational area of the plan consists of both the:

- (b)(1) Sec 1.7(e) and
- (b)(1) Sec 1.7(e) as established by EXORD. For more information on cyber engagement criterion, see Concept of Operations below.

Mission execution for CONPLAN 8039 is (b)(1) Sec 1.7(e) objective driven, effects-based, and may be impacted from any of the (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (see Figure 1, Terms of Reference). For detailed discussion on each sub-area, see the 8039 Terms of Reference.

c. (U) Effects in cyberspace. Effects in cyberspace can be generated by influencing some or all of its elements, the constructs that support these elements, or its intended purpose. See the Terms of Reference for detailed discussion on the elements of cyberspace (cyberspace triangle).

d. (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Commander, USSTRATCOM will utilize (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Example (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) are in Annex A, Appendix 3. (b)(1) Sec 1.4(a) (as defined in the Terms of Reference) are presented in Annex C.

e. (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) DOD must retain (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(1) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(a) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) See Figure 4 (below).

1 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

3 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

Figure 4: (S//REL to USA, AUS, GBR)
(b)(1) Sec 1.4(a)

(b) (U) Operational. See (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(2) (U) Critical Factors.

(a) (U) Strategic.

1 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) These capabilities can be (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (as described in the Terms of Reference).

2 ~~(S//Rel to USA, AUS, GBR)~~ (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Ultimately, the goal of cyber warfare is to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Figure 3, Terms of Reference and Figure 5 below).

(b)(1) Sec 1.4(a)

Figure 5:
(S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

a ~~(S//Rel to USA, AUS, GBR)~~ (b)(1) Sec 1.4(a) In order to affect any element of cyberspace, the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) More detailed discussions on

(b)(1) Sec 1.4(a) are found in Annex C. More detailed discussions covering (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) can be found in Annexes B & C.

b (U) Defensive considerations. Optimally, actors attempt to gain and maintain confidence in their use (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) listed above). Operational planners (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) Generally as systems become larger and more complex there are more opportunities to exploit.

c (U) The following rules apply to this methodology:

(1) (U) Primacy of purpose. The focus of attack on any cyberspace system is to affect that system's intended purpose. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(2) (U) Cascading effects. Multiple attacks on varying elements can have cumulative effects and even a single attack can have cascading effects in, through and outside of the cyberspace domain.

d (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b) (U) Operational. See (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(3) (U) Courses of Action.

(a) (~~S//Rel to USA, AUS, GBR~~) General. Cyberspace threats are not limited to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) The general (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) with respect to their effort. The (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) However, those potential adversaries who (b)(1) Sec 1.4(a)

(c) (~~S//Rel to USA, AUS, GBR~~) Strategic Objectives. The principal strategic objectives of an adversary's offensive cyber operations are (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) This activity may fall into more than one category. See Annex B for a detailed discussion of adversary capabilities and general courses of action.

(d) (U) Operational Objectives. See (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) operational-level objectives.

f. (U) Friendly Forces.

(1) (U) Center of Gravity (COG).

(a) (~~S//Rel to USA, AUS, GBR~~) Strategic. For the purposes of CONPLAN 8039, COG analysis will cover CDRUSSTRATCOM's (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) COGs and critical capabilities based on analysis conducted per ref bk.

1 (U) Leadership. Represents those individuals within DOD who can influence critical missions and processes within cyberspace. Senior Leadership includes the President of the United States (POTUS), the SECDEF and those subordinate officers appointed by POTUS and SECDEF.

2 (U) Population. In this context is the aggregate of the US residents and their will to pursue national objectives and support leadership.

3 (U) Fielded Forces. Are those DOD forces/organizations who conduct military operations within cyberspace. Figure 6 (below) illustrates relationships between critical capabilities as crucial enablers for COGs.

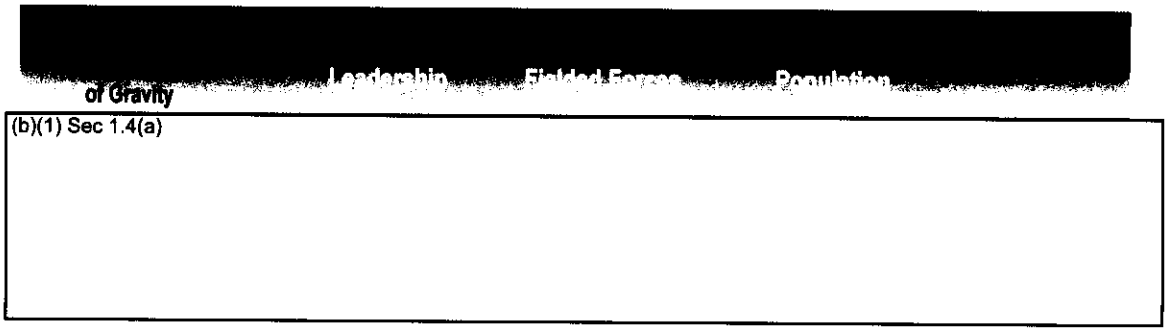


Figure 6: (~~S//REL to USA, AUS, GBR~~)
Friendly Center of Gravity

(b) (U) Operational. See Annex C for friendly operational-level COG analysis.

(2) (U) Critical Factors.

(a) (U) Strategic.

1 (~~S//Rel to USA, AUS, GBR~~) Friendly Critical Capabilities (CCs). The US utilizes cyberspace to enable the following functional critical capabilities (ref bk): (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (see Terms of Reference for cyberspace elements).

2 (~~S//Rel to USA, AUS, GBR~~) Friendly Critical Vulnerabilities (CVs). Friendly CVs are (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b) (U) Operational. More detailed blue force operational critical factor analysis will be conducted in Annex C.

(3) (U) Composition. Friendly forces consist of combatant commands (CCDRs), allies, services and agencies. Outside of DOD, the Computer Emergency Response Teams (CERTs) and the DHS, law enforcement agencies (LEAs), and counterintelligence (CI) organizations collectively provide, manage, and maintain cyberspace command, control, communications, computers, and intelligence (C4I) systems for the USG.

g. (~~S//Rel to USA, AUS, GBR~~) Assumptions.

(1) (S) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(2) (~~S//Rel to USA, AUS, GBR~~) Adversaries are and will (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(3) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(4) (~~S~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) adversary's objective

(5) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(6) (~~S//Rel to USA, AUS, GBR~~) Methods will be developed that can (b)(1) Sec 1.4(a)

(7) (U) Working relationships will exist with military and civilian Law Enforcement Agencies and Counterintelligence organizations to facilitate identification and apprehension of persons responsible for attacks and/or intrusions on DOD computers and DOD computer networks of the GIG.

(8) (~~S~~) The United States should (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) cyberspace operations.

(9) (U) Planning and conduct of cyberspace operations requires the integration of other elements of national power.

h. (U) Limitations.

(1) (U) Constraints.

(a) (U) Combatant commands will coordinate their planning with CDRUSSTRATCOM.

(b) (U) CDRUSSTRATCOM will coordinate planning with other combatant commanders.

(c) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(d) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) must be in compliance with US law and DOD Policy.

(2) (~~S//Rel to USA, AUS, GBR~~) Restraint. DOD (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

i. (U) Legal Considerations.

(1) (~~S//Rel to USA, AUS, GBR~~) CONPLAN 8039 contemplates military actions (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2. (~~S//Rel to USA, AUS, GBR~~) Mission. CDRUSSTRATCOM plans and directs integrated DOD operations in and through cyberspace (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

3. (U) Execution.

a. Concept of Operations.

(1) (~~S//Rel to USA, AUS, GBR~~) Purpose. The purpose of this plan is to provide a framework for cyberspace planning and to develop a structure for pre-planned authorities to conduct operations in and through cyberspace. Additionally, this plan (b)(1) Sec 1.4(a)

(2) (U) Method. The plan will:

(a) (U) Describe the operation and defense of the GIG.

(b) (U) Provide the context for a common planning structure.

(c) (U) Develop a system of RAs and Cyber Engagement Criteria for execution of pre-planned activities and authorities.

(d) (U) Clarify global vs. regional roles and responsibilities and lays out coordination methods and instructions.

(3) (~~S//Rel to USA, AUS, GBR~~) End-state. At the end state, the US (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Per refs v and x, CONPLAN 8039 will support the following termination criterion that support this end-state

(a) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(c) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(d) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(e) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(f) (~~S//Rel to USA, AUS, GBR~~) Cyberspace capabilities provide (b)(1) Sec 1.4(a)

(g) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(h) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(i) (U) Adversaries are deterred from establishing or employing offensive capabilities against US interests in cyberspace.

(j) (U) Adversaries who jeopardize US interests in cyberspace are defeated.

(k) (U) DOD is postured to support homeland security, critical infrastructure protection, and provide civil support.

(l) (U) US, allies, and coalition partners have freedom of action to operate in cyberspace.

b. (~~S//Rel to USA, AUS, GBR~~) General.

(1) (U) Common Context. In order to accomplish its UCP mandated cyberspace mission, outlined in ref e, CONPLAN 8039 establishes a common context with regard to cyberspace domain for military areas of operation and activities. This common context is established through the planning construct and the contents of the Terms of Reference.

(2) (U) Identify Threats and Prioritize Planning Efforts.

(a) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) plan. Combatant commanders who deviate from the (b)(1) Sec 1.7(e) will provide rationale to CJCS before developing courses of action.

(b) (~~S//NF~~) The United Sates information infrastructure is (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(c) (~~S//NF~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Rapid changes in technology, the integration of telecommunications and computer networks, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(3) (U) Plan (b)(1) Sec 1.7(e) CONPLAN 8039 will provide the methodology for cyberspace planning (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(U)(a) (~~S//Rel to USA, AUS, GBR~~) Actors. Broadly characterized as follows (excerpted and summarized from the National Institute of Standards and Technology (NIST) 800-82):

1 (U) National Governments/Foreign Intelligence Services. Characterized by sophisticated, well funded programs to develop cyber tools capable of causing a full spectrum of effects, from propaganda and low-level nuisance web page defacement to pervasive espionage, to widespread, long-duration damage to US critical interests and infrastructures.

2 (U) Terrorists. Characterized by a desire to destroy, incapacitate or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the US economy and damage public morale and confidence. Terrorists' cyber efforts are less sophisticated than nation states, but are increasingly dangerous and effective as their technical sophistication increases.

3 (U) Criminal groups. International organized crime and industrial espionage is less directly threatening to US security interests due to a focus on profit motive. Nonetheless, this category of actors presents a threat due to their ability to hire, develop and retain sophisticated talent and tools.

4 (U) Hacktivists. Hacktivists form a small, foreign population of politically active hackers that includes individuals and groups with anti-US motives. They pose a medium-level threat of carrying out an isolated but damaging attack. Most hacktivist groups appear bent on propaganda rather than damage to critical infrastructures. Their primary goal is to support political agendas with sub-goals of propaganda and causing damage to achieve notoriety for their cause.

5 (U) Hackers. This category includes a wide variety of sub-categories, including Phishers, Spamers, Spyware/Malware Authors, Script Kiddies and professional Black Hats. In general the large majority of hackers do not have sufficient talent to threaten difficult targets such as critical US and defense systems. Nonetheless, the large global population of hackers poses a relatively high threat of disruptions in a variety of networks and systems, with potential for property damage and loss of life. As the hacker population grows, so does the likelihood of an exceptionally skilled, lucky or malicious hacker attempting and succeeding in an extremely damaging attack.

(b) ~~(S//Rel to USA, AUS, GBR)~~ Scenarios. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) CONPLAN 8039 will draw upon the following to (b)(1) Sec 1.4(a) specific scenarios:

1 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) ref v (e.g. planning support to applicable USSTRATCOM CONPLANs/OPLANs, (b)(1) Sec 1.4(a) etc.).

2 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(c) (U) Objectives and (b)(1) Sec 1.7(e)

1 (U) For the purposes of this plan, CONPLAN 8039 will use the following (b)(1) Sec 1.7(e) derived from refs c, e, h, v and x.

a (S) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a). This also includes coordination with (b)(1) Sec 1.4(a) and the (b)(1) Sec 1.4(a) in securing US cyberspace in support of the respective Combatant Commanders.

b (S) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

c (S) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

2 (U) CONPLAN 8039 will support objectives and (b)(1) Sec 1.7(e) operations based on:

a (~~S//Rel to USA, AUS, GBR~~) When CDRUSSTRATCOM is the supported commander in response to a cyber threat, CONPLAN 8039 will provide the means to (b)(1) Sec 1.4(a)

b (~~S//Rel to USA, AUS, GBR~~) When CDRUSSTRATCOM is the supported commander for operations in and through cyberspace (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) cyber effects will be based on (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

c (~~S//Rel to USA, AUS, GBR~~) When CDRUSSTRATCOM is supporting commander to other Combatant Commanders, (b)(1) Sec 1.4(a) will provide supporting cyber effects based (b)(1) Sec 1.4(a) CONPLAN 8039. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) This also includes coordination (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a). For timing and tempo of operations, USSTRATCOM assigned cyber forces will follow the supported commander or agency's (b)(1) Sec 1.4(a) or planned construct.

d (~~S//Rel to USA, AUS, GBR~~) In order to successfully execute operations in and through cyberspace supported combatant commanders (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (objectives), and the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

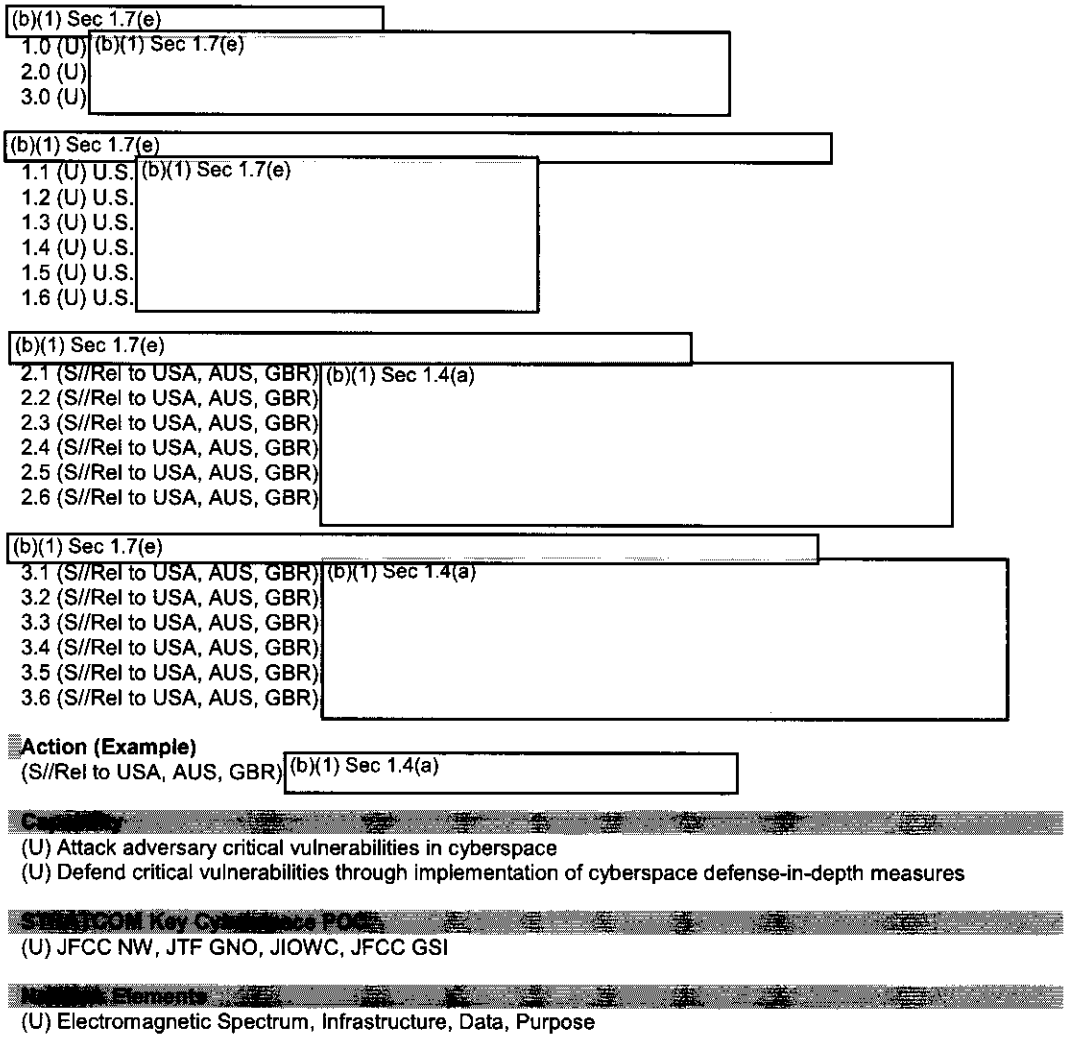


Figure 7: (~~S//Rel to USA, AUS, GBR~~) Synopsis of key CONPLAN 8039 execution concepts

(1) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) planners will consider
(b)(1) Sec 1.4(a)

(2) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) When planning in support of other plans, planners (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) as defined in ref O.

(3) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) When (b)(1) Sec 1.4(a)

e (U) Per ref bi, the supported commander plans joint operations based on analysis of national strategic objectives and development of theater objectives supported by (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(d) (U) Planning.

1 (~~S//Rel to USA, AUS, GBR~~) Planning will consider all (b)(1) Sec 1.4(a) and COA development. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Specific mission analysis and COA development will (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Further information on (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) and COA development can be found in Annex C and (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

2 (~~S//Rel to USA, AUS, GBR~~) Upon request for CONPLAN 8039 support, USSTRATCOM will collaborate with (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) commands /services/agencies (C/S/As) should be included in the planning process for coordination and deconfliction.

3 (~~S//Rel to USA, AUS, GBR~~) USSTRATCOM may request (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) to support objectives. In instances where another CCDR supported CDRUSSTRATCOM will facilitate this coordination. USSTRATCOM will work with the Office of the Secretary of Defense (OSD) and Joint Staff to garner (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

4 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) and will be approved via the EXORD that authorizes the supported operation or a separate EXORD, if needed. The criteria (b)(1) Sec 1.4(a) (see Figure 8, below) will be dependent upon:

(b)(1) Sec 1.4(a)

Figure 8: (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

*Note 1: (b)(1) Sec 1.4(a) can be found in the Terms of Reference.

*Note 2: Authorities listed are only exemplary in nature. Any
(b)(1) Sec 1.4(a)

*Note 3: Large X indicates (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) A need to use

(b)(1) Sec 1.4(a)

a (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) A more (b)(1) Sec 1.4(a) The planning effort must address the need for (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) that supports the access development of desired (b)(1) Sec 1.4(a)

b (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) will not normally require (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) t

c (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) see Terms of Reference. These definitions will be used when making a (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) within the purview of CONPLAN 8039. The probable (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

d (U) Authorities: The level of authority is generally (b)(1) Sec 1.7(e) engagement criteria; (b)(1) Sec 1.7(e) will normally be associated with (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) Independent of the scale of the

cyber engagement criteria, (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

e (~~S//Rel to USA, AUS, GBR~~) The engagement criteria (which encompasses the (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) will be delineated in the applicable EXORD. Within that EXORD, (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(4) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) CONPLAN 8039 will (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) in support of assigned objectives.

(a) (U) General.

1 (~~S//Rel~~) Upon plan approval and appropriate authorities granted via EXORD, CONPLAN 8039 will be used to (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) Operations will be coordinated with Combatant Commanders during the planning and execution phase to mitigate AOR/functional mission (s) impact.

2 (~~S//Rel~~) On order, CONPLAN 8039 will (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) and other numbered plans.

(b) (~~FOUO~~) Cyberspace desired effects.

1 (~~FOUO~~) (b)(1) Sec 1.7(e) This plan will define the range of effects in cyberspace by using (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) (see Terms of Reference).

2 (~~S//REL TO USA, AUS, GBR~~) To assist planners in building (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) (see Terms of Reference). (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) before a JFC must seek additional authorities. CONPLAN 8039 will use them as one of the components of the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) available to the JFC, but only by receiving specific permission from the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(c) (U) (b)(1) Sec 1.7(e) in cyberspace. In order to (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) in cyberspace, USSTRATCOM (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) These capabilities are all employed in support of the JFC.

1 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) CONPLAN 8039 recognizes there are (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) For prospective supported and supporting commands, USSTRATCOM has assigned component focal points for the (b)(1) Sec 1.4(a) in and through cyberspace. In each case, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Specific details outlining these supporting concepts and how each USSTRATCOM component (b)(1) Sec 1.4(a) CONPLAN 8039 can be found in Annex C.

2 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) This is accomplished by comparing the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) should be viewed as a way to
(b)(1) Sec 1.4(a)
planner must first understand the (b)(1) Sec 1.4(a) and then
(b)(1) Sec 1.4(a)

3 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
Planners should recommend the (b)(1) Sec 1.4(a)
types that (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) Commanders should ensure that these (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) In some cases, it may be
necessary to (b)(1) Sec 1.4(a)
to achieve the commander's objective. Again, it is
important to emphasize that (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(5) (U) Operations. As in the physical domains, (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) discussion and terminology can be
found in the Terms of Reference. This need for increasing
(b)(1) Sec 1.7(e)
usually require supplemental ROE (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) Exemplar supplemental ROE (b)(1) Sec 1.7(e)
(outside of ref o) are detailed in Annex J. Example
supplemental ROE for (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(a) (U) Supporting Command. USSTRATCOM will normally
(b)(1) Sec 1.7(e) as the supporting commander to other
CCDRs. USSTRATCOM will follow the (b)(1) Sec 1.7(e)
construct defined by the supported commander or activity
and employ cyber forces and execute operations in support
of plan objectives. General discussion on USSTRATCOM
cyberspace support is found in applicable USSTRATCOM
supporting CONPLANs. More detailed handling of these
activities will be captured in Annex C, (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(b) (U) Supported Command. When CDRUSSTRATCOM is designated the supported commander against cyber threat actors, CONPLAN 8039 will use the (b)(1) Sec 1.7(e) outlined in ref bi. See (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) but the process is situation dependent, and commanders have the flexibility to employ or recommend any appropriate, approved responses at any time.

(c) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) allows military commanders to develop (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

1 (~~S//Rel to USA, AUS, GBR~~) Process. Typically (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) If existing accesses to the (b)(1) Sec 1.4(a) are sufficient to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

2 (~~S//Rel to USA, AUS, GBR~~) Risk Relationship. When considering requesting or authorizing (b)(1) Sec 1.4(a) commanders should balance the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) relationship between (b)(1) Sec 1.4(a) commanders should consider (b)(1) Sec 1.4(a)

3 (~~S//Rel to USA, AUS, GBR~~) Authorities. IAW ref o, the authority to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) generally granted through an EXORD. When CDRUSSTRATCOM is the supported commander this authority maybe delegated to the JFCC NW Commander.

Further discussion of (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(d) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) See Figure 9, below, for a summary of (b)(1) Sec 1.4(a) discussed below. Each of the (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

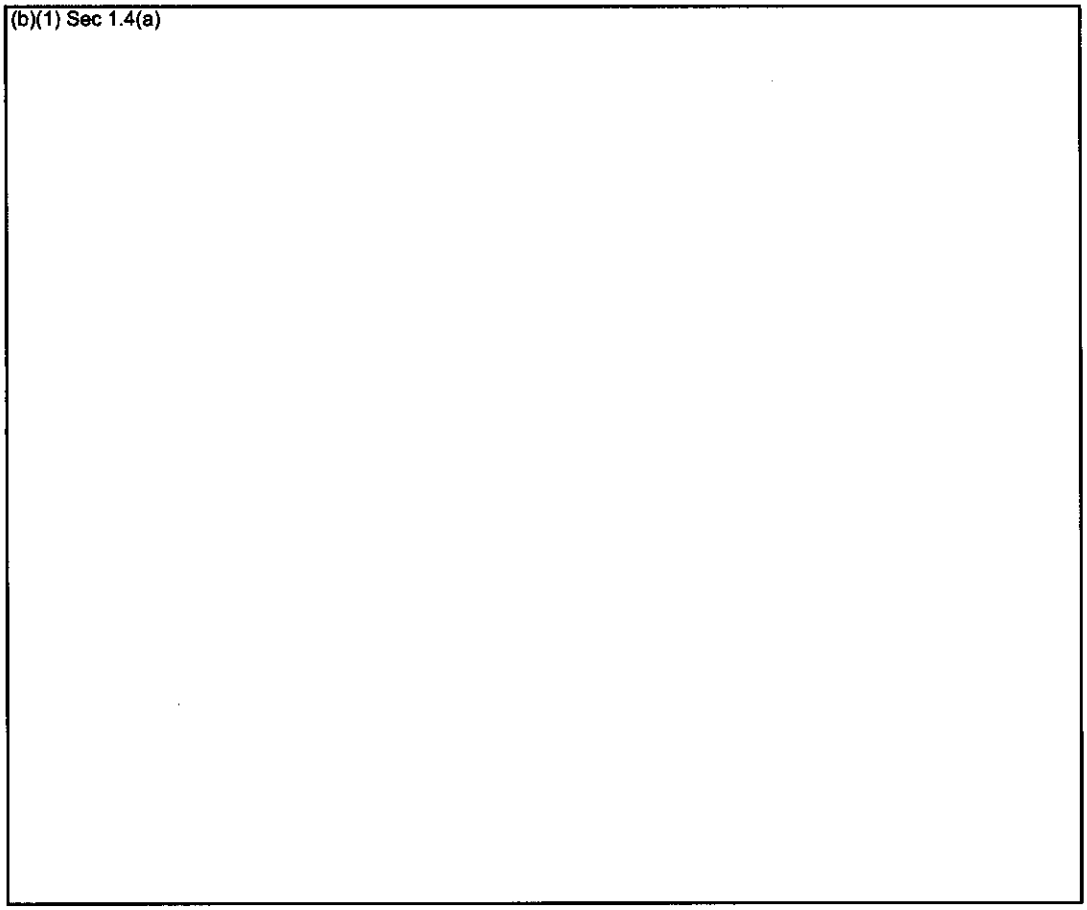


Figure 9 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (EXAMPLE)

(e) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

1 (~~S//Rel to USA, AUS, GBR~~) Commander's Intent. Support US government efforts to (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

2 ~~(S//Rel to USA, AUS, GBR)~~ (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
cooperation, even within the context of the cyberspace mission area. (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) The JFC will consider
(b)(1) Sec 1.4(a)

3 (U) (b)(1) Sec 1.7(e) The following are general (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

2.1 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2.1.1 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2.1.2 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2.1.3 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2.2 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2.2.1 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2.2.2 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2.2.3 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2.3 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2.3.1 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2.3.2 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2.3.3 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2.4 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2.4.1 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2.4.2 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2.4.3 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

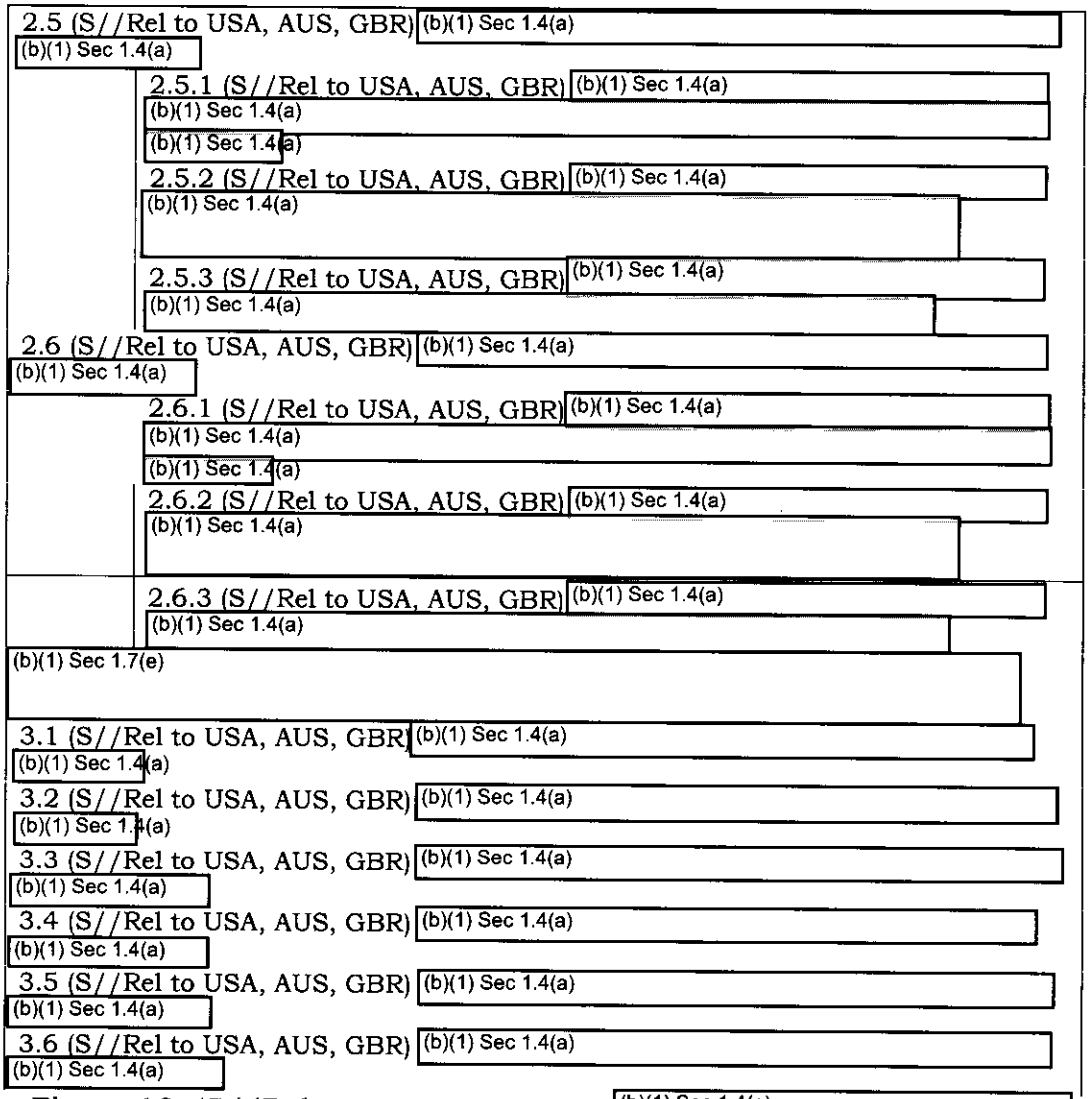


Figure 10: (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

4 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

a (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
Normally, the JFC (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) operations. Therefore, special circumstance and authorities in (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

b (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) accomplishment. In order to (b)(1) Sec 1.4(a) the JFC is normally (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

c (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

5 (U) Execution. Specific details on how cyber forces will execute their mission will be covered in Annex C and in (b)(1) Sec 1.7(e)

a (U) (b)(1) Sec 1.7(e) Execution activities are identified.

b (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) These are activities that are accomplished (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

c (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

d (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

6 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Cyber forces will (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Also, other domain-specific (b)(1) Sec 1.4(a) operations in and through cyberspace. Specific details on how cyber forces (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

a (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) As the cyber campaign progresses, the supported JFC must (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Refer to the Executive Summary (b)(1) Sec 1.4(a) and (b)(1) Sec 1.4(a)

b (U) (b)(1) Sec 1.7(e)

(1) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Unlike (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) the JFC can prioritize defense readiness based on likely (b)(1) Sec 1.4(a) In addition, the JFC can (b)(1) Sec 1.4(a) based on increased operational requirements for US cyberspace to function. A method to describe this is the (b)(1) Sec 1.4(a).

(2) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) See Figure 8, above to describe (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(3) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) USSTRATCOM may use (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

7 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Specific details on how (b)(1) Sec 1.4(a) will be covered in Annex C and (b)(1) Sec 1.4(a) As outlined above, CDRUSSTRATCOM can be the designated supported or supporting commander for operations in and through cyberspace. (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

a (~~S//Rel to USA, AUS, GBR~~) Supported Commander. As the supported commander, CDRUSSTRATCOM will:

(1) (~~S//Rel to USA, AUS, GBR~~) Determine (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
attain the objective.

(2) (~~S//Rel to USA, AUS, GBR~~) Highlight the
(b)(1) Sec 1.4(a)

(3) (~~FOUO~~) Determine (b)(1) Sec 1.7(e) o emphasize the desired end-state. Some cyberspace
(b)(1) Sec 1.7(e)

(4) (~~FOUO~~) Provide guidance on his objectives, desired
(b)(1) Sec 1.7(e)

b (U) Supporting Commander. As the supporting commander, CDRUSSTRATCOM will assist the supported JFC to accomplish the above tasks from a cyberspace perspective as required. General discussion on USSTRATCOM cyberspace support is found in applicable USSTRATCOM supporting CONPLANs. Specific details on USSTRATCOM cyberspace operational support will be provided in (b)(1) Sec 1.7(e)

(f) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

1 (U) Commander's Intent. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) establish/maintain normal operations of the DOD GIG, (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

2 (U) (b)(1) Sec 1.7(e) operations are characterized by (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) phase in that it is largely characterized by (b)(1) Sec 1.7(e) specifically support (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

3 (U) Objectives (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) That sections lists general operational (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) support the (b)(1) Sec 1.7(e) action in cyberspace and support to other operations through cyberspace will be covered in (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

4 (~~S//Rel to USA, AUS, GBR~~) Risk.

a (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Normally the JFC is (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Therefore, special circumstance and authorities in (b)(1) Sec 1.4(a) must be provided in order to (b)(1) Sec 1.4(a)

b (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

c c (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

5 (U) Execution. See (b)(1) Sec 1.7(e) above.

6 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) See (b)(1) Sec 1.4(a) above.

7 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) The cyberspace planner should consider (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) when crafting options for the commander.

(g) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

1 (~~S//Rel to USA, AUS, GBR~~) Commander's Intent. Prepare
(b)(1) Sec 1.4(a)

2 (U) Timing. (b)(1) Sec 1.7(e) operations in and through cyberspace (b)(1) Sec 1.7(e) to expand friendly freedom of action in cyberspace continue while the JFC (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) with the intent of resolving the crisis at the earliest opportunity. The supported JFC (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

across/through the DOD GIG. (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

3 (U) Objectives and (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

4 (~~S//Rel to USA, AUS, GBR~~) Risk.

a (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
Normally the JFC will consider taking (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

b (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) The JFC is normally focused on
(b)(1) Sec 1.4(a)

c (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
The JFC will consider using (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) and will be less concerned with
(b)(1) Sec 1.4(a)

5 (U) Execution. See (b)(1) Sec 1.7(e)

6 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) See
(b)(1) Sec 1.4(a)

7 (~~S//Rel USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
operations (b)(1) Sec 1.4(a) The
cyberspace planner must consider (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) if attributed in
(b)(1) Sec 1.4(a) when crafting options for the commander.

(h) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

1 (U) Commander's Intent. (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

cyberspace. In addition, USSTRATCOM may be called upon to (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

2 (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

JFC will not normally (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) The supported JFC will consider progressing to
(b)(1) Sec 1.7(e)

3 (U) Objectives and (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

4 (~~S//Rel to USA, AUS, GBR~~) Risk.

a (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

b (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

c (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

5 (U) Execution. See (b)(1) Sec 1.7(e)

6 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) See (b)(1) Sec 1.4(a)

7 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(i) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

1 (U) Commander's Intent. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

2 (U) Timing. The (b)(1) Sec 1.7(e) is typically characterized by a change (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) to ensure that the situation leading to the original crisis does not reoccur and/or its effects are mitigated. Throughout this segment, the JFC continuously assesses the impact of current cyberspace operations (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

3 (U) Objectives and (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

4 (U) Risk.

a (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Normally

the JFC is (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

b (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) In order to limit (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) the JFC is normally more focused
(b)(1) Sec 1.4(a)

c (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
In order to minimize (b)(1) Sec 1.4(a) in
(b)(1) Sec 1.4(a)

5 (U) Execution. See (b)(1) Sec 1.7(e)

6 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) See
(b)(1) Sec 1.4(a)

7 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
operations (b)(1) Sec 1.4(a) The planner
must consider the (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(j) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

1 (U) Commander's Intent. Provide support, as applicable
(b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) of cyberspace systems and/or
infrastructure, as directed.

2 (U) Timing. (b)(1) Sec 1.7(e) is predominately characterized by
cyberspace (b)(1) Sec 1.7(e) The
goal is for cyberspace forces to (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

3 (U) Objectives and (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

4 (U) Risk.

a (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

b (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) In order to (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) the JFC is normally more focused on (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

c (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
In order to minimize (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

5 (U) Execution. See (b)(1) Sec 1.7(e)

6 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) See
(b)(1) Sec 1.4(a)

7 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) The
cyberspace planner must consider (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

c. c. (U) Tasks.

(1) HQ USSTRATCOM.

(a) (U) Provide Commander's Intent by developing Operations Orders (OPORDs) and Execution Orders (EXORDs) to

support strategic/global DOD cyberspace operations, as necessary.

(b) (U) Provide an updated Commander's Intent with regard to cyberspace operations prior to execution of operations and (b)(1) Sec 1.7(e)

(c) (U) Ensure C/S/As' contingency and crisis plans for CO are integrated and coordinated across the DOD GIG.

(d) (U) Sponsor DOD-wide development of CO crisis action plans, policies, and doctrine in order to support and (b)(1) Sec 1.7(e)

(e) (~~S//Rel to USA, AUS, GBR~~) Develop strategic-level plans to (b)(1) Sec 1.4(a)

(f) (U) Advise and coordinate with supporting and supported commander on matters concerning the employment and limitations (e.g., logistics) of such support, assist in planning for the integration of such support into the supported commander's effort as a whole, and ensure that support requirements are appropriately communicated within USSTRATCOM.

(g) (U) Coordinate with combatant commanders to review and update their prioritization assessment for defense and reconstitution of their networks. Assessments shall identify current mission-critical, mission-essential, and mission-support networks.

(h) (~~S//Rel to USA, AUS, GBR~~) Per ref c, coordinate planning with other combatant commanders, to include assisting combatant commanders (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(i) (U) Support and coordinate CO information sharing with alliance and coalition partners concerning any ambiguous emerging threats based on guidance provided in the approved Delegation of Disclosure Letter (ref k) and applicable Memoranda of Agreement/Memoranda of

Understanding (MOA/MOU). Coordination and agreements will be IAW CJCSI 2300.01A and CJCSI 5130.01A. Disclosure of classified information will be IAW CJCSI 5221.01A.

(j) (U) Maintain liaison with appropriate government agencies, with OSD and Joint Staff oversight, for CO and COA development.

(k) (U) Based on guidance provided in approved information releasability policies and procedures, support and advocate increased information sharing with the private sector.

(l) (U) Per ref j, and Annex C, conduct Computer Network Assessment Conferences (NACs):

1 (U) Prior to execution of CONPLAN 8039.

2 (U) Prior to changing phases when not preempted by pre-planned responses.

3 (U) Prior to providing recommendations for the use of the elements of national power in cyberspace operations to SECDEF.

4 (U) Prior to developing conventional and special operations, CO and other IO COAs.

(m) (U) Communicate to the DOD Chief Information Officer (CIO) the level of agility and responsiveness of the DOD GIG to conduct CO. USSTRATCOM shall also identify to the DOD CIO threats to the DOD GIG. DOD CIO has legal responsibility under the Clinger-Cohen Act of 1996 to acquire architectural and configuration control over the DOD portion of the DOD GIG.

(n) (U) Reference COOP IAW ref bl in order to conduct operations when the ability to access the DOD GIG is denied.

(o) (~~S//Rel to USA, AUS, GBR~~) Identify desired (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) in support of other combatant commanders as directed.

(p) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) and coordinate approval with SECDEF and C/S/As, as required.

(q) (U) Exercise command and control of selected missions, as directed.

(r) (U) Assess the operational impact of recommended CO response actions.

(s) (U) Gather, analyze and report at the strategic level, combat assessment information necessary for continued defending/defeating operations.

(t) (U) As approved by the Secretary of Defense (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) as necessary.

(u) (U) Provide technical, planning and/or operational offensive cyber-related advice and, upon request, actions to contain (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) in their AORs.

(v) (~~S//Rel to USA, AUS, GBR~~) Identify and request (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) with respect to cyberspace.

(w) (~~S//Rel to USA, AUS, GBR~~) Identify and request (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(x) (~~S//Rel to USA, AUS, GBR~~) Request from the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(y) (~~S//Rel to USA, AUS, GBR~~) Develop and maintain (b)(1) Sec 1.4(a) cyberspace forces and activities.

(z) (U) Maintain network defense baseline for the DOD GIG.

(aa) (~~S//Rel to USA, AUS, GBR~~) Disseminate to C/S/As (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(bb) (U) ~~(S//Rel to USA, AUS, GBR)~~ As needed, develop and request supplemental ROE from the SECDEF.

(cc) ~~(S//Rel to USA, AUS, GBR)~~ Plan, coordinate and (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) when directed.

(dd) ~~(S//Rel to USA, AUS, GBR)~~ Continue and/or expand the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(ee) ~~(S//Rel to USA, AUS, GBR)~~ Develop and coordinate (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) based on assessment and recommendation from Joint Task Force – Global Network Operations (JTF-GNO).

(ff) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(gg) (U) Coordinate enhanced information sharing with allies, coalition partners and the private sector, based on approved Delegation of Disclosure Authority Official memorandum (ref l) and approved MOAs/MOUs. USSTRATCOM HQ/J4 is the OPR for all MOAs/MOUs.

(2) (U) USSTRATCOM Components when directed will:

(a) (U) Recommend changes to daily operations network configurations as a result of lessons learned.

(b) (U) Reference respective component (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(c) (U) Coordinate with HQ USSTRATCOM on matters pertaining to CO. Implement DOD-wide CO directions from CDRUSSTRATCOM for applicable networks.

(d) ~~(FOUO)~~ Direct and monitor compliance (including CTOs (Communications Tasking Order), IAVAs (Information Assurance Vulnerability Alerts), and INFOCON (Information Operations Condition)) of indigenous networks with approved DOD policies and procedures that regulate operations in the DOD GIG (see Annex C Operations) and report as required.

(e) ~~(FOUO)~~ Coordinate, execute and/or direct support troubleshooting and restoration actions for internal networks and systems as required.

(f) ~~(FOUO)~~ Monitor named areas of interests (NAIs) in support of JTF-GNO to detect threat activity against the DOD GIG (see Annex C, Operations).

(g) ~~(FOUO)~~ Implement response actions in support by JTF-GNO (IAW SROE), to correct faults, defeat threat activity, and deliver priority information across the DOD GIG (see Annex C, Operations).

(h) ~~(FOUO)~~ Implement contingency operations in support of JTF-GNO to restore capability and strengthen the DOD GIG against further faults, threats and information gaps across the DOD GIG (see Annex C, Operations).

(i) ~~(FOUO)~~ Report to JTF-GNO status of internal worldwide terrestrial, space and wireless transmission systems and enterprise services, and facilities.

(j) ~~(FOUO)~~ Establish, in support of JTF-GNO, procedures for dissemination of network operations (NETOPS) related advisories, alerts, and warning notices.

(k) ~~(FOUO)~~ Conduct nodal analysis of internal networks to determine Critical Nodes, provide this information, and assist JTF-GNO and HQ USSTRATCOM with defense and/or recovery/restoration operations as required.

(l) (U) Provide recommendations to HQ USSTRATCOM for policy, planning, ROE, COAs, INFOCON changes, requirements, and mission tactics, techniques and procedures (TTPs).

(m) (U) Operations will be coordinated with Combatant Commanders during the planning and execution phase to mitigate AOI/functional mission (s) impact.

(n) (U) The following USSTRATCOM Component commanders have specific tasks in support of CONPLAN 8039:

1 (U) Joint Functional Component Command Global Strike & Integration (JFCC GSI) when directed will:

a (U) With component support, will maintain common situational awareness for the headquarters and incorporating CO capabilities into integrated solutions for USSTRATCOM operations as a supported commander.

b (U) Through the Global Operations Center (GOC), USSTRATCOM Integration Operations Center (SIOC) and Joint Planning Working Group (JPWG), will integrate IO with all USSTRATCOM capabilities to assure the range of military operations is provided for DOD activities and operations.

c (~~S//Rel to USA, AUS, GBR~~) Develop operational-level plans to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) COAs must include various types of (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

d (~~S//Rel to USA, AUS, GBR~~) Establish a (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) cyberspace.

e (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) operations planning and (b)(1) Sec 1.4(a) to JTF GNO and other components in order to provide (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

2 (U) Joint Task Force - Global Network Operations (JTF-GNO) when directed will:

a (U) Develop cyber-related defense COAs in coordination with, JFCC NW, JIOWC and affected C/S/As as applicable that deter or defeat unauthorized activity targeted against the DOD GIG. Submit to HQ USSTRATCOM for approval.

b (U) As directed, conduct strategic, global cyber-related defense operations to defend DOD's use of cyberspace.

c (U) Coordinate development and planning of cyber-related defense measures with DOD and non-DOD organizations and agencies. This includes coordination with the DHS through the US CERT and the NCRCG during actual or potential cyber incidents. Submit to HQ USSTRATCOM for approval.

d (U) Provide coordination and technical assistance to C/S/As to minimize and deconflict operational impacts resulting from changes in INFOCON levels. This includes coordination with the DHS through the US CERT and the NCRCG during actual or potential cyber incidents that may impact U.S. cyberspace outside the DOD GIG.

e (U) Provide the consolidation of information from the service CERTs to all appropriate C/S/As.

f (U) Coordinate for enhanced information sharing with allies, coalition partners and the private sector, based on approved Delegation of Disclosure Authority Official memorandum (ref k) and approved MOAs/MOUs.

g (U//~~FOUO~~) Coordinate with the Law Enforcement Counterintelligence Center (LECIC) Defense Criminal Investigative Organizations (DCIOs) Liaison Officers for support of Service, federal, state and local law enforcement and counterintelligence agencies to counter, mitigate or halt threats to the DOD GIG.

h (U) Monitor and analyze (b)(1) Sec 1.7(e) intrusions and other cyber incidents of interest against the DOD's use of cyberspace and provide operational impact assessments to CDRUSSTRATCOM in coordination with service CERTs, DOD and service intelligence agencies.

i (U) Monitor C/S/As compliance with IAVAs and status of waivers and advise CDRUSSTRATCOM on matters pertaining to vulnerabilities of DOD cyber systems.

j (U) Provide situational awareness (e.g., COP) regarding the defensive status of the DOD GIG to C/S/As. This includes coordination with the DHS through the US CERT and the NCRCG during actual or potential cyber incidents.

k (U) Provide tactical warning to C/S/As for defense of the DOD GIG.

l (U) Sustain access to GIG backbone services.

m (U) Monitor INFOCON levels and implemented actions of C/S/As.

n (U) Provide and track waivers to selected INFOCON actions that cause unacceptable operational mission impact to C/S/As.

o (U) Coordinate with appropriate organizations to institute additional protection and defense measures to include using INFOCON procedures.

p (U) Provide operational assessment of GIG network performance after attacks or intrusions have occurred to HQ USSTRATCOM, SECDEF, CJCS and the C/S/As, as required.

q (U) Work with C/S/As, as required to develop assessment of operational impact of attacks and intrusions against DOD cyber systems.

r (U) Direct and coordinate restoration efforts. This includes determining and directing global alternate routing efforts and prioritization of network assets during network outages, attacks, and contingencies.

s (U) In response to network events or activities, as determined by CDRUSSTRATCOM or CDR JTF-GNO, Service Chiefs, or Secretaries, shall instantaneously attach Service CERTs/CIRTs to CDR JTF-GNO, who will exercise TACON upon contact with the service CERTs/CIRTs until such time that the responses to the events or activities are declared complete by CDR JTF-GNO, at which time Service Secretaries will resume control on the CERTs/CIRTs.

t (U) Recommend changes to daily operations network configurations as a result of lessons learned.

u (U) Gather, analyze and report cyber-related defense combat assessment to CDRUSSTRATCOM.

v (U) Coordinate and recommend changes to Global INFOCON posture levels to CDRUSSTRATCOM.

w (U) Identify strategic, global cyber-related defense intelligence requirements to USSTRATCOM in coordination with the geographic Combatant Commanders.

x (U) Determine and forward adversary's intent, capability, and information to CDRUSSTRATCOM and assess the risk of returning to a pre-hostility configuration.

y (U) After a cyber incident, coordinate return to daily operations network configurations and operations with C/S/As as soon as feasible.

z (~~S//Rel to USA, AUS, GBR~~) Provide situational awareness of (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

aa (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) Information Condition (INFOCON) exceptions from C/S/As.

bb (U) Coordinate cyber defense measures with C/S/As prior to implementation.

cc (U) Direct GIG operations and defense. Identify and advocate new desired characteristics and capabilities. C/S/As are responsible for implementing a network security baseline through a defense in depth strategy for their respective mission-critical, mission-essential and mission-support networks.

dd (U) Issue DOD-wide INFOCON level changes, based on assessed threats. Maintain awareness of INFOCON levels across the GIG and associated INFOCON implementation.

ee (U) Assess awareness of the operational impacts of changing INFOCON levels and recommended mitigation actions.

ff (U) Provide policy, direction and guidance to C/S/As regarding increased defense, network assurance operations and deterrence measures.

gg (~~S//Rel to USA, AUS, GBR~~) Develop and coordinate plans to implement (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

hh (U) Execute defensive operations and cyber defense IAW SROE (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

ii (~~FOUO~~) Accept Operational Control (OPCON) of service Network Operations Security Centers (NOSCs). Direct Liaison Authority (DIRLAUTH) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) is authorized.

jj (U) Submit cyberspace defense COAs to HQ USSTRATCOM to assure minimal impact to operation of the DOD GIG.

kk (~~S//Rel to USA, AUS, GBR~~) Submit military (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) to HQ USSTRATCOM.

ll (~~S//Rel to USA, AUS, GBR~~) Coordinate with C/S/As (b)(1) Sec 1.4(a)

mm (~~S//Rel to USA, AUS, GBR~~) Direct and coordinate the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

nn (~~S//REL to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Coordinate with other USSTRATCOM components in the development of courses of action and for the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

oo (U) Support Combatant Commands efforts to plan, coordinate, and conduct cyberspace and NETOPS activities.

3 (U) Joint Functional Component Command – Network Warfare (JFCC NW) when directed will:

a (~~S//Rel to USA, AUS, GBR~~) Provide the supported Commander (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) COAs. Coordinate CO with JFCC GSI to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Options/COAs must describe the (b)(1) Sec 1.4(a) Each option/COA will address the (b)(1) Sec 1.4(a) and (b)(1) Sec 1.4(a) in support of the overall operation.

b (~~S//Rel to USA, AUS, GBR~~) Support JTF-GNO by providing (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

c (~~S//Rel to USA, AUS, GBR~~) Coordinate (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) assets to achieve supported Commander objectives across all phases of the operation.

d (~~S//Rel to USA, AUS, GBR~~) Direct (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) the DOD GIG.

e (~~S//Rel to USA, AUS, GBR~~) Direct (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) use of cyberspace.

f (U) Coordinate employment of cyber warfare capabilities with JTF-GNO, JIOWC and other JFCCs. When directed, assume operational control (OPCON) or tactical control (TACON) of forces designated in the establishing deployment order.

g (~~S//Rel to USA, AUS, GBR~~) Develop COA recommendations for (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) USSTRATCOM missions and maintaining situational awareness for CDRUSSTRATCOM.

h (U//~~FOUO~~) Serve as the focal point for DoD (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(1) (U) Support JTF-GNO in their (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) to ensure operations are integrated and synchronized.

(2) (U) Coordinate intelligence gain/loss and technical assessments with the Intelligence Community for each network warfare course of action.

(3) (U) Coordinate and deconflict USSTRATCOM courses of action and as directed, the courses of action in support of other JFCs with the Intelligence Community.

i (U) Support Combatant Commands efforts to plan, coordinate, and conduct cyberspace activities.

4 (U) Joint Information Operations Warfare Command (JIOWC) when directed will:

a (U) Provide CDRUSSTRATCOM staff, JFCC NW, and JTF-GNO planners with IO and Strategic Communication expertise , as required, to conduct contingency and crisis action planning.

b (~~S//Rel to USA, AUS, GBR~~) Coordinate with JFCC NW, JFCC GSI, and JTF-GNO to ensure JIOWC's (b)(1) Sec 1.4(a)

c (~~S//Rel to USA, AUS, GBR~~) Establish and execute an (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) in coordination with appropriate C/S/As.

d (~~S//Rel to USA, AUS, GBR~~) Develop and (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

e (~~S//Rel to USA, AUS, GBR~~) Fully coordinate and synchronize (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

5 (U) Combatant Commands when directed will:

a (U) Conduct operations in and through cyberspace within their AORs, and coordinate with USSTRATCOM planners, as required

b (U) Review and update prioritization assessment of networks to identify those that are mission-critical, mission-essential, and mission-support networks, and share information with USSTRATCOM contributing to global situation awareness.

c (~~S//Rel to USA, AUS, GBR~~) Nominate appropriate
(b)(1) Sec 1.4(a)

d (U) Share (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
facilitating global situation awareness and tailored planning/operations.

e (U) Employ measures to ensure friendly forces are in compliance with all counter-vulnerabilities requirements.

f (~~S//Rel to USA, AUS, GBR~~) In coordination with USSTRATCOM, (b)(1) Sec 1.4(a) in support of CONPLAN 8039, to include (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

g (U) Enforce IAVA compliance within their specific enterprise.

h (U) Share operational assessments and technical reports to the JTF-GNO when network attacks and intrusions are targeted against computers and other cyber systems within respective AOR, to maintain awareness and enhance potential response and deterrent options.

i (~~S//Rel to USA, AUS, GBR~~) Provide recommendations for (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) to CDRUSSTRATCOM.

j (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) within respective AORs and AOIs.

k (U) Be prepared to support USSTRATCOM and LEAs in crisis, consequence management, and combat assessment within respective AORs.

l (U) Assist CDRUSSTRATCOM with (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

m (U) Per ref c, Combatant Commanders will deconflict and synchronize their planning with CDRUSSTRATCOM.

6 (U) Agencies. Specific agencies will be identified in Annex A.

a (U) General Tasks:

(1) (U) Share (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) awareness and tailored planning/operations.

(2) (U) Coordinate with USSTRATCOM on matters pertaining to CO. Implement DOD-wide CO directions from CDRUSSTRATCOM for applicable networks.

(3) (~~FOUO~~) Maintain DIRLAUTH with other Service and Agency (b)(1) Sec 1.7(e)

(4) (~~FOUO~~) Direct and monitor compliance (including CTOs, IAVAs, and INFOCON) of agency networks with approved DOD policies and procedures that regulate operations in the DOD GIG (see Annex C Operations) and report as required to JTF GNO.

(5) (~~FOUO~~) Share near-real time global situational awareness of Agency networks and systems to JTF-GNO. Provide a single POC/office to interface with JTF-GNO for this purpose.

(6) (~~FOUO~~) Coordinate, execute and/or direct troubleshooting and restoral actions for Agency networks and systems.

(7) (~~FOUO~~) Monitor Named Areas of Interest (NAIs) as tasked by JTF-GNO to detect threat activity against the DOD GIG (see Annex C).

(8) (~~FOUO~~) Implement response actions as directed by JTF-GNO (IAW SROE), to correct faults, defeat threat activity, and deliver priority information across the DOD GIG (see Annex C).

(9) (~~FOUO~~) Implement contingency operations as directed by JTF-GNO to restore capability and strengthen the DOD GIG against further faults, threats and information gaps across the DOD GIG (see Annex C).

(10) (~~FOUO~~) Report to JTF-GNO status of (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(11) (~~FOUO~~) Establish, in coordination with JTF-GNO, procedures for dissemination of NETOPS related advisories, alerts, and warning notices.

(12) (~~FOUO~~) Conduct nodal analysis of agency networks to determine Critical Nodes and provide Critical Node list to JTF-GNO.

(13) (~~FOUO~~) Share defense plans of critical nodes against physical and virtual threats with JTF-GNO

facilitating global situation awareness and tailored planning/operations.

b (U) Specific Organizations.

(1) (U) (b)(1) Sec 1.7(e)

a. (U//~~FOUO~~) Provide to C/S/As (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) actions, as well as mitigation strategies.

b. (~~S//Rel to USA, USA, AUS~~) Develop, in cooperation with USSTRATCOM and its Components, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Provide to C/S/As (b)(1) Sec 1.4(a) defense related tools and their associated training and documentation.

c. (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) and related techniques.

d. (U//~~FOUO~~) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) advice.

e. (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

f. (~~S//Rel to USA, AUS, GBR~~) Provide to C/S/As consolidated (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

g. (U//FOUO) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

h. ~~(S//Rel to USA, AUS, GBR)~~ Coordinate with
(b)(1) Sec 1.4(a)

i. (U//~~FOUO~~) Provide to C/S/As (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

j. U//~~FOUO~~) Provide to C/S/As (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
(U//~~FOUO~~) Provide to C/S/As (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

k. (U//~~FOUO~~) Share with C/S/As (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

l. (U//FOUO) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(2) (U) (b)(1) Sec 1.7(e)

a. (U) Provide CDRUSSTRATCOM with the
(b)(1) Sec 1.7(e)

b. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

c. (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

d. (~~S//Rel to USA, AUS, GBR~~) Coordinate with
(b)(1) Sec 1.4(a)

e. (~~S//Rel to USA, AUS, GBR~~) When required to
(b)(1) Sec 1.4(a)

f. (U) Assist CDRUSSTRATCOM (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

g. (U) Recommend, manage and perform (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

h. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
USSTRATCOM.

i. (U) Coordinate with JTF-GNO in the
(b)(1) Sec 1.7(e)

j. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

k. (U) Coordinate with C/S/As, (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

l. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

m. (U) In coordination with JTF-GNO, (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

n. (U) Assist JTF-GNO in (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

o. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

p. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) to ensure interoperability with the DOD GIG.

(3) (U) (b)(1) Sec 1.7(e)

a. (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
CONPLAN 8039. The scope of (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

b. (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

c. (~~S//Rel to USA, AUS, GBR~~) Coordinate with (b)(1) Sec 1.4(a)

(4) (U) (b)(1) Sec 1.7(e)

a. (~~S//Rel to USA, AUS, GBR~~) Identify internal (b)(1) Sec 1.4(a)

b. (~~S//Rel to USA, AUS, GBR~~) Provide USSTRATCOM (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

d. (U) Coordinating Instructions.

(1) (~~S//Rel to USA, AUS, GBR~~) Conditions for execution. CONPLAN 8039 is effective for planning purposes upon receipt. When CDRUSSTRATCOM or SECDEF approves this plan, it will (b)(1) Sec 1.4(a)

(2) (U) Direct liaison is authorized among CDRUSSTRATCOM components, C/S/As, supporting commands and planning headquarters. When developing supporting plans, maintain liaison with CDRUSSTRATCOM.

(3) (U) Component commands will develop supporting plans to CONPLAN 8039 and submit them to USSTRATCOM when tasked by CDRUSSTRATCOM.

(4) (U) ROE will be IAW ref o and modified with supplemental ROE as appropriate.

(5) (U) All CO forces supporting the CDRUSSTRATCOM mission will immediately establish liaison with CDRUSSTRATCOM LNO upon arriving in theater.

(6) (U) Commander's Critical Information Requirements (CCIR). The following are examples of CCIRs:

(a) (U) (b)(1) Sec 1.7(e) (See Annex B)

(b) (U) Friendly Forces Information Requirements (FFIRs). The following constitute FFIRs:

1 (U) Any increase/decrease in INFOCON worldwide.

2 (U) Any event (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

3 (U) Any event that (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

a (U) Any (b)(1) Sec 1.7(e) DOD GIG.

b (U) Any (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

c (U) Any access to the DOD GIG by unauthorized persons obtaining privileged user, administrator or root level access.

d (U) Any (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

e (U) Any (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

f (U) Any (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
imminently conduct these operations.

g (U) Any (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

h (U) Any (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) operational networks.

i (U) Any (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

j (U) Any (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

k (U) Any (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) C/S/As (e.g., GCSS, GCCS and DMS).

l (U) Any root level access, on a system shared by the DOD GIG, using new methods that exploit a system's vulnerabilities.

m (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) C/S/As (e.g., GCSS, GCCS and DMS).

4 (U) Any event that negatively affects execution of the Information Operations mission.

(c) (U) Essential Elements of Information (EEI).

1 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

2 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

3 ~~(C)~~ (b)(1) Sec 1.4(a) DOD GIG.

4 ~~(S//Rel to USA, AUS, GBR)~~ the DOD GIG (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

5 (C) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

6 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) DOD GIG and C4I systems.

4. (U) Administration and Logistics.

a. (U) Concept of Support. Supply support will be IAW Service doctrine. Teams consisting of tailored HQ USSTRATCOM, JFCC NW, JTF-GNO, JIOWC and Service component personnel will be provided administrative and logistical support by the requesting command.

b. (U) Logistics. CONPLAN 8039 is logistically supportable. Cyberspace forces may need to deploy under an ad hoc TPFDL.

c. (U) Personnel.

(1) (U) The parent command or agency will retain administrative responsibility for USSTRATCOM augmentation forces.

(2) (U) The appropriate USSTRATCOM Service component will assume administrative responsibility for military personnel (Active, Reserve or National Guard) assigned to USSTRATCOM's subordinate units.

(3) (U) Personnel accountability and direct management of military and DOD civilian resources (i.e., casualties, replacements, additional forces, etc.) will be the responsibility of the service component or the parent command or agency.

d. (U) Public Affairs (PA). The supported Combatant Command for CO in the operation will handle PA. When CDRUSSTRATCOM is the supported commander, the USSTRATCOM public affairs office will handle PA.

e. (U) Civil Affairs. Civil Affairs planning will be provided by U.S. Army Reserve Civil Affairs forces assigned to USSTRATCOM. CDRUSSTRATCOM will plan and execute Civil Affairs supporting CO when acting as the supported commander. Regional commanders will execute their Civil Affairs support to CO with organic personnel, JIOWC Combatant Commander teams as required, and U.S. Army Reserve Civil Affairs forces, as required.

f. (U) Meteorological and Oceanographic (METOC) Services. METOC in support of CO will be provided by USSTRATCOM JFCC GSI METOC Branch (JFCC GSI J332.)

g. (U) Geospatial Information and Services. Geospatial information in support of CO will be provided by USSTRATCOM/J2, in coordination with NGA.

h. (U) Medical Services. The Combatant Commander where CO is being conducted will provide medical services for supporting personnel.

5. (U) Command and Control (C2). The Service CO C2 structure as it applies to USSTRATCOM, JFCC NW, and JTF-GNO is not a standardized component structure, as the Army, Air Force, Navy and Marine Corps each have organized their cyberspace activities differently. See Annex J for specific C2 relationships.

Kevin P. Chilton
General, USAF
Commander

Annexes:

A--Task Organization
B--Intelligence
C--Operations
F--Public Affairs
J--Command Relationships
K--Command, Control, Communications and Computer Systems
N--Space Operations
S--Special Technical Operations
V--Interagency
Y--Strategic Communication
Z--Distribution

~~SECRET~~

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AFB NE 68113-6500
28 February 2008

ANNEX A TO USSTRATCOM CONPLAN 8039 (U)
(U) OPR: JFCC NW J52
TASK ORGANIZATION (U)

(U) References: Refer to Base Plan.

1. (U) Task Organization

a. (U) Supporting or Assigned Forces. While many DOD Components do not have organizations dedicated solely to cyber operations, there are DOD organizations not assigned to USSTRATCOM that have cyber capabilities. This annex identifies supporting or subordinate organizations capable of conducting or providing support to the cyber operations mission. To provide the broadest range of military capability, these forces will be made available to USSTRATCOM through various command relationships (Refer to Annex J, Command Relationships). Table 1 lists organizations that are designated in support of USSTRATCOM for CONPLAN 8039. Table 2 lists organizations subordinate or assigned to USSTRATCOM for CONPLAN 8039.

b. (U) (b)(1) Sec 1.7(e) The majority of these forces (b)(1) Sec 1.7(e) accomplish assigned tasks. For this reason, a (b)(1) Sec 1.7(e) is not included in this annex. (b)(1) Sec 1.7(e) required, it will be developed for a (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

c. (U) Shortfall Identification. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) It will also identify the forces shortfall (if required) that normally accompanies Annex A, Task Organization.

d. (U) Organizational Relationships. Responsibilities and organizational relationships are discussed in Annex J, Command Relationships.

2. (U) Supporting Organizations. The following commands or organizations are identified to provide support to USSTRATCOM for CONPLAN 8039.

ORGANIZATION	COMMANDER
US European Command	CDRUSEUCOM
US Pacific Command	CDRUSPACOM
US Joint Forces Command	CDRUSJFCOM
US Transportation Command	CDRUSTRANSCOM
US Central Command	CDRUSCENTCOM
US Special Operations Command	CDRUSSOCOM
US Northern Command	CDRUSNORTHCOM
US Southern Command	CDRUSSOUTHCOM
US Africa Command	CDRUSAFRICOM
US Element North American Aerospace Command	CDRUSELEMNORAD
US Navy	CNO
US Air Force	CSAF
US Army	CSA
US Marine Corps	CMC
Marine Corps Intelligence Activity	CO MCIA
Air Combat Command	COMACC
Central Intelligence Agency	DCIA
Defense Advanced Research Projects Agency	DARPA
Defense Business Transformation Agency	BTA
Defense Legal Services Agency	DLSA
Defense Commissary Agency	DeCA
Defense Contract Audit Agency	DCAA
Defense Contract Management Agency	DIRDCMA
Defense Finance and Accounting Service	DFAS
Defense Information Systems Agency	DIRDISA
Defense Intelligence Agency	DIRDIA
Defense Logistics Agency	DIRDLA
Defense Security Cooperation Agency	DSCA
Defense Security Service	DSS
Defense Threat Reduction Agency	DIRDTRA
Missile Defense Agency	MDA
National Geospatial-Intelligence Agency	NGA
National Security Agency/Central Security Service	DIRNSA
Pentagon Force Protection Agency	PFPA
American Forces Information Service	AFIS
Defense POW/MP Office	DPMO
Defense Technology Security Administration	DTSA
Defense Technical Information Center	DTIC
DOD Counterintelligence Field Activity	CIFA
DOD Education Activity)	DoDEA
DOD Human Resources Activity	DoDHRA
DOD Test Resource Management Center	TRMC

Office of Economic Adjustment	OEA
TRICARE Management Activity	TMA
Washington Headquarters Services	WHS
USAF Intelligence, Surveillance and Reconnaissance Agency	CDR AFISRA
USA Intelligence and Security Command	CDR INSCOM
USN Naval Security Group	COMNAVSECGRU
National Guard Bureau	CHIEF, NGB
Air Force Office of Special Investigations	AFOSI
Naval Criminal Investigative Service	NCIS
USA Criminal Investigation Division	CDR CID
Strategic Systems Programs/Naval Surface Warfare Center	SSP/NSWCDD
Joint Warfare Analysis Center	CDR, JWAC

Table 1: Supporting Organizations (U)

Table 1: Supporting Organizations (U)

3. (U) Subordinate Commands. The following commands are designated as subordinate commands for CONPLAN 8039.

SUBORDINATE COMMANDS	COMMANDER
JFCC Global Strike and Integration	CDR JFCC GSI
JFCC Intelligence, Surveillance, and Reconnaissance	CDR JFCC ISR
JFCC Integrated Missile Defense	CDR JFCC IMD
JFCC Network Warfare	CDR JFCC NW
JTF _ Global Network Operations	CDR JTF GNO
JFCC Space	CDR JFCC SPACE
STRATCOM Center for Combating WMD	CDR SCC WMD
Joint Information Operations Warfare Command	CDR JIOWC
Air Force Strategic Global Strike	AFSTRAT-GS/CC
Air Force Strategic Space	AFSTRAT-SPACE/CC
Marine Forces USSTRATCOM	COMMARFORSTRAT
US Fleet Forces Command	COMFLTFORCOM
Space and Missile Defense Command/Army Strategic Forces	CDR SMDC/ARSTRAT

Table 2: Subordinate Organizations (U)

Kevin P. Chilton
General, USAF
Commander

Appendixes:
1--(U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
2--(U) Shortfall Identification (Maintained in (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
3--(U) Military Deterrent Options (S)

Mark H. Owen
Brigadier General, USAF
Director, Plans and Policy

~~SECRET~~

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE NE 68113-6500
28 February 2008

APPENDIX 3 TO ANNEX A TO USSTRATCOM CONPLAN 8039(U)
(U) OPR: JFCC NW J52
(b)(1) Sec 1.7(e) (U)
(U) References: Refer to Base Plan.

1. (U) Situation. The USG harnesses all aspects of national power through the application of diplomatic, informational, economic and military deterrent options. This annex discusses (b)(1) Sec 1.7(e) to facilitate the objectives of CONPLAN 8039, Cyberspace Operation. (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) available to CDRUSSTRATCOM are implemented in the planning process. CDRUSSTRATCOM working with the affected Geographical Combatant Commander (GCC) will recommend (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) present a menu of choices for recommendation to the (b)(1) Sec 1.7(e). Should deterrence fail, (b)(1) Sec 1.7(e) freedom of action in cyberspace.

a. (U) Friendly. Refer to Base Plan and Annex A (Task Organization).

b. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

c. (U) Assumptions. Refer to Base Plan.

d. (U) Legal Considerations. Refer to Base plan and Appendix 8 (Rules of Engagement) to Annex C (Operations).

2. (U) Mission. Refer to Base Plan.

3. (U) Execution

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 06 December 2032~~

a. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) potential threats to US interests.

b. (~~S//REL USA, AUS, GBR~~) Elements of National Power. An effective (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) from the following categories may be implemented individually or in packages as appropriate to best meet the particular situation.

(1) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) They may pursue measures to increase (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) Other actions include measures to (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) options may also seek to gain support from the (b)(1) Sec 1.7(e)

(2) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) to maintain freedom of action in cyberspace. These options may be (b)(1) Sec 1.7(e)

(3) (U) (b)(1) Sec 1.7(e) increase/highlight assistance already provided (b)(1) Sec 1.7(e)

4. (U) Administration and Logistics. – Not used.

5. (U) Command and Control. – Refer to Base Plan and Annex J (Command Relationships).

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AFB NE 68113-6500
26 February 2008

ANNEX B TO CDRUSSTRATCOM CONPLAN 8039 (U)
(U) OPR: HQ USSTRATCOM/J23 INTELLIGENCE (U)
28 February 2008
(U) References:

a. (U) Joint Publication 2-0, Joint Doctrine for Intelligence Support to Operations, 9 March 2000 (U).

b. (U) Draft CJCSM 3314.01, Chairman of the Joint Chiefs of Staff Manual, Intelligence Campaign Planning Guidance, 30 November 2007 (U).

c. (U) (b)(1) Sec 1.7(e) updated semi-annually, (S//SI//NF).

d. (U) Joint Publication 2-01.3, Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace, 24 May 2000 (U).

e. (U) National Intelligence Support Plan (NISP) in Support of USSTRATCOM CONPLAN 8039, Date TBD (S//COMINT//REL).

f. (U//FOUO) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (S//SI).

g. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (TS//SI).

h. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (TS//SI).

i. (U//~~FOUO~~) CJCSI 3110.02D, Intelligence Planning Objectives, Guidance and Tasks, 5 March 2003 (S).

j. (U//~~FOUO~~) DCID 7/3, Information Operations and Intelligence Community Related Activities, 1 July 1999.

1. (U) 1. (U) Situation. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) It is designed to provide intelligence

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2032~~

information at the strategic level that may be applicable to any state or non-state actor with a cyberspace capability and access or intent to use cyberspace to threaten U.S. networks. (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

a. (~~S//REL USA, AUS, GBR~~) Characteristics of the Area. The cyberspace environment is global in scale and is characterized by the use of electronics to store, modify, and exchange data via networked systems and associated physical infrastructures. The potential operational area is the entire cyberspace domain. [See the CONPLAN 8039 Base Plan paragraph 1 for a detailed description of Characteristics of Area / Area of Concern, Area of Interest (AOI), Area of Responsibility (AOR), Operational Area (AO), and Centers of Gravity (COGs).] The primary focus is to defend the DoD Global Information Grid (GIG) and (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

b. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(1) (U) End State and Courses of Action

(a) (~~S//REL USA, AUS, GBR~~) The foundations of intent (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
Also included in this plan are (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) end states such as:

1. (S//REL USA, AUS, GBR USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2. (S//REL USA, AUS, GBR USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

3. (S//REL USA, AUS, GBR USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(b) (~~C//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) full scope cyberspace operations capabilities (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) including (b)(1) Sec 1.4(a) cyberspace programs. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) residing or transiting DoD information systems.

(c) (U//~~FOUO~~) (b)(1) Sec 1.7(e) to include hackers, terrorists, insiders, and criminals, intend to access, deny, degrade, exploit, or modify data residing on U.S. cyberspace systems. (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(2) (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(3) (~~C//REL USA, AUS, GBR~~) Capability to Collect, Process, and Disseminate Intelligence. (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

c. (~~S//REL USA, AUS, GBR USA, AUS, GBR~~) Friendly. Cyberspace operations require a (b)(1) Sec 1.4(a) effort. See the NISP to this CONPLAN for additional details on friendly intelligence capabilities and activities.

(1) (~~S//REL USA, AUS, GBR USA, AUS, GBR~~) DoD intelligence organizations (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) conduct intelligence operations in support of cyberspace operations. DoD Intelligence must also develop or improve the capability to:

(a) (~~S//REL USA, AUS, GBR USA, AUS, GBR~~) Provide (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b) (~~S//REL USA, AUS, GBR USA, AUS, GBR~~) Improve DOD's understanding of cyberspace networks, (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) See CONPLAN 8039 Base Plan for more details concerning (b)(1) Sec 1.4(a)

(c) (~~S//REL USA, AUS, GBR USA, AUS, GBR~~) Apportion intelligence assets (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(d) (~~S//REL USA, AUS, GBR USA, AUS, GBR~~) Prioritize efforts as directed by combatant command Joint Intelligence Operations Centers (JIOCs) and as illustrated by the CONPLAN 8039 (b)(1) Sec 1.4(a)

(2) (~~S//REL USA, AUS, GBR USA, AUS, GBR~~) Combatant command J2s will assess the effectiveness of the CONPLAN 8039 IP effort, including the (b)(1) Sec 1.4(a) this annex, the NISP, associated Functional Support Plans (FSPs), and other supporting documentation and processes in their respective AORs and forward (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) Forward ISR-related shortfalls for cyberspace operations to USSTRATCOM/J8 for advocacy and support.

d. (U) Legal Considerations. Given the unique nature of cyberspace, the legal framework associated with intelligence collection in support of cyberspace operations must be well understood. (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) All intelligence operations under this plan will be conducted in compliance with applicable U.S. domestic and international law. In particular, intelligence activities (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) Additional legal considerations can be found in the CONPLAN 8039 Base Plan.

2. (~~S//REL USA, AUS, GBR USA, AUS, GBR~~) Mission. Commander, US Strategic Command, plans and directs integrated DoD cyber operations to

(b)(1) Sec 1.4(a)

interests. See NISP Base Plan for the National Intelligence Mission Statement

3. (U) Execution

a. (~~S//REL USA, AUS, GBR USA, AUS, GBR~~) Concept of Intelligence Operations. This annex is the base document for the cyberspace operations IP effort. It outlines the intelligence community support for USSTRATCOM's CONPLAN 8039 Cyberspace Operations and the Military Strategic Framework identified in the National Military Strategy for Cyberspace Operations. The goal (b)(1) Sec 1.4(a)

(1) (~~S//REL USA, AUS, GBR USA, AUS, GBR~~) Purpose and Means. See CONPLAN 8039 Base Plan for the overall purpose. The 2005 Contingency Planning Guidance (CPG) advises the Chairman, Joint Chiefs of Staff (CJCS), to (b)(1) Sec 1.4(a)

This annex provides guidance and direction to the (b)(1) Sec 1.4(a) that supports USSTRATCOM CONPLAN 8039 planning and execution, and combatant command cyberspace operations planning. (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

support cyberspace operations. Specifically, the CONPLAN 8039 (b)(1) Sec 1.4(a)

(a) (U) Develop intelligence requirements and tasks and establish a common framework to understand the threat posed by state and non-state actors that have the capability and intent to threaten U.S. cyberspace.

(b) (U) Designate missions, roles, and responsibilities for DoD intelligence agencies in support of combatant command execution of cyberspace operations planning and operations.

(c) (U) Integrate and synchronize with intelligence plans of (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(d) (U) Describe an integrated operational architecture to facilitate the development and dissemination of an intelligence (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(e) (U) Identify doctrine, organization, training, material, leadership and education, and personnel shortfalls to successfully conduct cyberspace

intelligence operations and develop mitigation strategies and responsibilities to correct them.

(f) (U) Identify intelligence collection, analysis, and production requirements, thereby allowing (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) responsibilities and allowing USSTRATCOM to advocate for solutions to shortfalls.

(g) (U) Improve intelligence collection, analysis, and production capabilities (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) cyberspace activities.

(2) (~~S//REL USA, AUS, GBR~~) General. CONPLAN 8039 follows an effects-based planning construct and is organized along the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(3) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Responsibilities. USSTRATCOM is charged with leading the (b)(1) Sec 1.4(a) for cyberspace operations (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) See the NISP for additional details on the CONPLAN 8039 (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(4) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(a) (~~S//REL USA, AUS, GBR~~) Identify and understand (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) A clear understanding of these concepts is required to conduct an effective cyberspace operations campaign. Intelligence support is required for friendly forces to (b)(1) Sec 1.4(a) that allow the U.S. to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) cyberspace activity (b)(1) Sec 1.4(a)

(c) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) cyberspace related activity. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(5) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(6) (U) National Intelligence Support

(a) (~~S//REL USA, AUS, GBR~~) Per (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) directed plan. Combatant commands (b)(1) Sec 1.4(a) will provide rationale to (b)(1) Sec 1.4(a)

(b) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(c) (~~S//REL USA, AUS, GBR~~) The NISP, (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(d) (U) USSTRATCOM JFCC-ISR provides the ISR Support Plan (ISRSP), which is also part of the NISP. The ISRSP will outline ISR capabilities and requirements to be performed both day-to-day and during crisis.

(7) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

b. (U) Tasks

(1) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) cyberspace operations requirements.

(2) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) and
(b)(1) Sec 1.4(a) for conducting cyberspace intelligence operations.

(3) (U) Develop strategic cyberspace operations (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) Essential Elements of Information (EEIs), (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(4) (U) In conjunction with USD(I) and (b)(1) Sec 1.7(e) develop Memorandum of Agreement/Command Arrangement Agreements where necessary.

(5) (U) Conduct required cyberspace operations IPRs.

(6) (U) Monitor cyberspace I&W indicators.

(7) (U) Establish strategic priorities for cyber threats (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(8) (U) Support combatant command (b)(1) Sec 1.7(e) cyberspace operations requirements.

(9) (U) Monitor day-to-day execution of the CONPLAN 8039 (b)(1) Sec 1.7(e) and identify or report changes in the ability of DoD Intelligence to provide the support identified in the ITL to USSTRATCOM.

(10) (U) Assess DoD cyberspace intelligence capabilities and determine if (b)(1) Sec 1.7(e)

(11) (~~S//REL USA, AUS, GBR~~) Integrate CONPLAN 8039 (b)(1) Sec 1.4(a) with other USSTRATCOM global plans.

(12) (U) Participate, as required, in national-level cyberspace operations intelligence planning and coordination efforts.

c. (U) Procedures for processing (b)(1) Sec 1.7(e) is combatant command dependent and will be promulgated in the various combatant command CONPLANs and OPLANs. At USSTRATCOM, the J2 is responsible for processing (b)(1) Sec 1.7(e)

d. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

e. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) agencies contributing to this (b)(1) Sec 1.4(a) effort have been identified in the CONPLAN (b)(1) Sec 1.4(a) support of CONPLAN 8039 requirements. See the NISP for detailed information on (b)(1) Sec 1.4(a)

(1) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(2) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(3) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(4) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(5) (U) Counterintelligence (CI). See Appendix 3 (Counterintelligence).

(6) (U) Other Collection Activities. None.

f. (U) Processing and Evaluation. See the NISP and (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

g. (~~S//REL USA, AUS, GBR~~) Analysis and Production. USSTRATCOM/J2 (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) either a RAC or a CAC for each intelligence task listed in the ITL, were identified based on (b)(1) Sec 1.4(a) and the collection, analysis, and production assessments completed by agencies within DoD Intelligence. Organizations that do not meet the RAC/CAC criteria can be identified as providing "other support capabilities." A RAC is the lead organization responsible for producing the finished intelligence product to the requesting combatant command. The RAC will specify the need for and scope of the support that CACs will provide to the RAC. Each RAC and CAC will update the assessment of their ability to satisfy assigned tasks from the ITL (b)(1) Sec 1.4(a) or when deemed necessary by USSTRATCOM, USD(I), (b)(1) Sec 1.4(a)

h. (U) Dissemination and Integration

(1) (~~S//REL~~) Reports Required. Reports will differ based on the information contained in (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(2) (~~S//REL~~) Formats. Formats will differ based on the information contained in (b)(1) Sec 1.4(a)

(3) (~~S//REL USA, AUS, GBR~~) Distribution. USSTRATCOM uses (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) and SIPRNET. Each combatant command will determine dissemination requirements to support execution of its associated cyberspace operations

CONPLANs and OPLANs. See the NISP for detailed information on integration efforts to support cyberspace operations planning and operations.

(4) (U) Foreign Disclosure. To the greatest extent possible, all intelligence reports will be classified as "releasable to" as many allied partners as practical, especially Great Britain, Canada, and Australia. The combatant command(s) responsible for executing cyberspace operations will identify disclosure and intelligence sharing requirements needed to support the specific operations.

(5) (U) (b)(1) Sec 1.7(e) if applicable.

i. (U) Coordinating Instructions

(1) (U) Conferences

(a) (U) USSTRATCOM/J2 will host, as required, planning conferences to address updates to this CONPLAN and the associated IP effort. Attendance from combatant command J2s, (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
USSTRATCOM/J2 will send the announcement via message traffic and other means to ensure widest possible information dissemination (e.g., e-mail, JWICS and SIPRNET web pages, Secure Video Teleconference (SVTC) sessions, etc.).
(b)(1) Sec 1.7(e)

(b) (U) USSTRATCOM components and centers may host intelligence planning conferences to support specific USSTRATCOM or combatant command planning efforts or to address cyberspace operations related issues in their specific areas of expertise.

(2) (U) See the NISP for specific instructions on DoD, U.S. government interagency, and multi-national coordinating instructions.

(U)(3) (~~S//REL USA, AUS, GBR~~) USSTRATCOM uses a variety of collaborative tools to coordinate cyberspace operations activity. SIPRNET is the preferred collaboration venue to ensure the greatest inclusion of operators, planners, and intelligence personnel from all echelons of command. The paragraphs below outline the major cyberspace operations coordination activities for USSTRATCOM. Although current collaborative tools may change, the basic functionality will remain and be used in support of mission objectives.

(a) (~~S//REL USA, AUS, GBR~~) SIPRNET (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(U) (b) (~~S//REL USA, AUS, GBR~~) JWICS Page. USSTRATCOM uses the JWICS SKIWeb portal and 8039 IP page for coordination on activities and information dissemination that requires higher classification levels than what is maintained on SIPRNET.

(c) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) USSTRATCOM/ J2 uses (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(d) (U) Secure Video Teleconference (SVTC). USSTRATCOM has a number of (b)(1) Sec 1.7(e) for coordination and collaboration on cyberspace operations activities.

a. (U) Orders to Subordinate and Supporting Units

(1) (U) JFCC-NW

(a) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) plan development.

(b) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) defense of the DoD Global Information Grid (GIG).

(c) (~~S//REL USA, AUS, GBR~~) Coordinate intelligence collection/ analysis (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) and distribute as required.

(d) (~~S//REL USA, AUS, GBR~~) Coordinate with all other functional component commands for (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(2) (U) JFCC–ISR

(a) (U) Develop, maintain, and update a Global ISR strategy for cyberspace operations and an ISR Functional Support Plan to the NISP within the IP process.

(b) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) required by the CONPLAN 8039 NISP.

(3) (U) Joint Functional Component Command for Global Strike and Integration (JFCC-GSI)

(a) (~~S//REL USA, AUS, GBR~~) Coordinate with JFCC-NW for (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(4) (U) Joint Task Force-Global Network Operations (JTF-GNO)

(U) (a) (~~S//REL USA, AUS, GBR~~) Coordinate with USSTRATCOM/J2 for inclusion of CONPLAN 8039 IP into JTF-GNO planning efforts.

(U) (b) (~~S//REL USA, AUS, GBR~~) Provide intelligence support as required by the CONPLAN 8039 NISP.

(c) (~~S//REL USA, AUS, GBR~~) Provide intelligence planning support and assets as required to JFCC-NW related to (b)(1) Sec 1.4(a)

(d). (~~S//REL USA, AUS, GBR~~) Coordinate with JFCC-NW for (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(e) (~~S//REL USA, AUS, GBR~~) Provide cyberspace (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(5) (U) Joint Information Operations Warfare Command (JIOWC)

(a) (~~S//REL USA, AUS, GBR~~) Provide intelligence planning support as required to JFCC-NW related to (b)(1) Sec 1.4(a)

(b) (~~S//REL USA, AUS, GBR~~) Provide intelligence support as required to support (b)(1) Sec 1.4(a) and CONPLAN 8039 NISP.

(c) (~~S//REL USA, AUS, GBR~~) Coordinate with JFCC-NW for (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

b. (U) Requests to Higher, Adjacent, and Cooperating Units

(1) (U) USD(I). USD(I) is responsible for DoD coordination with other government agencies (OGAs) for intelligence issues. As the synchronizer and integrator of DoD intelligence support for cyberspace operations,

USSTRATCOM will work through USD(I) for issues requiring support from OGAs and also with the combatant command J2s for any PN issues.

(2) (U) (b)(1) Sec 1.7(e)

(a) (U) (b)(1) Sec 1.7(e) IP efforts (b)(1) Sec 1.7(e) IP process with other active IP efforts.

(b) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(c) (U) Lead development of the NISP in support of the IP; (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) enable the IP to function as a whole.

(d) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(e) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(f) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(g) (U) (b)(1) Sec 1.7(e)

(3) (U) Joint Staff/ (b)(1) Sec 1.7(e)

(a) (U) Develop (b)(1) Sec 1.7(e) in support of cyberspace operations.

(b) (U) Provide a (b)(1) Sec 1.7(e) to the NISP for this CONPLAN IP.

(4) (U) (b)(1) Sec 1.7(e)

(a) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(b) (U) Post updated versions of IP products (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(c) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(d) (U) Provide support as required by the CONPLAN 8039 NISP.

(5) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(6) (U) (b)(1) Sec 1.7(e)

(a) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) CONPLAN 8039 ITL.

(b) (~~S//REL USA, AUS, GBR~~) Coordinate, as appropriate for (b)(1) Sec 1.4(a)

(7) (U) GCC J2s

(U)(a) (~~S//REL USA, AUS, GBR~~) Provide cyberspace-related intelligence requirements for inclusion into the CONPLAN 8039 ITL.

(b) (~~S//REL USA, AUS, GBR~~) Coordinate, as appropriate for cyberspace operations issues, with USSTRATCOM/J2 to ensure synchronization between the respective GCC's plans and CONPLAN 8039, to (b)(1) Sec 1.4(a) for cyberspace operations intelligence requirements.

(8) (U) USJFCOM/J2

(a) (U) Work with (b)(1) Sec 1.7(e) USSTRATCOM, and the GCCs to develop an (b)(1) Sec 1.7(e)

(b) (U) Develop procedures and training to support (b)(1) Sec 1.7(e) intelligence and the IP process in support of this CONPLAN 8039.

(c) (U) Develop modeling and simulation of processes in the IP process.

(d) (U) Develop modeling against (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(e) (U) Develop an automated (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) IPs.

c. (U) Shortfalls and Limiting Factors

(1) (U) The Services, Combatant Commands, and Agencies often (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(2) ~~(S)~~ Intelligence community (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

d. (~~S//REL USA, AUS, GBR~~) Miscellaneous. Combatant commands, CSAs, Service intelligence centers, and USSTRATCOM components may evaluate the effectiveness of CONPLAN 8039 and this IP effort and forward any requests or recommendations to USSTRATCOM/J2 for improvements to this Annex, the (b)(1) Sec 1.4(a)

4. Administration and Logistics N/A

5. Command and Control

a. (U//~~FOUO~~) Intelligence Relationships. USSTRATCOM HQ and each JFCC, Center, and JTF have organic intelligence capabilities. Each provides tailored application of intelligence to satisfy respective commanders' requirements by minimizing duplication and maximizing integration.

(1) (U//~~FOUO~~) USSTRATCOM/J2. Provides strategic-level intelligence support to the HQ and components. HQ J2 leverages authorities and resources to ensure effective intelligence support across the USSTRATCOM intelligence enterprise, while facilitating collaboration between mission partners and the integration and synchronization of intelligence needs. HQ J2 is organized to provide intelligence planning (IP) effort in support of command planning activities. Figure 1 shows a high level representation of the command relationships with key organizations relating to cyberspace operations.

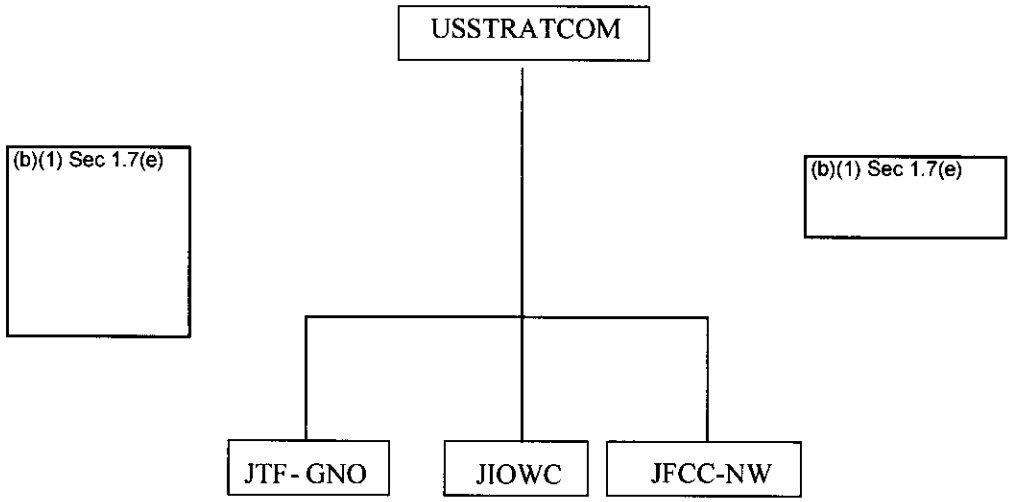


Figure 1 – (U) Command Relationships

(2) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(3) (U) Joint Task Force-Global Network Operations J2 (JTF-GNO/J2). Provides tailored intelligence in support of the operation and defense of the GIG, including DoD-wide computer network defense (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
business missions. The JTF-GNO/J2 provides timely and relevant intelligence to the Commander, Joint Task Force – Global Network Operations, JTF Staff, and components through (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) in support of the operation and defense of the Global Information Grid.

(4) (U) Joint Information Operations Warfare Command J2 (JIOWC/J2). Focal point for intelligence support to information operations within the JIOWC. JIOWC/J2 coordinates directly with combatant command and JTF intelligence entities, to include Joint Intelligence Operation Centers. JIOWC/J2 provides (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

Additionally, the JIOWC/J2 assists (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(5) (U) Joint Functional Component Command-Network Warfare J2 (JFCC-NW/J2). Provides intelligence to support the optimization of planning, integration, coordination, execution, and force management of the Network Warfare missions in support of joint warfighters. In coordination with JTF-GNO, JFCC-NW maintains situational awareness for the DoD GIG while (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) In addition to the wide range of products JFCC-NW provides to support cyberspace operations planning, (b)(1) Sec 1.7(e)

b. (U) Communications. USSTRATCOM/J2, component J2s, and relevant combatant command J2s make up the USSTRATCOM Intelligence Enterprise (SIE) to collaborate on intelligence support. The SIE is the customer in Figure 2, and the information exchange between agencies in the cyberspace environment is depicted in the diagram. The SIE submits a Production Request (PR) via (b)(1) Sec 1.7(e) The dotted lines within the customer box are to show that, ideally, each affected member of the SIE should receive a copy of the PR to ensure receipt of the finished intelligence product.

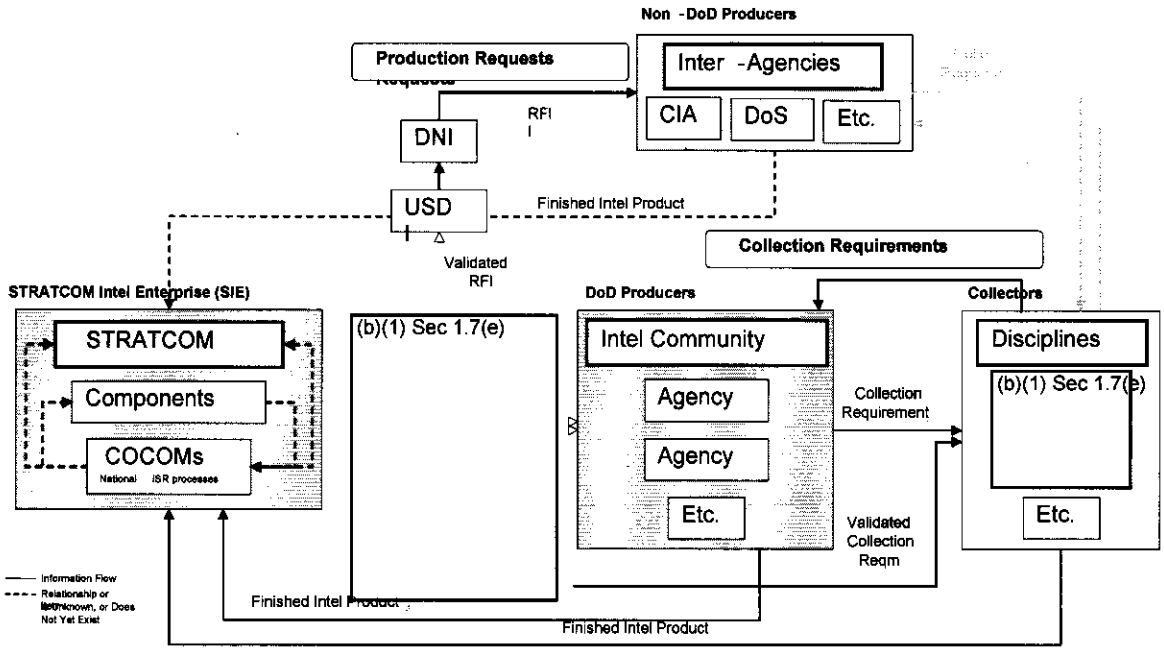


Figure 2 – (U) Communications and Information Exchange

(1) (U) The PR (b)(1) Sec 1.7(e) to ensure the appropriate subtasking of PRs to the producer(s). The producer accomplishes the PR and submits their own collection requirements, if needed, to the appropriate

collector. As mentioned above, the JFCCs have been directed to submit production requirements directly to the DoD producers. In the case where the PR and a non-DoD agency meet, the PR is routed through the USD(I) and the Director of National Intelligence (DNI), assigned to the appropriate non-DoD producer who may task a collector if needed, and then the finished intelligence product is routed back to the STRATCOM Intelligence enterprise (SIE). The process for a non-DoD agency to task a collector is not directed by this CONPLAN and, therefore, is grayed out in the diagram.

(2) (U) Collection requirements (CR) that originate from the SIE are (b)(1) Sec 1.7(e) prior to fielding by the collectors. The combatant command process for tasking national assets follows the path shown in the diagram. (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) and ensure appropriate subtasking of both PRs and CRs.

Appendices
1- (b)(1) Sec 1.7(e)
2- (b)(1) Sec 1.7(e)
3--Counterintelligence (CI)
4- (b)(1) Sec 1.7(e)
5- (b)(1) Sec 1.7(e)
6--Intelligence Support to Information Operations (IO)
7- (b)(1) Sec 1.7(e)
8-
9-

Kevin P. Chilton
General, USAF
COMMANDER

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AFB NE 68113-6500
28 February 2008

APPENDIX 1 TO ANNEX B TO CDRUSSTRATCOM CONPLAN 8039 (U)
(U) OPR: HQ J2
(b)(1) Sec 1.7(e) (U)

1. (U) General. (b)(1) Sec 1.7(e) are the basic (b)(1) Sec 1.7(e) requirements to support planning and operations regarding computer network operations. The (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) to support this plan.

2. (U) (b)(1) Sec 1.7(e) have been identified for the (b)(1) Sec 1.7(e) CONPLAN 8039 execution. Due to the similarity in intelligence requirements for (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) will be combined for these (b)(1) Sec 1.7(e)

3. (U) Each (b)(1) Sec 1.7(e) will list the supporting tasks and subtasks that further define the cyberspace operations intelligence requirements. The (b)(1) Sec 1.7(e) are:

a. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

b. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

c. (U (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

d. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2008 2032~~

e. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

f. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

g. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) cyberspace networks?

Kevin P. Chilton
General, USAF
COMMANDER

HEADQUARTERS, U.S. STRATEGIC COMMAND
OFFUTT AIR FORCE BASE NE 68113-6500
28 February 2008

APPENDIX 2 TO ANNEX B TO CDRUSSTRATCOM CONPLAN 8039 (U)
(U) OPR: HQ J2
(b)(1) Sec 1.7(e) (U)

(U) References:

a. (U) (b)(1) Sec 1.7(e), 25 Jan 73 (S).

b. (U) (b)(1) Sec 1.7(e) 10 Aug 88 (U).

c. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e), 31 May 01 (U).

d. (U) Joint Pub 2-01, Joint Intelligence Support to Military Operations, Appendix C, 26 Aug 02 (S).

e. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) 12 Jun 95 (U).

f. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) U//FOUO).

g. (U) (b)(1) Sec 1.7(e) June 05 (TS//TK).

h. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) 1 May 06 (U).

1. (U) Situation. This appendix provides a review of general responsibilities and procedures for submitting (b)(1) Sec 1.7(e) requirements to support planning, (b)(1) Sec 1.7(e) intelligence, readiness, posturing, situational awareness, and mission execution. Additional (b)(1) Sec 1.7(e) capability which may contribute to USSTRATCOM (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) Combatant Commands and tasked by their respective Service.

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2008 2032~~

a. (U) (b)(1) Sec 1.7(e) See 8039 Annex B (Intelligence) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

b. (U) Friendly. Refer to Base Plan.

c. (U) Assumptions. Refer to Base Plan.

d. (U) Legal Considerations. Refer to Base Plan and Annex B (Intelligence).

e. (U) Collection Priorities

(1) (U) Priority 1 through Priority 7. Not applicable.

(2) (U) (b)(1) Sec 1.7(e) USSTRATCOM/J2 Requirements
(b)(1) Sec 1.7(e) support to HQs staff elements.
USSTRATCOM Joint Functional Component Commands (JFCCs), components, and subordinate commands manage cyber operations (b)(1) Sec 1.7(e) functions for their organizations."" JFCC-Intelligence, Surveillance, and Reconnaissance (JFCC-ISR)"" (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(3) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(a) (U) Conduct all-source intelligence analysis/assessments.

(b) (U) Support command components and assigned units.

(c) (U) Support real-time global cyber operations and intelligence decision-making.

(d) (U) Support Commander, USSTRATCOM, in operations to support the President of the United States, the Secretary of Defense (SecDef), and other Unified Commanders.

2. (U) Mission. Refer to Base Plan.

3. (U) Execution. Refer to Annex B (Intelligence), para. 3.

a. (U) Concept of Operations

(1) (U) (b)(1) Sec 1.7(e) Organizations

(a) (S//REL) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(b) (U) The (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(c) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(d) (U) (b)(1) Sec 1.7(e) provide timely, responsive processing and validation of USSTRATCOM (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) feedback on the status of requirements.

b. (U) Responsibilities

(1) (U) JFCC-NW. Provide timely submission for (b)(1) Sec 1.7(e) needs in support of this CONPLAN. Maintain all appropriate tabs to this appendix.

(2) (U) (b)(1) Sec 1.7(e)

(a) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(b) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(c) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(d) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(3) (U) (b)(1) Sec 1.7(e)

(a) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(b) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(c) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(d) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

c. (U) Tasks. Refer to Annex B (Intelligence).

d. (U) Coordinating Instructions. Refer to Annex B (Intelligence).

4. (U) Administration and Logistics. Not Applicable.

5. (U) Command and Control

a. Command and Control. Refer to Annex J (Command Relationships).

b. Communications Systems. Refer to Annexes B (Intelligence) and K (C4 Systems).

Kevin P. Chilton
General, USAF
COMMANDER

HEADQUARTERS, U.S. STRATEGIC COMMAND
OFFUTT AIR FORCE BASE NE 68113-6500
28 February 2008

APPENDIX 3 TO ANNEX B TO CDRUSSTRATCOM CONPLAN 8039 (U)
(U) OPR: HQ J2
COUNTERINTELLIGENCE (CI) (U)

(U) References:

a. (U) Executive Order 12333, United States Intelligence Activities, 4 Dec 81 (U).

b. (U) DOD Regulation 5200.1-R, Information Security Program Regulation, Jan 97 (U).

c. (U) DOD Directive 5105.67, Dept of Defense Counterintelligence Field Activity, 19 Feb 02. (U)

d. (U) DOD Directive 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense, 7 Jan 80 (U).

e. (U) DOD Directive 5240.1, DOD Intelligence Activities, 25 Apr 88 (U).

f. (U) DOD Regulation 5240.1R, Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons, Dec 82 (U).

g. (U) DOD Directive 5240.2, DOD Counterintelligence, 22 May 97 (U).

h. (U) DOD Instruction 5240.4, Reporting of CI and Criminal Violations, 22 Sep 92, w/Ch 1, 8 Apr 92 (U).

i. (U) DOD Instruction 5240.8, Security Classification Guide for Information Concerning the DOD Counterintelligence Program (U) ASD(NII), 16 Nov 00 (C).

j. (U) DOD Instruction C-5240.10, Counterintelligence Support to the Combatant Commands and the Defense Agencies, 14 May 04 (U).

k. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (U).

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2032~~

1. (U//~~FOUO~~) Office of the Under Secretary of Defense, Deconfliction of DOD Counterintelligence (CI) Cyber Operations with the Intelligence Community (IC) (U//FOUO), 2 Feb 07.

1. (U) Situation

a. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) US IO; C4ISR; critical infrastructure; and cyberspace-related systems, technologies, facilities, and resources exist. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Refer to Annex B of Base Plan for current overarching threat information and (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

b. (U) Friendly

(1) (U) US National Agencies. Prior to, during, and following execution of any portion of this plan, CI, law enforcement, security, or intelligence support may be requested of the following organizations: DHS; Department of Justice (DOJ), including the Federal Bureau of Investigation (FBI); Central Intelligence Agency (CIA); NSA; DIA; National Counterintelligence Executive (NCIX); U.S. Marshals Service (USMS); CIFA; the Service CI, law enforcement, and security organizations, including AFOSI, NCIS, U.S. Army INSCOM, U.S. Marine Corps CI, United States Coast Guard (USCG) CI, and the U.S. Army CID; and various state-level departments, such as the National Guard and state and local police.

(a) (U) USSTRATCOM/Counterintelligence Staff Office (CISO) will serve as the focal point for integrating, synchronizing, and coordinating all USSTRATCOM CONPLAN 8039-related CI activities.

(b) (U) The U.S. Air Force, Army, Navy, and Marine Corps CI elements will provide CI support to their respective Services in support of the USSTRATCOM mission.

(c) (~~S//REL USA, AUS, GBR~~) Each tasked CI organization will (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) with USSTRATCOM CISO.

(2) (U) Command CI Structure. Upon execution of CONPLAN 8039, the USSTRATCOM CISO (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) and will perform associated duties in coordination with affected geographic combatant command/functional combatant command CISOs and designated Task Force CI Coordinating Authorities (TFCICAs).

(a) (U) USSTRATCOM CISO is responsible to plan, coordinate, advocate, and integrate the overall collaborative CI effort in support of this plan. Unless execution authority is transferred to another combatant commander, CDRUSSTRATCOM is the supported Commander. USSTRATCOM CISO is the CI representative for CDRUSSTRATCOM.

(b) (U) If another combatant commander is designated the supported Commander under this plan, that command's CISO becomes responsible for all planning, coordination, and integration of CI support to this plan and USSTRATCOM CISO becomes a supporting CI element. Supported combatant command CISO will designate a TFCICA.

(c) (~~S//REL USA, AUS, GBR~~) All combatant command CISOs and Service CI agencies will ensure the supported TFCICA receives, in a timely manner, (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
information copies of all CI planning, coordination, (b)(1) Sec 1.4(a)

(d) (U) The respective Service and its CI organizational headquarters will exercise operational control over its Military Department CI resources, unless specified otherwise by legal authority.

(e) (U) Administrative control of Military Department CI resources remains with the CI organization of the respective Service.

(f) (U) Assigned and supporting CI assets will utilize all available CI activities to support this plan. CI activities include all (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) available within CI investigations, operations, collections, and analysis and production.

(g) (U) All CI information relative to this plan will be made known to USSTRATCOM Commander and the supported Commander through the Commander's CISO or other CI element, if so named. CI information will be shared through the most expeditious means available.

(3) (U) Allied. Allied and coalition elements provide support based on national plans and agreements.

c. (U) Assumptions

(1) (U) The supported CISO, when required, will serve as or appoint a TFCICA. The TFCICA will establish CI reporting channels and requirements with component and other agency CI organizations upon implementation or execution of this plan.

(2) (U) All command elements and components will have dedicated CI support.

(3) (U) Components and national support agencies will provide pre-execution and post-execution CI support and services.

(4) (U) All CI organizations will follow appropriate US laws, directives, regulations, and policies regarding CI activities that involve US persons, enemy prisoners of war, and the LOAC.

2. (U) Mission. See Base Plan.

3. (U) Execution

a. (~~S//REL USA, AUS, GBR~~) Concept of Operations. The integration and synchronization of CI in support of this CONPLAN is the responsibility of CISO. Upon implementation of this CONPLAN, the CISO assumes the roles and responsibilities of the (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(1) (~~S//REL USA, AUS, GBR~~) Information collection and protection

(b)(1) Sec 1.4(a)

(2) (U) The discharge of special CI requirements assigned by higher authority, e.g., USD(I), CJCS, etc.

(3) (U) Supporting Service CI elements will accomplish CI missions within respective jurisdictions in accordance with established Service policies and

procedures. Assigned CI elements will be guided by applicable DOD, Joint Staff, or combatant command policies and procedures. All Service CI elements will provide information and coordination copies of Service-unique field CI (b)(1) Sec 1.7(e) activities that are supporting this CONPLAN.

b. (U) Tasks

(1) (U) Counterintelligence Collection and Reporting

(a) (U) Service CI Elements. Forward Service-unique field CI collections and standard (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(b) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(c) (U) USSTRATCOM (b)(1) Sec 1.7(e) CISO

(1) (U) Develop CI collection requirements specific to USSTRATCOM and in coordination with JFCC NW, JTF GNO, and other affected combatant commands/agencies.

(2) (U) Ensure all products generated in support of this plan are distributed to Commander USSTRATCOM, JFCC NW, JTF GNO, Joint Staff/J2, other combatant commands and task forces as appropriate.

(3) (U) Coordinate CI collection activities and maintain liaison with national level CI and law enforcement agencies as well as other affected COCOM CISOs.

(4) (U) Coordinate with national level agencies for collection, analysis, and production in support of critical mission needs.

(2) (U) Counterintelligence Analysis and Production. See para. 3.b.(1), above.

(3) (U) Counterintelligence Investigations. Investigations will be conducted by the military services and/or the appropriate national agencies. Services will brief CDRUSSTRATCOM through the CISO (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) affecting this CONPLAN.

(4) (~~C//REL~~) Counterintelligence Operations. Individual Service components and/ or appropriate national agencies (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) activities as directed or required in support of this CONPLAN. Services will brief CDRUSSTRATCOM through the CISO (b)(1) Sec 1.4(a) operations and activities affecting this CONPLAN.

(5) (U) Functional Services. Individual service components and/or appropriate national agencies will conduct CI functional services as required by this CONPLAN. Services will brief CDRUSSTRATCOM through the CISO (b)(1) Sec 1.7(e) on the overall status of functional services activities.

c. (U) Coordinating Instructions. All higher, lateral, and subordinate Service and DOD level CI elements will keep the USSTRATCOM CISO/ (b)(1) Sec 1.7(e) as appropriate, of their CI operations and activities. USSTRATCOM CISO (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) in support of this CONPLAN. These roles and responsibilities (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

4. (U) Administration and Logistics. USSTRATCOM CISO (b)(1) Sec 1.7(e) manages the Command's CI program. In this role, the USSTRATCOM CI Staff Office will assist the component's CI services in coordinating their activities and to identify Service-specific requirements. New CI requirements should be forwarded to USSTRATCOM CISO (b)(1) Sec 1.7(e) USSTRATCOM CI Staff Office coordinates with USSTRATCOM (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) as required, to satisfy CI requirements in support of USSTRATCOM (b)(1) Sec 1.7(e)

5. (U) Command and Control

a. (U) Command Relationships. This CONPLAN does not require an assumption of OPCON or TACON of Service CI elements. Commander, USSTRATCOM, through the CISO (b)(1) Sec 1.7(e) exercises staff coordination authority over supporting Service CI elements. If CDRUSSTRATCOM cannot obtain necessary agreement on an issue, CDRUSSTRATCOM will request resolution of the issue from the Director of CI, Deputy Assistant Secretary of Defense for Counterintelligence & Security, through the CJCS. Such requests will be forwarded via the JCID, to CJCS. Military Department/Service CI units designated to support operations retain their command and organizational integrity. Administrative control also remains with the CI organization of each Military Department/Service. CI units are responsible for supporting their Services and responding to CISO (b)(1) Sec 1.7(e) requests for support and coordination. All CI activity will be conducted in conformity with legal and policy restrictions regarding CI activities (b)(1) Sec 1.7(e)

b. (U) Command, Control, Communications, Computers, and Intelligence (C4I). Reporting will be in accordance with established Service procedures and channels and in message format. Message traffic will be addressed to USSTRATCOM OFFUTT AFB NE// for (b)(1) Sec 1.7(e) or SSOSTRATCOM//J2// for (b)(1) Sec 1.7(e)

Tabs:
A - (U) Counterintelligence (CI) Target List – Not used.
B - (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) USSC
C - (U) Umbrella CI Force Protection Source Operation Proposal – Not used.

Kevin P. Chilton
General, USAF
COMMANDER

(INTENTIONALLY BLANK)

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE, NE 68113-6500
28 February 2008

APPENDIX 4 TO ANNEX B TO CDRUSSTRATCOM CONPLAN 8039 (U)
(U) OPR: JFCC NW J2
(b)(1) Sec 1.7(e) (U)

(U) References. Refer to Base Plan.

a. (U) (b)(1) Sec 1.7(e) 20 Mar 2006 (S).

b. (U) (b)(1) Sec 1.7(e) 13 Apr 2007 (U).

1. (~~S//REL USA, AUS, GBR~~) Situation. This appendix provides a review of general responsibilities and procedures for (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

a. (U) (b)(1) Sec 1.7(e) Refer to Annexes B (Intelligence) and (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

b. (U) Friendly. Refer to Base Plan.

c. (U) Assumptions. Refer to Base Plan.

2. (U) Mission. Refer to Base Plan.

3. (U) Execution

a. a. (~~C//REL~~) (b)(1) Sec 1.4(a) HQ USSTRATCOM/J2 will coordinate all (b)(1) Sec 1.4(a) to support HQs staff elements. USSTRATCOM JFCCs and subordinate commands will manage (b)(1) Sec 1.4(a) for their organizations and manage/coordinate (b)(1) Sec 1.4(a) conducted by assigned intelligence analysts. Individual USSTRATCOM components will manage (b)(1) Sec 1.4(a) for their specific operating environment in coordination with HQ USSTRATCOM/J2, other USSTRATCOM components, other COCOM/J2s, (b)(1) Sec 1.4(a) other USG agencies, and

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 06 December 2032~~

the IC. DOD Component J2 (b)(1) Sec 1.4(a) elements will coordinate and/or assist

with (b)(1) Sec 1.4(a) among other things:

(1) (U) Determine (b)(1) Sec 1.7(e) at strategic, operational, and tactical levels.

(2) (U) Identify the (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e).

(3) (U) Project how the (b)(1) Sec 1.7(e)

(4) (~~S//REL USA, AUS, GBR~~) Review Intelligence, Surveillance and Reconnaissance (ISR) (b)(1) Sec 1.4(a)

b. (~~C//REL~~) (b)(1) Sec 1.4(a). USSTRATCOM/J5 will lead, record, coordinate and update CDR USSTRATCOM (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Individual USSTRATCOM component J5 elements will record, validate, coordinate, and update (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) In addition, HQ USSTRATCOM/J5 will coordinate with all involved (b)(1) Sec 1.4(a) related to the plan. Individual USSTRATCOM/J5 elements will perform the same function at the component level related to supporting plans. HQ USSTRATCOM/J5 (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Individual USSTRATCOM/J5 elements will perform the same function at the component level. DOD Components and JIATF members will maintain and share cyberspace situational awareness.

(1) (U) Component SJA elements will maintain approved Supplemental Rules of Engagement.

(2) (U) Component J5 elements will maintain respective (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(3) (U) Component J5 elements, supported by their respective J2 elements, (b)(1) Sec 1.7(e) USSTRATCOM organizational oversight.

c. (U) (b)(1) Sec 1.7(e)

(1) (~~C//REL~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) elements responsible for the (b)(1) Sec 1.4(a) Traditionally, external organizations conduct the majority of (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) JFC staff. However, (b)(1) Sec 1.4(a) procedures and the scarcity and dispersion of cyber space (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(2) (~~C//REL~~) At any time, any agency may (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(a) (U) (b)(1) Sec 1.7(e) the best opportunity for recommendations to (b)(1) Sec 1.7(e) include:

1. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

2. (U) LOAC, ROE, or treaty considerations

3. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

4. (U) Intelligence (b)(1) Sec 1.7(e)

5. (U) (b)(1) Sec 1.7(e)

6. (U) (b)(1) Sec 1.7(e)

7. (U) (b)(1) Sec 1.7(e)

8. (U) To deconflict with friendly operations

(b) (~~C//REL~~) Component (b)(1) Sec 1.4(a) will maintain the authoritative (b)(1) Sec 1.4(a)

(3) (U) Component (b)(1) Sec 1.7(e) elements will request approval via JS (b)(1) Sec 1.7(e) IAW the (b)(1) Sec 1.7(e) thresholds or ROE.

d. (U) Capabilities Analysis. Under the oversight and direction of STRATCOM J2, component (b)(1) Sec 1.7(e) J3, and J8 elements will determine asset capability and availability, and, in coordination with individual component J2 and SJA, will estimate (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) Individual components and mission partners will consider (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

e. (U) Commander's Decision and Force Assignment

(1) (~~C//REL~~) Component (b)(1) Sec 1.4(a) will establish (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) to present (b)(1) Sec 1.4(a) for approval.

(2) (U) (b)(1) Sec 1.7(e) will match their components' (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) This action will take into account the results of capabilities analysis as well as (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(3) (~~C//REL~~) (b)(1) Sec 1.4(a) available will (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) as soon as possible in a subsequent (b)(1) Sec 1.4(a)

f. (U) Mission Planning and (b)(1) Sec 1.7(e) Component J3s will ensure tasked units (b)(1) Sec 1.7(e) IAW the applicable (b)(1) Sec 1.7(e)

g. (~~C//REL~~) (b)(1) Sec 1.4(a) In coordination with component J3s, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

h. .(~~C~~) (b)(1) Sec 1.4(a) If operations (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) will modify this Appendix and other documents to incorporate (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) associated with (b)(1) Sec 1.4(a) provide enough data to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

i. (~~S//REL USA, AUS, GBR~~) Definitions

(1) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) USSTRATCOM is defined as (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

by the commander through (b)(1) Sec 1.4(a) including (b)(1) Sec 1.4(a) This knowledge of the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) permits commanders to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(2) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(3) (~~S//REL USA, AUS, G~~BR) Situational Awareness (SA). This activity encompasses (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) all echelons of the chain of command establish and maintain an understanding of the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(4) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

j. (~~S//REL USA, AUS, GBR~~) Coordinating Instructions. (b)(1) Sec 1.4(a) should compare and evaluate the merit (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

4. (U) Administration and Logistics. Refer to Base Plan.

5. (U) Command and Control. Refer to Base Plan, Annexes J (Command and Control) and K (C4 Systems).

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

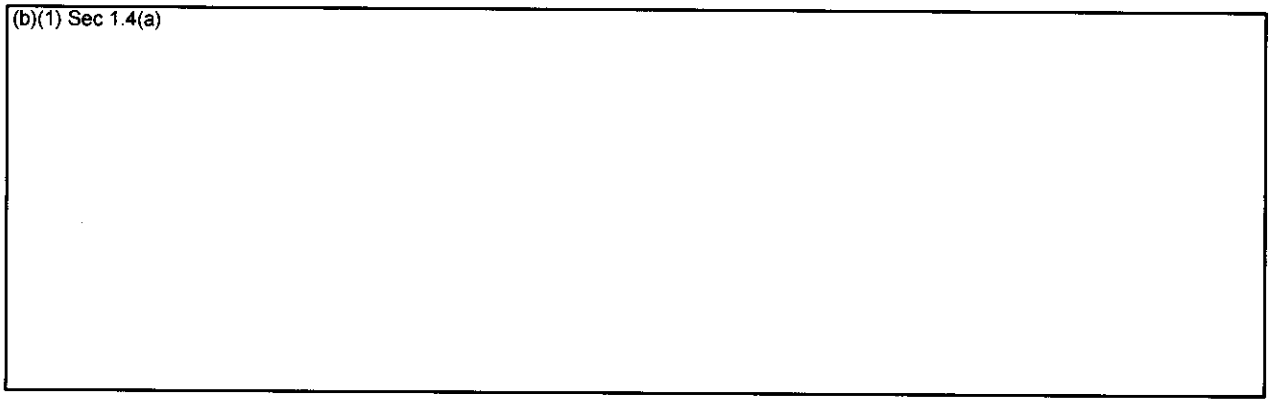


Figure B-4-1 (b)(1) Sec 1.4(a) (S//REL USA, AUS, GBR)

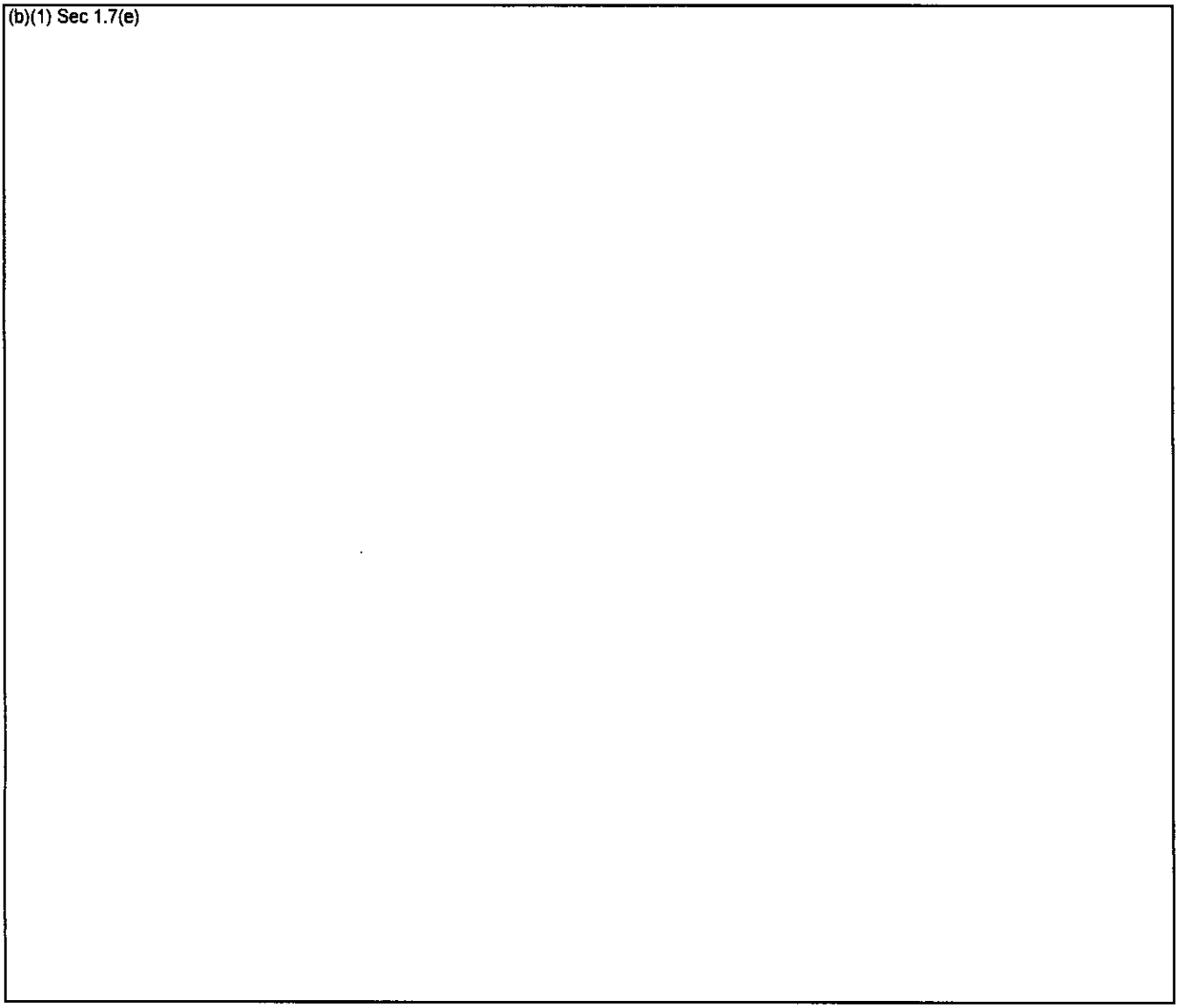


Figure B-4-2 (b)(1) Sec 1.7(e) (U//FOUO)

Kevin P. Chilton
General, USAF
COMMANDER

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE, NE 68113-6500
28 February 2008

APPENDIX 5 TO ANNEX B TO CDRUSSTRATCOM CONPLAN 8039 (U)
(U) OPR: HQ J2
(b)(1) Sec 1.7(e) (U)

(U) References:

a. (U) (b)(1) Sec 1.7(e) 3 Aug 98 (S//NF).

b. (U) (b)(1) Sec 1.7(e) 30 Jun 97 (S).

c. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (DRAFT) (S//NF).

d. (U) (b)(1) Sec 1.7(e) 1 Jun 92 (S//NF).

e. (U) Joint Pub 2-01, Joint Intelligence Support to Military Operations, Appendix C, 7 Oct 04 (U).

f. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) 7 Mar 2006 (S//NF).

1. (U) Situation. This appendix reviews general responsibilities and procedures for submitting (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

a. (U) (b)(1) Sec 1.7(e) Refer to 8039 Annex B (Intelligence) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

b. (U) Friendly. Refer to Base Plan.

c. (U) Assumptions. Refer to Base Plan.

2. (U) Mission. Refer to Base Plan.

3. (U) Execution. Refer to Annex B (Intelligence), para. 3.

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2032~~

a. (U) Organization. USSTRATCOM/J2 (b)(1) Sec 1.7(e) management support to HQs staff elements per ref (f). USSTRATCOM JFCCs, components, and subordinate commands perform cyber operations (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) for their organizations. JFCC ISR will closely collaborate with USSTRATCOM subordinate J2 (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) Ultimately, reporting agencies will be responsible to the Command and its subordinates.

b. (U) Concept of Operations. USSTRATCOM (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) are assigned to USSTRATCOM, JFCCs, or other component organizations, CONOPS for the (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) will be developed by the receiving organization and coordinated with USSTRATCOM/J2.

(1) (U) Tasks. Not applicable.

(2) (U) Requirements and Reporting. See refs (a) and (f) for the authorities, procedures, and formats for submitting (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(a) (C//REL) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b) (U) (b)(1) Sec 1.7(e) See para. 3.b.(2)(a) above.

(c) (U) External Tasking of (b)(1) Sec 1.7(e) Not applicable.

(d) (U) Other (b)(1) Sec 1.7(e) Reporting Procedures/Formats. Not applicable.

(e) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

c. (U) Coordination

(1) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) in support of this CONPLAN.

(2) (U) (b)(1) Sec 1.7(e) to USSTRATCOM provides (b)(1) Sec 1.7(e) coordination. The (b)(1) Sec 1.7(e) USSTRATCOM/J2 and other command

elements are kept fully aware of (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) requirements.

(3) (U) (b)(1) Sec 1.7(e) liaise with Commander, USSTRATCOM, component commands, and assigned units. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

4. (U) Administration and Logistics. See Annex B (Intelligence).

5. (U) Command and Control. See Annexes B (Intelligence) and J (Command and Control).

a. (U) Command Relationships. Not applicable.

b. (U) Communications. Not applicable.

Kevin P. Chilton
General, USAF
COMMANDER

(INTENTIONALLY BLANK)

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE, NE 68113-6500
28 February 2008

APPENDIX 6 TO ANNEX B TO CDRUSSTRATCOM CONPLAN 8039-07(U)
(U) OPR: HQ USSTRATCOM/J2
INTELLIGENCE SUPPORT TO INFORMATION OPERATIONS (IO) (U)

(U) References:

a. (U) Joint Pub 2-0, Joint Doctrine for Intelligence Support to Operations, 9 Mar 2000 (U).

b. (U) Joint Pub 2-01, Joint and National Intelligence Support to Military Operations, 7 Oct 2004 (U).

c. (U) Joint Pub 3-13, Joint Doctrine for Information Operations, 13 Feb 2006 (U).

d. (U) (b)(1) Sec 1.7(e) 13 Apr 2007 (U).

e. (U) Joint Pub 5-0, Doctrine for Planning Joint Operations, 26 Dec 2006 (U).

f. (U) Defense Intelligence Management Document, DI-2700-75-99, Analyst Information Requirements for Information Operations / Information Warfare, Feb 1999 (U).

(U) 1. ~~(S//REL USA, AUS, GBR)~~ Situation. This appendix specifies how information operations intelligence support will be conducted in support of USSTRATCOM CONPLAN 8039. See also Appendix 3 to Annex C (Information Operations) and Annex B (Intelligence).

a. (U) (b)(1) Sec 1.7(e) Refer to Annexes B (Intelligence) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

b. (U) Friendly

(1) ~~(S//REL USA, AUS, GBR)~~ Production Management. Production

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2032~~

management for this plan is organized using the IP processes and documented in the (b)(1) Sec 1.4(a) IO crosses the functional responsibility of several intelligence agencies and production centers often requiring direct coordination.

(2) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(a) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(b) (S//REL USA, AUS, GBR TO USA, ACGU) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(c) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) that assist a wide range of planning options.

(d) (~~S//REL USA, AUS, GBR~~) USSTRATCOM and its JFCCs collaborate with the (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) IO.

(3) (~~S//REL USA, AUS, GBR~~) IO (b)(1) Sec 1.4(a) Information is
(b)(1) Sec 1.4(a)
developed with:

(a) (U) JCS - J2S: Coordination of Political-Military Assessments and compartmented requests for information (RFIs).

(b) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
level for support to 8039's intelligence requirements.

(c) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
the Headquarters building.

(d) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) via an assigned LNO.

(e) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(f) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) to enable combat commanders to develop operational courses of action. They serve operational
(b)(1) Sec 1.4(a)
databases, and detailed analysis.

(4) (U) Staff Coordination. Cyber intelligence requirements may require other support (e.g., collection and counter intelligence support). To facilitate this intelligence support, JIOWC coordinates with the following internal staff offices:

(a) (U) (b)(1) Sec 1.7(e)

(b) (U) (b)(1) Sec 1.7(e) support.

(c) (U) JIOWC Intelligence Operations assistance

(d) (U) (b)(1) Sec 1.7(e)

c. (U) Assumptions. Refer to the Base Plan and Annex B (Intelligence).

2. (U) Mission. Refer to the Base Plan.

3. (U) Execution

a. (~~S//REL USA, AUS, GBR~~) Operational Requirements. IO requires broad-based, dedicated intelligence support. (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
and access must be developed as early as possible. For example, (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) source of intelligence.

b. (~~S//REL USA, AUS, GBR~~) Information Requirements. (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
must be made. It is critical that (b)(1) Sec 1.4(a) of the

(b)(1) Sec 1.4(a) kept current. Identifying requirements and initiating collection (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(1) (~~S//REL USA, AUS, GBR~~) Leadership. (b)(1) Sec 1.4(a) of key personnel, strategic communications, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) etc) will require updating.

(2) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(3) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(4) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(5) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) etc.

(6) (U) Military and Civil (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) for example.

(7) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) of the operation, for example.

(8) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) validated prior to release.

c. (U) Collection

(1) (U) Collection Management. JIOWC will coordinate with respective J2 elements to ensure de-confliction of IO intelligence requirements.

(2) (U) Supporting Systems

(a) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) requirements will focus on the aforementioned (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b) (U) (b)(1) Sec 1.7(e) supports all elements of IO. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) of IO.

(c) (U) OSINT. Open Source Intelligence includes radio, television, speeches, newspapers, technical manuals, and the Internet. Along with public polling and survey data, such OSINT (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(3) (~~S//REL USA, AUS, GBR~~) Capabilities Analysis. Access to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Additionally, intelligence to support cyberspace will require extensive (b)(1) Sec 1.4(a) analysts.

(4) (U) Processing, Production, Application, and Dissemination

(a) (U) Communication with Collection Management. Continuous assessment and analysis of intelligence collection is necessary in order to anticipate and/or react to the information situation as it develops.

(b) (U) Coordination. IO planners coordinate directly throughout the planning process and ensure that the appropriate J2 elements are included in planning at the appropriate phases.

(c) (U) Correlation. Information will be provided directly to the operator in a wide variety of formats. Products will be considered "draft" until reviewed and coordinated by the appropriate leadership.

(d) (U) Foreign Capability or Activity Assessment. N/A

(e) (U) (b)(1) Sec 1.7(e) to Annex B (Intelligence).

(f) (U) Database Management. Web-based tools and services, (b)(1) Sec 1.7(e)

(g) (U) (b)(1) Sec 1.7(e) N/A

(h) (U) C4 Network Analysis. USSTRATCOM plans, integrates and coordinates DOD GNO by directing GIG operations and defense, and identifies and advocates these desired characteristics and capabilities. USSTRATCOM

integrates global C2 networks, identifies desired C2 capabilities, develops architectures and concepts, and manages doctrine development. USSTRATCOM's operations and C2 centers provide rapid integrated C2 for employing military capabilities.

(i) (U) Capabilities Analysis. N/A

4. (U) Sustaining Functions

a. (~~S//REL USA, AUS, GBR~~) Automated data processing. Computer requirements must meet the accreditation requirements of the network. The (b)(1) Sec 1.4(a)

(1) (U) (b)(1) Sec 1.7(e)

(2) (U) (b)(1) Sec 1.7(e)

(3) (U) (b)(1) Sec 1.7(e)

(4) (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

b. (U) Capabilities Analysis. Not used.

c. (U) Communications. (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

5. (U) Command and Control. Refer to Annex B (Intelligence).

Kevin P. Chilton
General, USAF
COMMANDER

INTENTIONALLY BLANK

(a) (U) OASD/PA provides overarching guidance and policy to combatant command PA personnel. This guidance will be disseminated by USSTRATCOM/PA and/or the supported/supporting GCC/PA.

(b) (U) After the initial announcement of the execution of this plan, OASD/PA may delegate release authority to the supported commander. Once delegated this responsibility, the supported commander will determine if, when, and what release authority will be delegated to component/supporting commands and operational task forces.

(c) (U) USSTRATCOM will lead the coordination of information among OASD/PA, JFCC NW/PA, JTF GNO/PA and the affected COCOM(s) as quickly and as often as required. USSTRATCOM will issue PA guidance as required.

(d) (U) Detailed interaction and coordination among PA, IO, and DOD PA must occur throughout all phases of any operation.

e. (U) Security Review. Although "information sharing" is key, PA offices at all levels must exercise "security at the source." OPSEC will be considered throughout all phases of the operation. The supported command PA function will conduct security and policy review when necessary.

4. (U) Admin and Logistics. Refer to Base Plan.

5. (U) Command and Control. Refer to Base Plan and Annex J (Command Relationships).

Kevin P. Chilton
General, USAF
Commander

OFFICIAL:

JILL H. VOTAW
CAPT, USN
Chief, Public Affairs

(a) (U) Ensure subordinate units receive and comply with the PA policy and guidance in this Annex, and any other specified OASD/PA-approved PAG.

(b) (U) Propose information that can be used for a detailed PA communication plan, or Proposed Public Affairs Guidance (PPAG).

(c) (U) Coordinate any planned PA programs and activities related to this plan with USSTRATCOM/PA.

(d) (U) Develop local PA annexes to supporting plans assigning responsibilities and providing command-specific guidance (public information, internal information, and community relations) necessary to successfully implement this plan. As appropriate, coordinate PA annexes of supporting plans with logistics, communications and operations planners, and USSTRATCOM/PA.

(e) (U) Be prepared to exercise release authority delegated to Component Commanders or Task Force Commanders (TFC).

(f) (U) Provide Component Commanders and TFCs advice and counsel on PA matters concerning USSTRATCOM operations, as required, and immediately inform USSTRATCOM/PA of any incident or action resulting from communications that are likely to require action at the USSTRATCOM; Service; Joint Staff or OASD level; be of immediate news interest; or cause unfavorable public reaction or publicity.

d. (U) Coordinating Instructions

(1) (U) Release Authority. Release authority will be delegated to the lowest level possible consistent with published PA guidance.

(2) (U) Reporting Requirements. All supporting PA functions will provide a daily SITREP, by 1700 ZULU, to USSTRATCOM/PA, via NIPR email if possible. The SITREP will include: electronic copies or internet links of articles published in the preceding 24 hours; planned press releases; a summary of completed PA actions and future media engagements; a list of PA personnel deployed; and any new messages or talking points. USSTRATCOM will publish a consolidated SITREP each day.

(3) (U) There will be no releases, statements, responses to media inquiries or other public announcements by USSTRATCOM or assigned forces concerning this plan without authorization from OASD/PA. The general conduct and control of PA activities will be as follows:

(1) (U) PA will:

(a) (U) Be involved in all appropriate planning boards and groups to include Information Operations Working Groups (IOWG), Operational Planning Groups and Long Range Planning Elements, etc.

(b) (U) Plan for specific contingencies and formulate tailored courses of action for each Phase of operations to affect regional and international opinion.

(c) (U) Counter enemy propaganda with the truth. Actively use truthful, fact-based, accurate and timely public information products to respond to enemy threats, deception and lies.

(d) (U) Ensure all personnel required to interact with media and the community are well-versed on the PA guidance, media guidelines, and prepared to assist media members as necessary.

(e) (U) As news releases and statements are issued to the media, they should also be disseminated to the internal audience via SKIWEB, STRATWEB, and other available resources.

(2) (U) CDRUSSTRATCOM will: Assign high priority to PA programs and direct commanders to assign dedicated assets and support a PA program consistent with OPSEC, INFOSEC, PAG, regulations and policies.

(3) (U) USSTRATCOM/PA will:

(a) (U) Provide CDRUSSTRATCOM and his staff advice and counsel on PA matters concerning operations as required. Develop PA policy, guidance and plans as required.

(b) (U) Maintain liaison with OASD/PA, JFCC NW/PA, JTF_GNO/PA, and GCC/PAs on PA policy matters.

(c) (U) Coordinate PA activities with IO and SC to synchronize themes and messages.

(d) (U) Ensure rapid communication of PAG to component and task force PA offices.

(4) (U) Geographic Combatant Command PA (GCC/PA) will: Provide regular feedback on significant PA activity within the area of responsibility/ area of interest to OASD/PA, CJCS/PA and USSTRATCOM/PA.

(5) (U) USSTRATCOM Component Command /Task Force PA Offices will:

used as a military deception capability or to provide disinformation to internal or external audiences.

2. (U) Mission. Refer to Base Plan.

3. (U) Execution

a. (U) Concept of Operations. The supported command for execution will lead the efforts to develop, coordinate and synchronize a comprehensive PA program with the supporting PA functions and OASD/PA, which is aligned with and directly supports USG communication objectives. As a supporting command, USSTRATCOM retains responsibility for providing coordinated JFCC NW and JTF GNO PA products (in addition to other USTRATCOM components as applicable) to the supported command PA function. Regardless, the intent is to provide truthful information of sufficient breadth and timeliness which supports the efforts to educate the audience with the cyberspace domain and its impact on military operations.

b. (U) Themes and Messages. The following overarching themes and messages are contained in NSPD 38.

(1) (U) The US is committed to ensuring the free and secure flow of information through cyberspace. Global economic growth and security depend upon the networks and systems that constitute cyberspace. Maintaining freedom of action in cyberspace in the 21st Century is as inherent to US interest as freedom of the seas became in the 19th Century and access to air and space in the 20th Century.

(2) (U) We will continue to lead international and domestic efforts to ensure the security of global information infrastructures upon which cyberspace depends.

(3) (U) The US reserves the right to respond to attacks in and through cyberspace by nations, terrorist groups, or other adversaries in a manner it deems appropriate.

(4) (U) We will maintain the capabilities to operate in the cyberspace domain to deter, deny, or defeat any adversary that seeks to harm US national and economic security.

(5) (U) We will ensure that our actions in this domain are undertaken in a manner that is lawful and protects our Constitutional liberties.

c. (U) Tasks. Consistent with current OASD/PA guidance, and within the constraints of Operations Security (OPSEC), Information Security (INFOSEC), safety and privacy of US military personnel, their families and DOD civilians;

k. (U) DOD Instruction 5410.19, Public Affairs Community Relations Policy Implementation, 13 November 2001

1. (U) Situation

a. (U) General

(1) (U) This annex assigns responsibilities and provides overarching guidance for military Public Affairs (PA) activities in support of CDRUSSTRATCOM CONPLAN 8039-07(S) for combatant and supporting commands.

(2) (U) The preeminent factor in PA support of this strategic concept involves coordinating and communicating DOD efforts in broad themes and public affairs strategies by establishing a common context in the cyberspace domain for military areas of operation and developing a deeper understanding of this domain and its impact on warfighting. In support of this plan, PA efforts must be well-synchronized with other USG and DOD communication strategies. This requires a comprehensive PA plan that extends from OASD/PA to USSTRATCOM, its components, and integrated with Geographic Combatant Commands (GCC) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

b. (U) (b)(1) Sec 1.7(e) Refer to Base Plan.

c. (U) Friendly. Refer to Base Plan.

d. (U) Assumptions. Refer to Base Plan.

e. (U) Policy. PA is a function of command and consists of public information, internal (or command) information, and community relations activities designed to educate and inform external and internal publics and stakeholders. Public Affairs activities are conducted in accordance with existing DOD directives and policy, the DOD Principles of Information, and current Office of Assistant Secretary of Defense for Public Affairs (OASD/PA) guidance. Other policy considerations follow:

(1) (U) PA activities are complementary to, yet distinct from, Information Operations (IO). PA activities contribute to IO by providing truthful, fact-based, accurate and timely information, using approved OASD public affairs guidance (PAG), to keep the public informed about the military's missions and operations in support of military objectives, countering enemy propaganda, dissuading and deterring enemy actions, and maintaining the trust and confidence of the US population, our friends and allies. By law, and by doctrine, PA activities are prohibited from intentionally deceiving the public. PA activities will not be

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AFB, NE 68113-6500
28 February 2008

ANNEX F TO CDRUSSTRATCOM CONPLAN 8039 (U)
(U) OPR: USSTRATCOM J020
PUBLIC AFFAIRS (U)

(U) References: Refer to Base Plan.

a. (U) JP 3-61, Doctrine for Public Affairs in Joint Operations, 14 May 1997

b. (U) DOD Directive 5122.5, Assistant Secretary of Defense for Public Affairs, 27 Sep 2000

c. (U) DOD Directive 5200.1, DOD Information Security Program, 13 December 1996

d. (U) DOD Directive 5230.9, Clearance of DOD Information for Public Release (Change 1), 15 July 1999

e. (U) DOD Instruction 5230.29, Security and Policy Review of DOD Information for Public Release, 6 August 1999

f. (U) DOD Directive 5400.13, Joint Public Affairs Operations, 9 January 1996

g. (U) DOD Instruction 5400.14, Procedures for Joint Public Affairs Operations, 22 January 1996

h. (U) DOD Instruction 5405.3, Development of Proposed Public Affairs Guidance, 5 April 1991

i. (U) DOD Instruction 5410.15, DOD Public Affairs Assistance to Non-Government, Non-Entertainment-Oriented Print and Electronic Media, 28 March 1989

j. (U) DOD Directive 5410.18, Community Relations Policy, 20 November 2001

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 27 February 2033~~

(4) (U) Other USSTRATCOM components will review and provide CONPLAN 8039 (b)(1) Sec 1.4(a) additions and deletions, to USSTRATCOM J534.

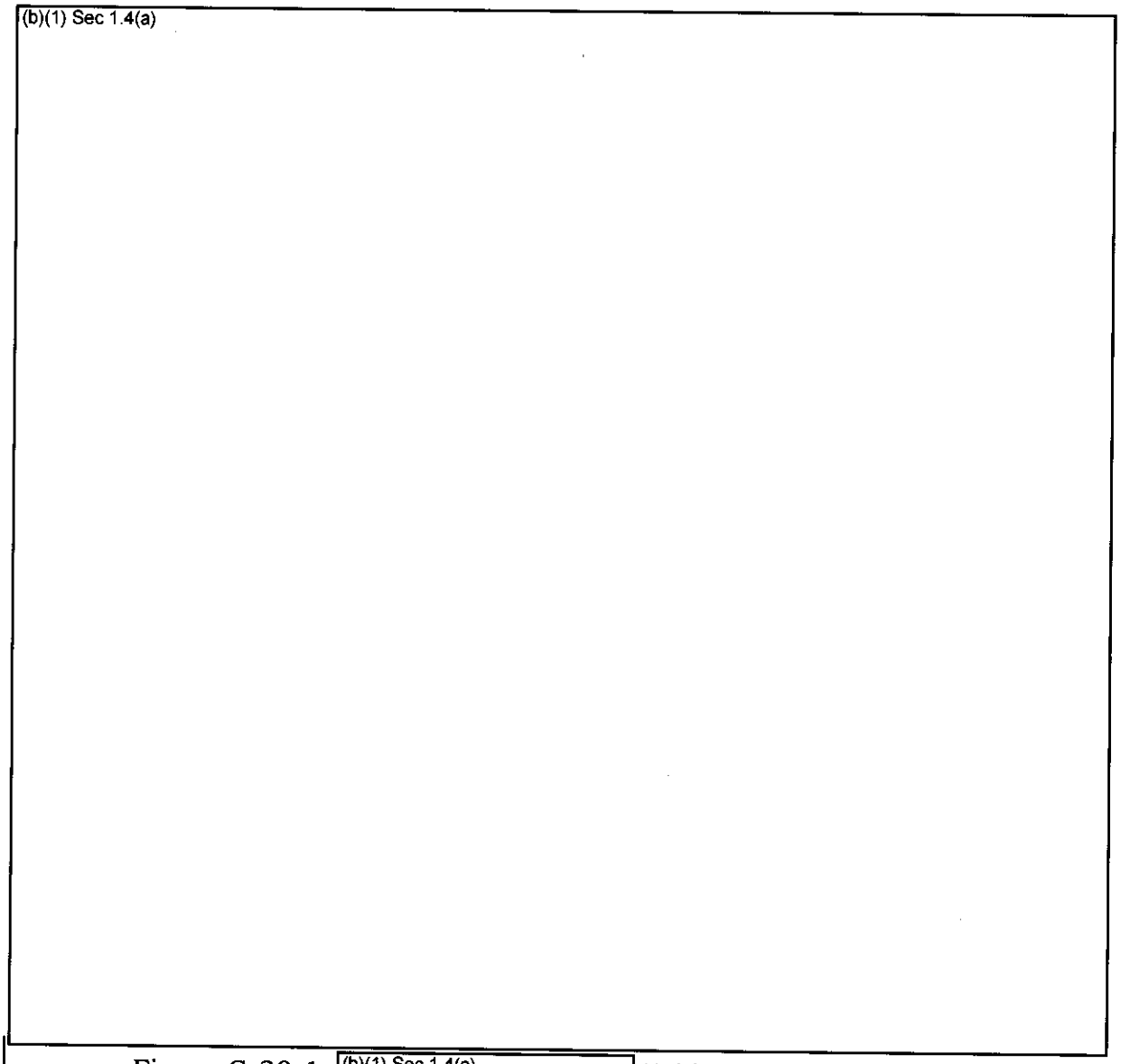


Figure C-20-1, (b)(1) Sec 1.4(a) (S//REL USA, AUS, GBR)

4. (U) Administration and Logistics. Refer to Base Plan.

5. (U) Command and Control. Refer to Base Plan.

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (e), and (g)~~
~~Declassify on: 27 February 2033~~

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE NE 68133-6500
27 February 2008

APPENDIX 20 TO ANNEX C TO CDR USSTRATCOM CONPLAN 8039 (U)
(U) OPR: JFCC NW J52
(b)(1) Sec 1.7(e) (U)

(U) References: Refer to Base Plan and Annex C (Operations).

1. (U) Situation. Refer to Base Plan.

2. (U) Mission. Refer to Base Plan.

3. (U) Execution

a. (~~S//REL USA, AUS, GBR~~) Concept of Operation. The (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
of the Base Plan.

b. (U) Tasks

(1) (U) HQ USSTRATCOM J534 will maintain the CONPLAN 8039 (b)(1) Sec 1.7(e) and receive inputs from USSTRATCOM components during CONPLAN 8039 periodic reviews.

(2) (~~S//REL USA, AUS, GBR~~) JTF_GNO will review and provide CONPLAN 8039 (b)(1) Sec 1.4(a) to include recommended additions and deletions, to USSTRATCOM J534 for (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a).

(3) (~~S//REL USA, AUS, GBR~~) JFCC NW will review and provide CONPLAN 8039 (b)(1) Sec 1.4(a) additions and deletions, to USSTRATCOM J534 for (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

operational or strategic level. (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(6) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(7) (U) Operational Effects: Desired operational-level outcomes necessary to achieve a phase objective. Operational effects incorporate all elements of national power available to the theater commander.

(8) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) systems for a specific purpose.

(9) (U) Political, Military, Economic, Social, Infrastructure, and Information (PMESII): Construct for defining systems behaviors.

(10) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
throughout the campaign.

f. (U) Tasks. Refer to Base Plan.

g. (U) Coordinating Instructions. Refer to Base Plan.

4. (U) Administration and Logistics. Refer to Base Plan.

5. (U) Command and Control. Refer to Base Plan.

(b)(1) Sec 1.4(a)

circumstances.

d. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) Commanders at all levels will ensure that (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) USSTRATCOM will integrate and coordinate DOD Components plans and address synchronization, advocacy, and allocation issues that arise.

e. (U) Definitions

(1) (U) Campaign effects: Desired theater-level outcomes or conditions that allow CDR UNC/CFC to achieve the operational objectives.

(2) (U) Effect: The physical, functional, or psychological outcome, event or consequence that results from a specific action or actions that produces desired changes in enemy actions, reactions, or inabilities to act.

(3) (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) provides a conceptual alternative to traditional attrition and maneuver warfare.

(b)(1) Sec 1.7(e)

(4) (U) Indicator: criteria that we are going to measure. Indicators may

(b)(1) Sec 1.7(e)

(5) (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(1) (U) Reassess the adversary utilizing the (b)(1) Sec 1.7(e) and threat analysis to determine the new (if any) cyberspace operations threat posed by that adversary.

(2) (U) Reassess the (b)(1) Sec 1.7(e) and determine if the actions applied cause a significant change in capability or intent of the actor.

(3) (U) Determine if any (b)(1) Sec 1.7(e) were met.

(4) (U) Assess resources to ensure current resources are adequate and sufficient. If additional resources or capabilities are required, USSTRATCOM, JCS, and OSD must re-enter the DOD PPBS cycle to address near and long term needs and to acquire, as quickly as possible, capabilities that address immediate needs.

(5) (U) Determine unintentional and undesired effects of actions applied. Ensure other DOD Components and USG agencies are aware of actions, as effects in cyberspace (with few exceptions) are trans-regional.

b. (U) If the applied tasks were not successful in achieving the desired effect:

(1) (U) Reassess the actor utilizing the (b)(1) Sec 1.7(e) and threat analysis to determine the new (if any) cyberspace operations threat that the adversary actor poses remains valid.

(2) (U) Evaluate the (b)(1) Sec 1.7(e)

(3) (U) Determine if other associated effects were met.

(4) (U) Assess current resources to ensure adequacy and sufficiency. If additional resources or capabilities are required, USSTRATCOM, JCS, and OSD must re-enter the DOD PPBS cycle to address near and long term needs and to acquire, as quickly as possible, capabilities that address immediate needs.

(5)(U) Determine if any unintentional and or undesired effects occurred. Ensure other DOD Components and USG agencies are aware of actions, as effects in cyberspace (with few exceptions) are trans-regional.

c. (~~S//REL USA, AUS, GBR~~) Interagency Efforts. Refer to Annex V (Interagency). USSTRATCOM, through OSD, JS, and in coordination with the applicable Combatant Commands' (b)(1) Sec 1.4(a) will engage the interagency to develop a common situational awareness of USG, (b)(1) Sec 1.4(a) and (b)(1) Sec 1.4(a) threats in cyberspace. (b)(1) Sec 1.4(a)

processes, the USSTRATCOM staff develops a (b)(1) Sec 1.4(a) across (b)(1) Sec 1.4(a)

(c) (U) (b)(1) Sec 1.7(e) Assessment Guidance.

1 (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Using available assessments and analysis, the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) operations in and through cyberspace. This may (b)(1) Sec 1.4(a) to re-align with new combatant commander's priorities.

2 (U) Assessing Effectiveness. Following the execution of cyberspace operations applied tasks; commanders responsible for the execution of those applied tasks assess the performance of tasks and report findings to the (b)(1) Sec 1.7(e)

3 (U) Assessing (b)(1) Sec 1.7(e) defined in para 3e(5)). USSTRATCOM HQ staff and applicable components assess (b)(1) Sec 1.7(e) for individual tasks conducted during the course of operations. When performing this assessment, answer the following questions: Are we doing things right? Were the tasks performed correctly? Insights into this aspect of task execution inform advocacy and military decision-making processes that support the cyberspace operations campaign cycle. The assessment of (b)(1) Sec 1.7(e) for newly integrated capabilities across the DOTMLPF informs the advocacy process by (b)(1) Sec 1.7(e) operational needs in terms of support and sufficiency. USSTRATCOM will assign an Office of Primary Responsibility (OPR) to each applied task. The OPR (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) for each applied task.

4 (U) Assessing (b)(1) Sec 1.7(e) defined in para 3e(4)). USSTRATCOM and Components must also assess the (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) will answer the questions: Are we doing the right things? Did the applied task have the desired effect on the threat? USSTRATCOM will assign an OPR to each applied task. The OPR (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

a. (U) If the applied tasks were successful in achieving the desired effect:

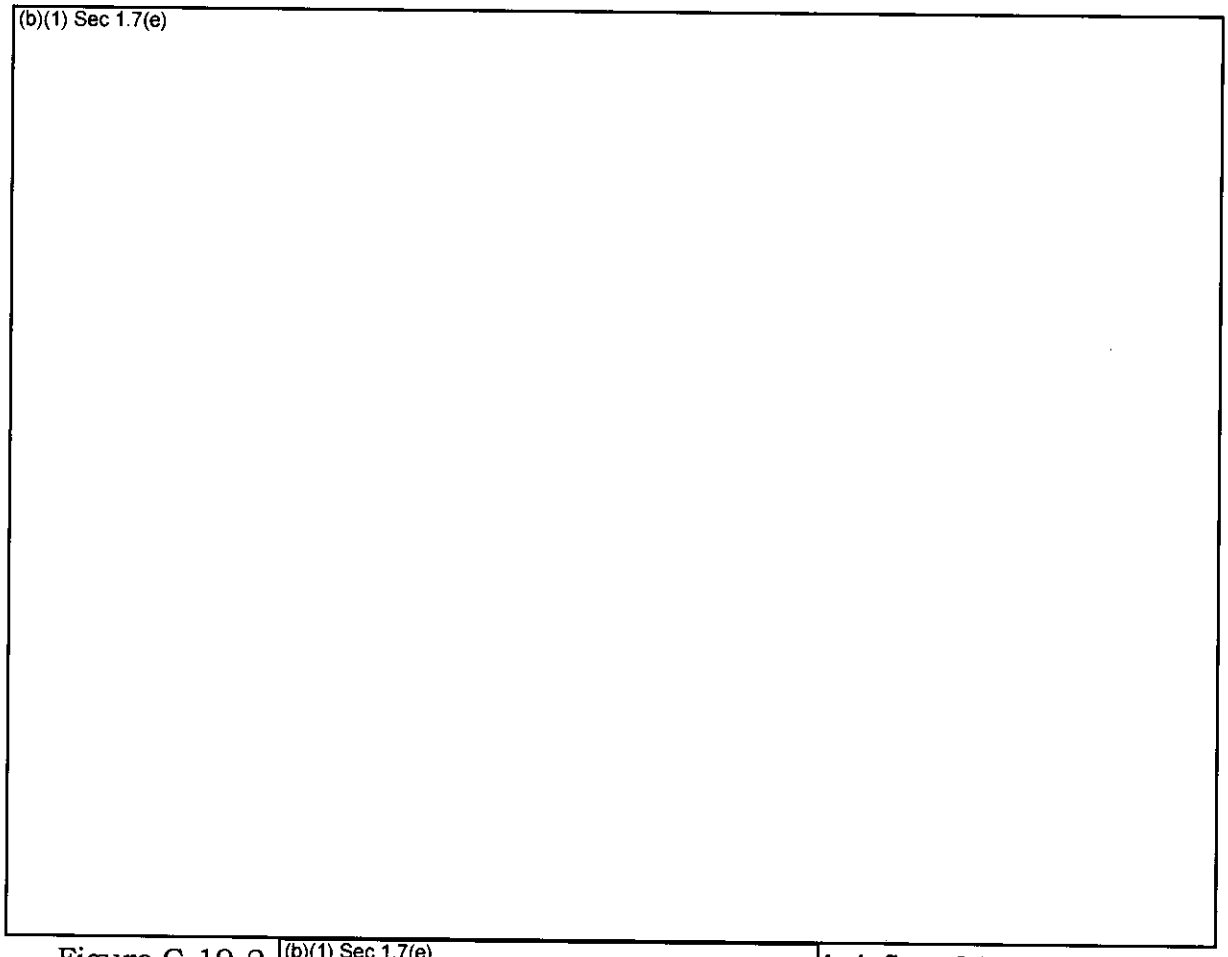


Figure C-19-2, (b)(1) Sec 1.7(e) briefing, May 2006) (U)

(3) (U) (b)(1) Sec 1.7(e)

(a) (U) (b)(1) Sec 1.7(e) The linkage above provides a baseline starting point to develop (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) operational level applied tasks.

(b) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Once specific (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) The overall criteria for the actual prioritization (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b) (U) The USSTRATCOM staff and components analyze the mission using all tools available- Operational Net Assessment (ONA, defined in para 3e(8)), CIE COA analysis, Virtual Information Environment (VIE), etc to understand the operational environment and determine what Political, Military, Economic, Social, Infrastructure, and Information (PMESII, defined in para 3e(10)) system behaviors and /or capabilities - (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) COCOM theater objectives.

(c) (U) Based on CDRUSSTRATCOM's verification of the task to objectives and the analysis of the adversary and the operational environment provided by the staff and components, the commander's intent is issued to all components and supporting agencies. This normally includes his vision of what needs to be done (purpose), a broad concept for how CDRUSSTRATCOM intends to accomplish the objectives (method) and key measures for determining success (end state). CDRUSSTRATCOM provides planning guidance to focus staff and component development of COAs to accomplish his vision/end state for (b)(1) Sec 1.7(e) CONPLAN 8039). COAs within (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) will fuse and synchronize the appropriate DIME and/or PMESII actions, in time and space, against those decisive points within the operational environment which most directly produce the effects that will achieve his stated objectives. The goal is unity of effort or harmonization of all elements of DIME/PMESII toward a common goal.

(d) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) which produce decision points (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) based upon the commander's guidance and intent. Refer to Base Plan for CONPLAN 8039 (b)(1) Sec 1.4(a)

(e) (U) USSTRATCOM integration and collaboration mechanisms will be used to develop (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) which is the primary means to provide operational level assessment. All appropriate DOD Components and USG Agencies will be invited to participate. (b)(1) Sec 1.7(e) (See Figure C-19-2 below).

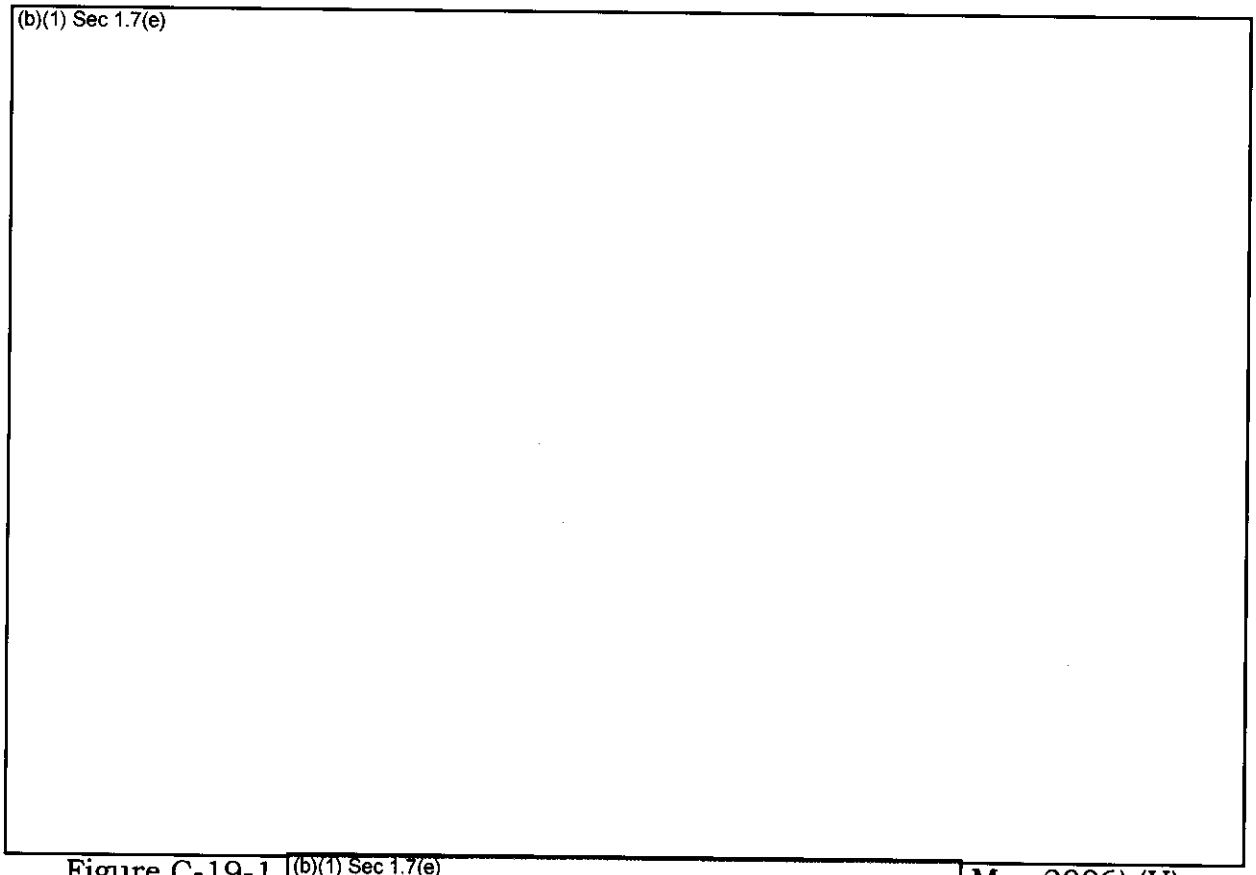


Figure C-19-1, (b)(1) Sec 1.7(e) May 2006) (U)

(1) (U) Evaluate and Prioritize Threat. (See (b)(1) Sec 1.7(e) for a detailed discussion of the (b)(1) Sec 1.7(e).

(2) (U) Tailored Planning

(a) (U) The tailored planning process uses an (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) Through an analysis of the national strategic objectives, utilizing the products from the (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) USSTRATCOM develops (b)(1) Sec 1.7(e) (CONPLAN 8039, reference chart with (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)
CONPLAN 8039 Base Plan.

4 (U) Emphasizes unity of effort through a strengthening of interagency operations by:

a. (U) Supporting improvements in strategy development and planning within DOD and with interagency partners to shift emphasis from DOD-centric approaches toward USG interagency and coalition/allied solutions.

b. (U) Developing stronger links between planners in the OSD, the Joint Staff, Combatant Commands, Services and the IC.

c. (U) Facilitating communication by developing shared perspectives and a better understanding of each agency's roles, missions, and capabilities.

d. (U) Improving the effectiveness of operations in and through cyberspace through the accomplishment of objectives and promoting efficiency throughout the operational mission area by effectively allocating, integrating, and using limited resources.

(c) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) established for this appendix (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) and as referenced in the CONPLAN 8039 base plan (para 3.a.(3).

b. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) This appendix provides a framework for continuous and sustained efforts throughout DOD (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) in an operational environment).

(3) (U) (b)(1) Sec 1.7(e) Refer to Base Plan and Annex A (Task Organization).

(4) (U) (b)(1) Sec 1.7(e) Refer to Base Plan and Annex B (Intelligence) (b)(1) Sec 1.7(e)

(5) (U) Friendly Capabilities. Refer to Base Plan and Annex A (Task Organization).

(6) (U) Assumptions. Refer to Base Plan and Annex C (Operations).

(7) (U) Legal Considerations. Refer to Base Plan and Annex C (Operations).

2. (U) Mission. Refer to Base Plan.

3. (U) Execution

a. (U) Concept of Operations

(1) (U) Commander's Intent

(a) ~~(S//REL USA, AUS, GBR)~~ Purpose. The purpose of CONPLAN 8039 (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
The purpose of this appendix is to set the framework for integration and synchronization of USSTRATCOM plans in support of operations in and through cyberspace, and define activities and metrics to assess their effectiveness. (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(b) (U) Method. This appendix uses a strategic framework that:

1 (U) Includes a process for the development of a (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) for CONPLAN 8039 is shown at Appendix 20 to Annex C.

2 (U) Includes an (b)(1) Sec 1.7(e) to describe the overall
(b)(1) Sec 1.7(e)

3 (U) Includes logical lines of operation in which DOD will focus
(b)(1) Sec 1.7(e)

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE NE 68133-6500
28 February 2008

APPENDIX 19 TO ANNEX C TO USSTRATCOM CONPLAN 8039 (U)
(U) OPR: JFCC NW/J52
(b)(1) Sec 1.7(e) GUIDANCE (U)

References: Refer to Base Plan.

a. (U) Commander's Handbook for an (b)(1) Sec 1.7(e) to Joint Operations, 24 Feb 06

1. (~~S//REL USA, AUS, GBR~~) Situation. Since the advent of the Information Age, the US, at all levels of government and society, has become increasingly dependent upon the world-wide network of software, computers, and telecommunications infrastructure as the foundation of our national economy. DOD (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

a. (U) General

(1) (~~S//REL USA, AUS, GBR~~) Function. This appendix describes plans and functions to integrate and synchronize STRATCOM's (b)(1) Sec 1.4(a) within the DOD GIG and operations in and through cyberspace in support of (b)(1) Sec 1.4(a) USSTRATCOM command goal. This appendix also expands upon the (b)(1) Sec 1.4(a) described in the CONPLAN 8039 Plan Summary (para 1.b(1)), Base Plan, and Annex C to (b)(1) Sec 1.4(a). This appendix describes the strategic framework within the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) cyberspace operations.

(2) (U) Area of Concern. Refer to Base Plan.

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 27 February 2033~~

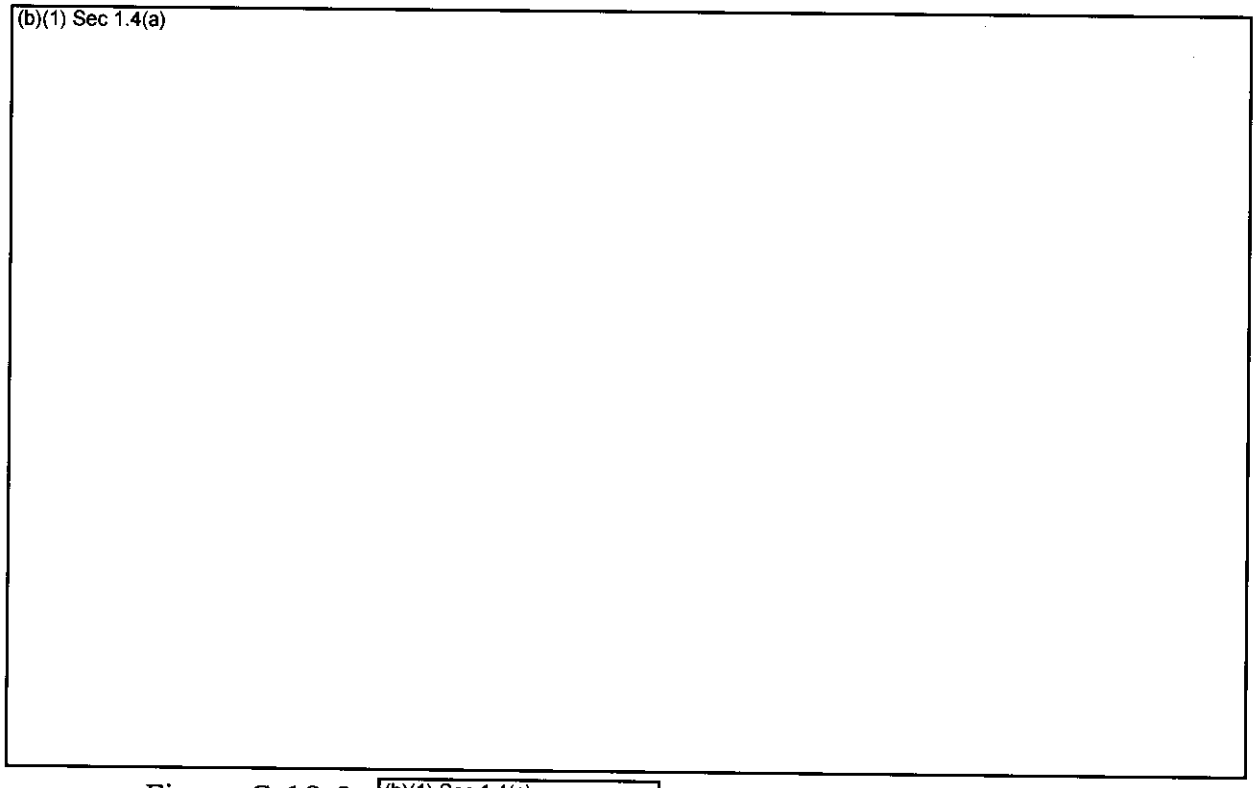


Figure C-18-3 – (b)(1) Sec 1.4(a) (S//REL USA, AUS, GBR)

(3) (~~S//REL USA, AUS, GBR~~) ICW JFCC GSI (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(4) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(5) (~~S//REL USA, AUS, GBR~~) Identify COA support requirements
(b)(1) Sec 1.4(a)

(6) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) if identified as supported commander.

(7) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
JFCC GSI a post mission analysis feedback.

(8) (~~S//REL USA, AUS, GBR~~) Request assistance in organizing, training and otherwise preparing (b)(1) Sec 1.4(a) from JFCC GSI, if required.

(9) (~~S//REL USA, AUS, GBR~~) Support JFCC GSI through the (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

c. Figure C-18-2 below is a graphical depiction of (b)(1) Sec 1.4(a)

(3) (~~S//REL USA, AUS, GBR~~) Prepare and maintain plans in support of (b)(1) Sec 1.4(a)

(4) (~~S//REL USA, AUS, GBR~~) Recommend (b)(1) Sec 1.4(a) when appropriate.

(5) (~~S//REL USA, AUS, GBR~~) Establish (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(6) (~~S//REL USA, AUS, GBR~~) Coordinate and lead the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) development.

(7) (~~S//REL USA, AUS, GBR~~) Provide support to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) as required or directed.

(8) (~~S//REL USA, AUS, GBR~~) In preparation for follow-on operations, monitor situations generated intelligence, follow-on operations possibilities, additional coordination requirements, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(U) (9) (~~S//REL USA, AUS, GBR~~) Ensure all open action items are evaluated for closure.

(10) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) conduct a post-mission analysis.

(11) (~~S//REL USA, AUS, GBR~~) Assist in organizing, training and otherwise preparing (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

b. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(1) (~~S//REL USA, AUS, GBR~~) Using existing infrastructures (i.e. CAT, Crisis Action Center [CAC], Command Center, Operations Center, Joint Operations Center [JOC], JIOC), (b)(1) Sec 1.4(a) The GCC determines the appropriate command and structure arrangements for respective (b)(1) Sec 1.4(a)

(2) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

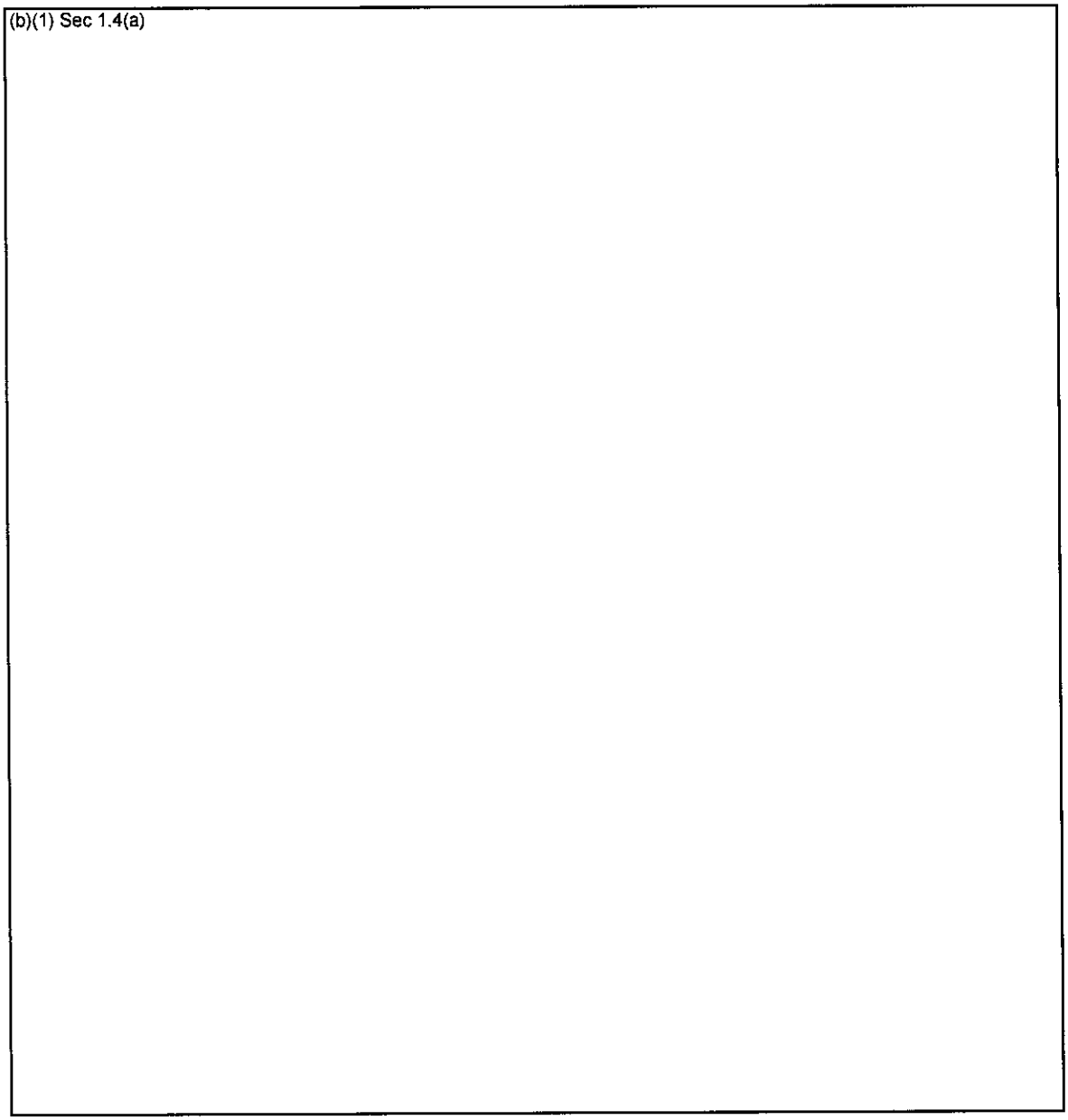


Figure C-18-2 – (b)(1) Sec 1.4(a) (S//REL USA, AUS, GBR)

3. (U) (b)(1) Sec 1.7(e) Responsibilities and Requirements.

a. (U) USSTRATCOM.

(1) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) operations under this plan, as required.

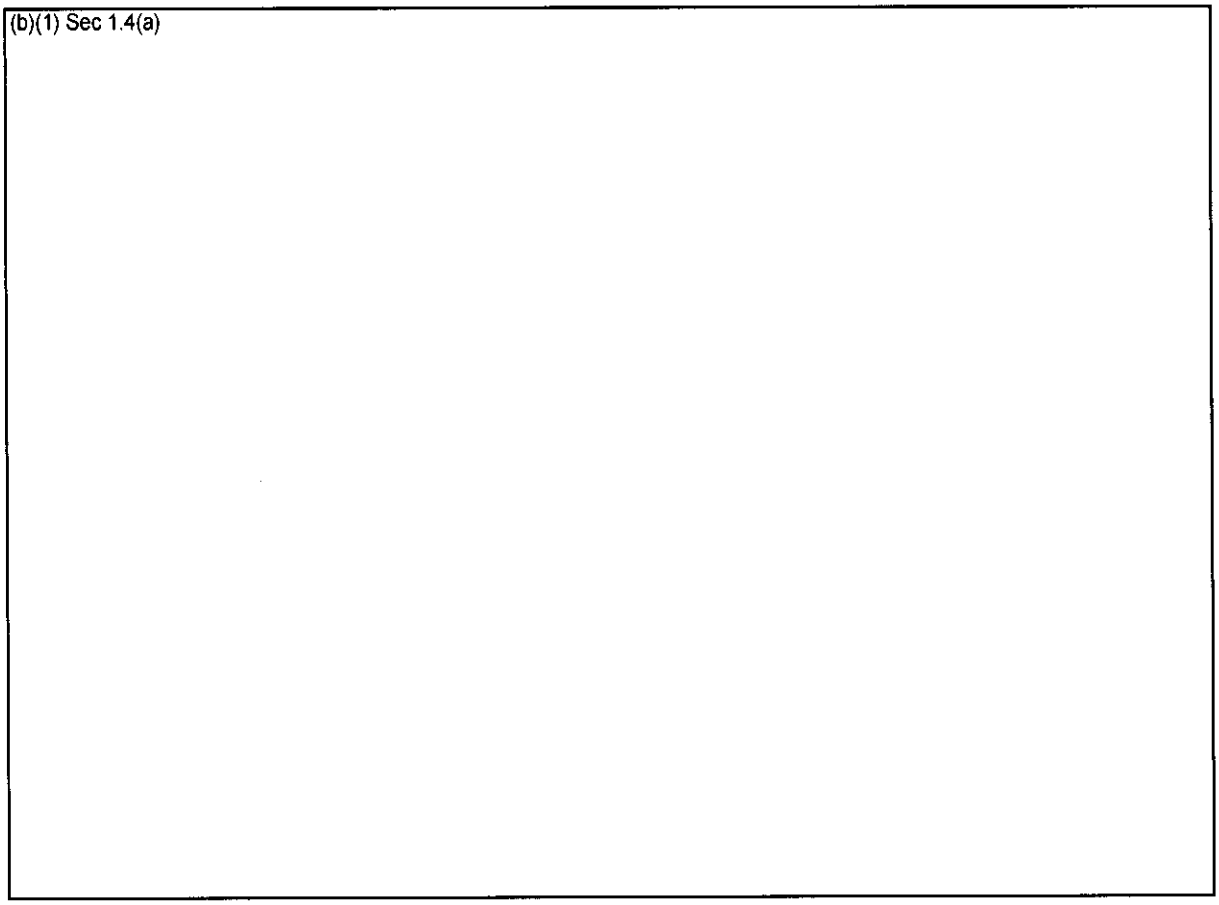
(2) (~~S//REL USA, AUS, GBR~~) Monitor through JFCC GSI (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(2) (~~S//REL USA, AUS, GBR~~) CDRUSSTRATCOM will review the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) USSTRATCOM operational recommendation.

e. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) The purpose of this (b)(1) Sec 1.4(a)

f. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) The supported Combatant Commander (b)(1) Sec 1.4(a)

g. (U) Figure C-18-2 below depicts the (b)(1) Sec 1.7(e)



(~~S//REL USA, AUS, GBR~~) Figure (C-18-1 – (b)(1) Sec 1.4(a)

c. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) The purpose of this (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

d. (U) (b)(1) Sec 1.7(e) The purpose of this (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) planning.

(1) (~~S//REL USA, AUS, GBR~~) JFCC GSI ICW the (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) USSTRATCOM operational recommendation. This recommendation will be presented for consideration to the Joint Staff and includes (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
USSTRATCOM recommendation for the way ahead.

(b)(1) Sec 1.4(a)

a. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
establish/manage the planning timeline and expectations.

(1) (~~S//REL USA, AUS, GBR~~) GCCs and JFCC GSI continuously analyze current intelligence to determine if sufficient information exists (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
Combatant Commanders, other government agencies, and other planning partners in attendance. (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(2) (~~S//REL USA, AUS, GBR~~) A (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
provides initial tasks for participants, delineates the planning timeline and collaboration instructions, defines required products, (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

b. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) The purpose of this
(b)(1) Sec 1.4(a)
determining potential solutions.

(1) (~~S//REL USA, AUS, GBR~~) JFCC GSI conducts and leads mission analysis in a (b)(1) Sec 1.4(a)
Combatant Commands, Services, and participating USG agencies (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(2) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) JFCC GSI works with the supporting (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(3) (~~S//REL USA, AUS, GBR~~) Mission analysis will produce a (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE, NE 68113-6500
28 February 2008

APPENDIX 18 TO ANNEX C TO USSTRATCOM CONPLAN 8039(U)
(U) OPR: JFCC GSI J39 OCR: 8 IOF
(b)(1) Sec 1.7(e) FOR CYBERSPACE OPERATIONS (U)

(U) References: See Base Plan and Annex C (Operations).

(U)1. (~~S//REL USA, AUS, GBR~~) Situation

a. (~~S//REL USA, AUS, GBR~~) General. (b)(1) Sec 1.4(a) is the process for producing USSTRATCOM recommended COAs (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) or when directed by the Joint Staff (JS), for CDRUSSTRATCOM. This process is generally used for (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) executed by USSTRATCOM, (b)(1) Sec 1.4(a) and other organizations in order to facilitate synchronized and integrated effects. Several variables may dictate that the cyberspace operations (b)(1) Sec 1.4(a) differ from what is found in this appendix, (b)(1) Sec 1.4(a) in addition depending on interagency involvement, (b)(1) Sec 1.4(a) circumstances may be encountered. These situations will be handled on a by case basis. For example, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) commence planning and coordination with JFCC GSI.

2. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 27 February 2033~~

(b)(1) Sec 1.4(a)

(c) (U) Coordinate with DOD Components to determine the operational impact of changing DOD INFOCON levels.

(d) (U) Provide recommended changes to DOD INFOCON levels to CDRUSSTRATCOM.

4. (U) Administration and Logistics. Refer to Base Plan.

5. (U) Command and Control. Refer to Appendix 17 (NetOps) to Annex C (Operations).

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE NE 68113-6500
28 February 2008

TAB E TO APPENDIX 17 TO ANNEX C TO CONPLAN 8039 (U)
(U) OPR: JTF-GNO J5
INFORMATION OPERATIONS CONDITION (INFOCON) (U)

References: Refer to Base Plan and Appendix 17 (NetOps) to Annex C (Operations).

1. (U) Situation. Refer to Base Plan.

2. (U) Mission. Refer to Base Plan.

3. (U) Execution

a. (U) Concept of Operation. The INFOCON system, including responsibilities, processes and procedures, applies to all DOD information systems and networks operating at the Secret level (not to include closed, special enclave, or IC networks) and below under the purview of Office of the SECDEF, the Military Departments, the CJCS, The Combatant Commands, The Office of the Inspector General of the DOD, the Defense Agencies, the DOD Field Activities, and all other organizational entities within the Department of Defense hereafter referred collectively as the "DOD Components." The system also governs any interconnections between Public and DOD Unclassified networks, DOD Unclassified and Classified networks, and Classified and Classified networks.

b. (U) Tasks

(1) (U) CC/S/A will:

(a) (U) Implement the INFOCON System IAW DODI-O 8530, CJCSI 6510.01, Strategic Directive 527-1, and USSTRATCOM and JTF_GNO guidance.

(2) (U) JTF_GNO will:

(a) (U) Monitor, track and provide global situational awareness on the Global INFOCON Indicators.

(b) (U) Develop the execution guidance for implementation of the

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 27 February 2033~~

INFOCON directive and incorporate it into NetOps plans.

(INTENTIONALLY BLANK)

(c) (U) Ensure that the DOD GIG is optimally delivering the information required by DOD GIG users in accordance with information delivery priorities.

(d) (U) Ensure visibility of the information flowing across the DOD GIG and of those systems used to store, catalog, discover and transport information.

(e) (U) Monitor information flows and access; determine impact to network capacity; and ensure that user profiles are being satisfied with a reasonable quality of service.

(f) (U) Determine the sources responsible for providing information and stage information content throughout the DOD GIG in support of a given operation.

(g) (U) Track and maintain knowledge of the various requests and user profiles for information; coordinate changes in the operating parameters of DOD GIG assets; identify new products; review and validate the user-profile database; and develop joint policies and procedures governing information flow across the DOD GIG.

(2) (U) JTF GNO will:

(a) (U) Direct GCM activities.

(b) (U) Provide DOD GIG users with an awareness of relevant, accurate information and automated access to newly discovered information for timely, efficient delivery in a usable format.

(c) (U) Provide guidance to capitalize on the content management framework found within the Net-Centric Enterprise Services (NCES) and Net-Centric Data Strategy.

(d) (U) Facilitate the placement, posting and transport of information required by DOD GIG users.

4. (U) Administration and Logistics. Refer to Base Plan.

5. (U) Command and Control. Refer to Appendix 17 (NetOps) to Annex C (Operations).

timely and efficient information delivery and/or search information databases to retrieve desired products as required.

(4) (U) Improve bandwidth utilization.

(5) (U) Enhance all aspects of the DOD GIG transport capabilities.

b. (U) The core GCM services are Content Discovery, Content Delivery and Content Storage. These core services are envisioned to be enterprise wide services used by the entire DOD to ensure our information is available to all authorized users.

(1) (U) Content Discovery. Content Discovery provides the ability to quickly search for information throughout the DOD GIG. Using any appropriate web browser, whether on a desktop computer or wireless device, operational staffs can search across multiple sources from one place, vice making several attempts. Once the product is located, the Content Delivery service permits the users to pull in the needed product.

(2) (U) Content Delivery. Information that is requested by a DOD GIG user is delivered using the GCM delivery service. Content Delivery provides the user the capability to replicate files and directives, publish and subscribe to information based on roles and responsibilities, and provide assured, timely transport of the information to include notification of when the information was read by a distant user. Items are delivered across multiple, heterogeneous communication systems with delivery and read receipt notifications, providing assured delivery of information products.

(3) (U) Content Storage. Content Storage provides physical and virtual places to host data on the network with varying degrees of persistence. These information storage capabilities will be located throughout the DOD GIG.

c. (U) Tasks. CDRUSSTRATCOM, through the JTF_GNO and the NetOps Community, directs GCM through the policies, procedures, programs, and operations that prepare DOD systems, networks and personnel to manage the content of the DOD GIG, and coordinates with the interagency as required.

(1) (U) CC/S/A will:

(a) (U) Act on JTF GNO direction with regard to GCM activities.

(b) (U) Ensure the Content Discovery, Storage, and Delivery services as well as mitigation are operating correctly and that information is "maneuvered" to the optimum location on the DOD GIG.

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE NE 68113-6500
28 February 2008

TAB D TO APPENDIX 17 TO ANNEX C TO CONPLAN 8039 (U)
(U) OPR: JTF-GNO J5
GIG CONTENT MANAGEMENT (GCM) (U)

References: See Base Plan and Appendix 17 (NetOps) to Annex C (Operations).

1. (U) Situation. Refer to Base Plan.

2. (U) Mission. Refer to Base Plan.

3. (U) Execution

a. (U) Concept of Operations. GCM is the essential task that ensures information is available on the DOD GIG. At any time within the DOD GIG, there are information consumers and producers, who either publish or access the information required to accomplish their mission. Information exists in file sizes ranging from kilobytes to terabytes, all of which must be identifiable and accessible to appropriate users. GCM enables information users to define and set information needs to facilitate timely information delivery and to search information databases and retrieve required products. GCM maneuvers information across the DOD GIG, focusing on positioning and re-positioning of content to the optimum location in order to satisfy mission needs. This essential task adjusts information delivery methods and priorities for enhanced SA, and allows information producers to advertise, publish and distribute information. GCM is accomplished by enabling DOD GIG users to safeguard, compile, catalog, discover, cache, distribute, retrieve and share data in a collaborative environment. GCM will allow NetOps centers to optimize the flow and location of information over the DOD GIG by positioning and repositioning data and services to optimum locations on the DOD GIG in relation to the information producers, information consumers, and the mission requirements. Some of the objectives of GCM are:

(1) (U) Enable commanders to adjust information delivery methods and priorities for enhanced SA.

(2) (U) Enable information producers to advertise, publish, and distribute information to the warfighter.

(3) (U) Enable users to define and set information needs to facilitate

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 27 February 2033~~

(INTENTIONALLY BLANK)

(e) (U) Direct RA and coordinate with network warfare mission partners, JFCC NW, and others as appropriate IAW CJCSI 3121.01B.

(f) (U) Coordinate with LE/CI for investigation of the malicious activity.

(g) (U) Validate and prioritize identified critical assets meeting established CIP criteria, and ensure remediation, mitigation, and reconstitution plans are developed and maintained by asset owners.

(h) (U) Establish standards and programs for GIG management and defense, training, awareness, and certification across DOD IAW OSD policy and USSTRATCOM direction.

4. (U) Administration and Logistics. Refer to the Base Plan.

5. (U) Command and Control. Refer to the Base Plan and Annex J (Command Relationships).

(d) (U) Alert others on the GIG of local incident status to correct the intrusion.

(e) (U) Certify, accredit and report on all networks, peripherals, and edge devices in their portion of the GIG in addition to enforcing information security (INFOSEC).

(f) (U) Conduct security readiness reviews and vulnerability analysis assessments of subordinate units for compliance with CTOs and IAVAs and report compliance to JTF_GNO.

(g) (U) Ensure compliance of GIG management and defense training, awareness and certification programs per established policies and directives.

(h) (U) Develop and deconflict local contingency plans to defend against malicious activity in their portion of the GIG and provide copies to JTF GNO.

(i) (U) Conduct risk assessment of their networks.

(j) (U) Share GND information with Allies and coalition partners in accordance with formal agreements and national disclosure policies except where limited by law, policy, or security classification.

(k) (U) Provide reporting as tasked.

(l) (U) Develop and maintain remediation, mitigation and reconstitution plans for CIP criteria.

(2) (U) JTF GNO

(a) (U) Direct GND activities.

(b) (U) Notify the NetOps Community of ongoing or developing threats and anomalies via SA Reports, IAVAs, or Information Assurance Vulnerability Bulletins (IAVBs) and reduce potential risks by issuing CTOs and/or conducting a Significant Event Conference (SIEC).

(c) (U) Provide guidance and execution instructions for managing and increasing OPSEC control measures for the GIG and NetOps Community in response to the identified threat level.

(d) (U) Assess the possible impact the anomaly or incident will have on the rest of the GIG. JTF_GNO will direct GND activities and actions in accordance with the defined NetOps C2 construct. The NetOps Community will manage its affected portions of the GIG through local procedures (JTTPs).

HEADQUARTERS, U.S. STRATEGIC COMMAND
OFFUTT AIR FORCE BASE NE 68113-6500
28 February 2008

TAB C TO APPENDIX 17 TO ANNEX C TO CONPLAN 8039 (U)
(U) OPR: JTF-GNO J5
GIG NETWORK DEFENSE (GND) (U)

References: Refer to Base Plan.

1. (U) Situation. Refer to Base Plan.

2. (U) Mission. Refer to Base Plan.

3. (U) Execution

a. (U) Concept of Operations

(1) (U) GND activities consist of the policies, procedures, programs and operations that prepare DOD systems, networks and personnel to protect the GIG, as well as coordination with the interagency as required.

(2) (U) CDRUSSTRATCOM, through JTF_GNO and the NetOps Community, directs GND.

(3) (U) GIG constituent systems that meet the definition of a National Security System (NSS) must follow the appropriate Information Assurance (IA) guidelines and policies for NSS in accordance with the National Manager for NSS. Other GIG systems not designated NSS must be provided adequate IA to not jeopardize the security of GIG NSS systems.

b. (U) Tasks

(1) (U) CC/S/A will:

(a) (U) Act on JTF_GNO direction with regard to GND.

(b) (U) Detect and perform analysis of an anomaly or intrusion, providing JTF_GNO with incident reports through their GND Tier Structure.

(c) (U) Direct RA in their portion of the GIG IAW CJCSI 3121.01B.

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 06 December 2032~~

INTENTIONALLY BLANK

4. (U) Administration and Logistics. Refer to Base Plan.

5. (U) Command and Control. Refer to Appendix 17 (NETOPS).

(5) (U) Electromagnetic Spectrum Management. Ensures combatant commanders and subordinate commanders are aware of spectrum management decisions that impact mission accomplishment, and provides for efficient employment of the electromagnetic spectrum in terms of planning, allocation, coordination with other spectrums, interference resolution, and (b)(1) Sec 1.7(e)

b. (U) Tasks. CDRUSSTRATCOM, through JTF_GNO and the NetOps community, directs GEM through the policies, procedures, programs, and operations that prepare DOD systems, networks and personnel to manage the DOD GIG, and coordinates with the interagency as required.

(1) (U) CC/S/A will:

(a) (U) Act on JTF_GNO direction with regard to GEM.

(b) (U) Report outages, degradations, and upgrade operations having an operational impact on GIG functionality.

(c) (U) Monitor and adjust their portion of the DOD GIG to ensure its health and integrity (in accordance with Information Assurance Control Implementation guides).

(d) (U) Build and maintain SA over their portion of the DOD GIG.

(e) (U) Report network outages, degradations, and upgrade operations having an operational impact on the DOD GIG functionality using the CND Tier structure.

(f) (U) Maintain robust and redundant DOD GIG capability.

(g) (U) Develop, as necessary, standardized local procedures to implement JTF_GNO guidance (e.g., Joint Tactics, Techniques and Procedures (JTTPs)).

(2) (U) JTF GNO will:

(a) (U) Direct GEM activities.

(b) (U) Build and maintain SA over the DOD GIG infrastructure.

(c) (U) Report outages, degradations, and upgrade operations having an operational impact on the DOD GIG.

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE NE 68113-6500
28 February 2008

TAB B TO APPENDIX 17 TO ANNEX C TO CONPLAN 8039 (U)
(U) OPR: JTF-GNO J5
GIG ENTERPRISE MANAGEMENT (GEM) (U)

References: Refer to Appendix 17 (NetOps).

1. (U) Situation. Refer to Base Plan.

2. (U) Mission. Refer to Base Plan.

3. (U) Execution

a. (U) Concept of Operations. GEM encompasses the DOD GIG's IT services management. This consists of the many elements and processes needed to communicate across the full spectrum of the DOD GIG, and include the following:

(1) (U) Enterprise Services Management. Provides services for end-user applications, web-based services, remote hosted applications, discovery, storage, software applications and other IT components of applications.

(2) (U) Systems Management. Comprises all measures necessary to ensure the effective and efficient operations of GIG information systems, elements of systems, and services. Provides day-to-day management of information systems, elements of systems, and services to include operating systems, databases, and hosts of the end-users.

(3) (U) Network Management. Provides networked system services with the desired level of quality and guaranteed availability. Networks use all available means of communication including terrestrial, airborne and/or satellite, and include: switched networks, data networks, Video Teleconferencing (VTC) networks, satellite networks and wireless networks.

(4) (U) Satellite Communications Management. Provides day-to-day operational management of all apportioned and non-apportioned SATCOM resources, to include appropriate support when disruption of service occurs. This includes global SATCOM system status and maintains global SA to include each combatant commander's current and planned operations as well as Space, Control, and Terminal Segment asset and operational configuration management.

161

INTENTIONALLY BLANK

(f) (U) Non-DOD NETOPS activities will be executed per memorandum of agreement with the DOD.

c. (U) Tasks: JTF-GNO will:

(1) (U) Direct the operations and defense of the DOD GIG with the authority and responsibilities assigned by the President, SECDEF and CDRUSTRATCOM and is thereby empowered to order actions that execute directions given.

(2) (U) Ensure both the operational and functional chains of command are included in JTF-GNO orders.

(3) (U) Ensure that NETOPS activities are executed at the lowest level of command possible within the NETOPS Community.

(4) (U) Use the decision matrix (Figure C-17-A-4) to help determine if the NETOPS incident is a global event. A "yes" answer to any of these four criteria may drive the incident to be "fought" at a "global" level.

(a) (U) An incident crosses a Geographic Combatant Command (GCC) boundary.

(b) (U) An incident affects multiple combatant commanders.

(c) (U) An incident impacts multiple DOD agency enterprises.

(d) (U) An incident is beyond a combatant commander's capabilities.

Criteria / Incident	CROSSES THEATER BOUNDARY	IMPACTS MULTIPLE COCOMS	IMPACTS OTHER AGENCIES	BEYOND THEATER CAPABILITIES	GLOBAL EVENT?

Figure C-17-A-4: Decision Matrix (U)

4. (U) Administration and Logistics. See Base Plan.

5. (U) Command and Control. Refer to Appendix 17 (NETOPS)

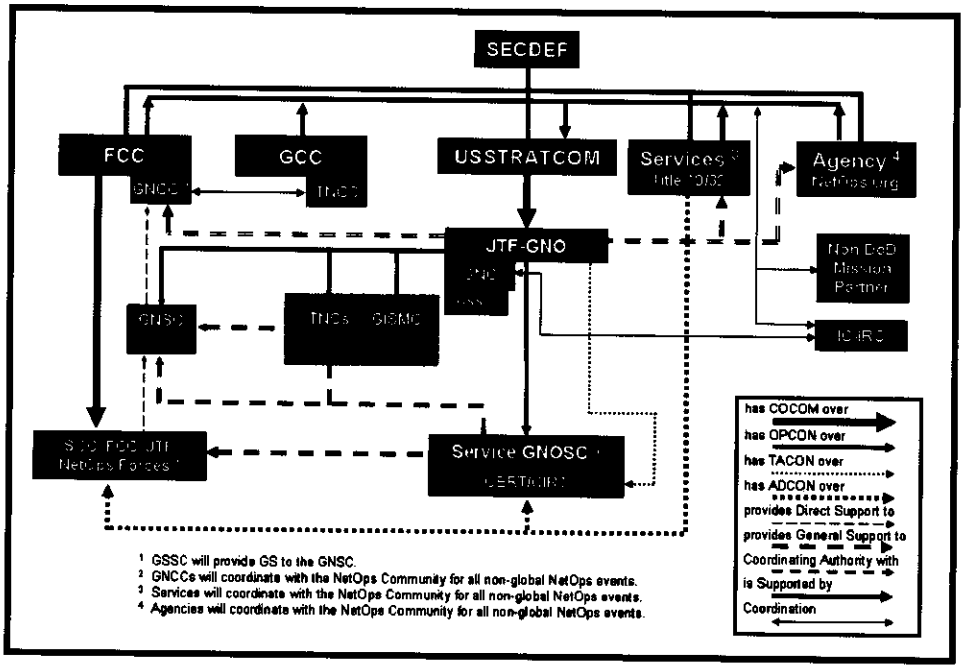


Figure C-17-A-3: Non-Global NETOPS C2 with USSTRATCOM as Supported Command (U)

(a) (U) The supported commander has the authority to take whatever NETOPS action is deemed necessary, to support the mission and has final decision responsibility.

(b) (U) The establishing authority (CDRUSSTRATCOM) will outline the generic responsibilities of the supported and supporting commanders as they apply to NETOPS during global, theater, and the non-global NETOPS events.

(c) (U) Simultaneous collaboration, both vertically and horizontally, is fundamental to SA and is vital in determining the impact of an incident (global, theater or non-global).

(d) (U) In time-critical situations, such as when an immediate Network Defense (ND) action is warranted to defend the DOD GIG within an area of responsibility (AOR), action may be initiated by the supported CC/S/A prior to collaborating or collaboration may be abbreviated. Collaboration must then follow, in order to mitigate or remediate global affects, if any.

(e) (U) NETOPS activities affecting (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(2) (U) Supporting Command. CDRUSSTRATCOM is the supporting commander when designated by the SECDEF in an EXORD or when executing a mission for NETOPS events that are not deemed global or non-global by CDR, JTF-GNO per authority delegated by CDRUSSTRATCOM (see Figure C-17-A-2). COCOMs, JTF-GNO, JTF-GNO Service NETOPS Components, FCCs, and Agencies shall provide support to the affected CC/S/A for theater NETOPS events. Non-DOD U.S. government (USG) organizations, intergovernmental organizations (State and Local), non-governmental organizations (NGO), multinational military commands (alliances and coalitions), as well as commercial and research communities may also provide support per inter-governmental agreements. Most NETOPS events begin as theater events in a local enclave that are under the control of the respective GCC. Theater NETOPS events are those activities occurring within a theater that have the potential to impact the operations in that theater.

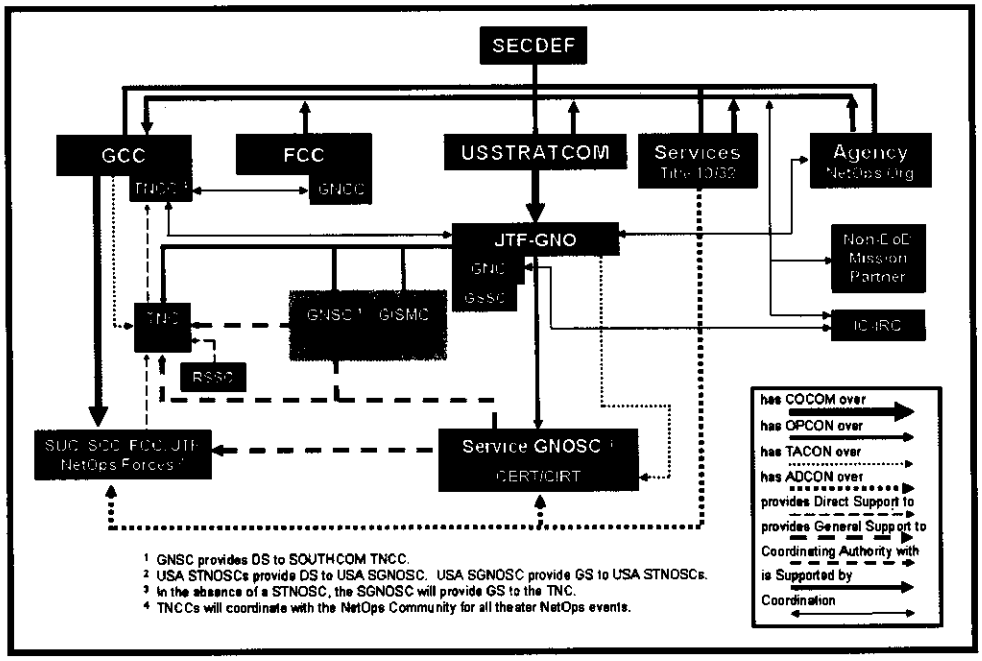


Figure C-17-A-2: Theater NETOPS C2 with GCC as Supported Command (U)

mission while operating and defending against NETOPS events that have a global or non-global impact (see Figures C-17-A-1 and C-17-A-3). CDR, JTF-GNO, via delegated authority from CDRUSSTRATCOM, will determine when a network incident requires him/her to assume this role. In such circumstances, CDR, JTF-GNO, will issue orders and direction with the authority of CDRUSSTRATCOM, to the CC/S/As and other stakeholders with connection to the DOD GIG to ensure availability and integrity of the DOD GIG. While this supported relationship gives CDRUSSTRATCOM global authority, it does not negate the COCOM's authority over NETOPS forces as specified in the UCP, 5 May 06. JTF-GNO Service NETOPS Components will support the execution of operating and defending against global and non-global NETOPS events, while synchronizing actions with affected COCOMs and their respective Components. Global NETOPS events are those activities that have the potential to impact the operational readiness of the DOD GIG and require a coordinated response amongst CC/S/As. CC/S/As are responsible for leading their respective responses to global NETOPS events in accordance with USSTRATCOM and JTF-GNO direction. Non-global NETOPS events are those activities whose impact affects FCCs, unassigned Title 10 Service forces, or Defense Agencies and are neither global nor theater in nature. JTF-GNO will provide GS to the FCCs, Services, and Agencies for non-global NETOPS events. USSTRATCOM and JTF-GNO, in conjunction with CC/S/As, will establish JTTPs that provide specifics for executing the supported/supporting relationships with regard to global NETOPS events.

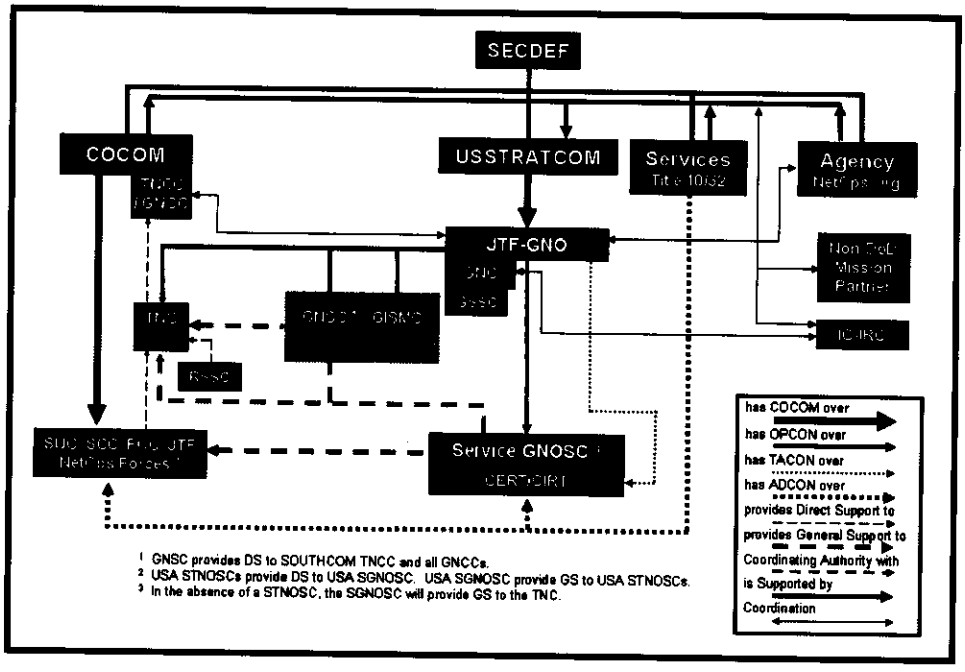


Figure C-17-A-1: Global NETOPS C2 with USSTRATCOM as Supported Command (U)

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE NE 68113-6500
28 February 2008

TAB A TO APPENDIX 17 TO ANNEX C TO CONPLAN 8039-07 (U)
(U) OPR: JTF-GNO J5
NETOPS COMMAND AND CONTROL (C2) (U)

References: See Appendix 17 (NETOPS) to Annex C (Operations)

1. (U) Situation. See Base Plan.

2. (U) Mission. See Base Plan.

3. (U) Execution

a. (U) Concept of Operations. In order to execute its UCP missions, CDRUSSTRATCOM delegates operational and tactical level planning, force execution, and day-to-day force management to JFCCs, Task Forces (TF), and Centers. These JFCCs, TFs, and Centers conduct operations for USSTRATCOM while the Headquarters focuses on strategic-level integration and advocacy of its assigned missions. At the request of CDRUSSTRATCOM, the SECDEF assigned the Director, Defense Information Systems Agency (DISA) as Commander, JTF-GNO, with authorities and responsibilities for Global Network Operations and Defense. Global NETOPS is conducted by JTF-GNO, unless otherwise directed by CDRUSSTRATCOM. Such operations include apprising CDRUSSTRATCOM on NETOPS matters impacting the DOD GIG's integrity and support of DOD missions. CDR, JTF-GNO, via delegated authority from CDRUSSTRATCOM, manages the apportionment and allocation of GIG system and network resources.

b. (U) NETOPS. NETOPS faces the same set of hierarchical C2 complexities as any other joint force operation. To facilitate net-centricity, NETOPS must adopt new Information Age C2 structures and processes that breed self-synchronized support for effective operations and defense of the DOD GIG. Today, rapidly changing technology and a lack of acquisition standardization challenges effective operation and defense of the DOD GIG from one centralized headquarters. Thus, effective operation and defense of the DOD GIG requires trained and certified NETOPS operators at all levels, with a common purpose, vision, and understanding of CDRUSSTRATCOM's intent. Until technology advances, JTF-GNO, in concert with Combatant Commands, Services and Agencies (CC/S/As) will develop full situational awareness of the DOD GIG through common processes, standards and instrumentation, enabling near real time manipulation of any asset in order to optimize net-centric services.

(1) (U) Supported Command. CDRUSSTRATCOM is the supported commander when designated by the SECDEF in an EXORD or when executing a

C – GIG Network Defense (GND)
D – GIG Content Management (GCM)
E – Information Operations Conditions (INFOCONs)

(2) (U) Assured information protection offers digital, electronic, and cognitive protection to counter attacks against US interests in cyberspace. For example, GND and GCM activities include information assurance and protection of data.

(3) (U) Assured information delivery offers cyber and cognitive protection to counter attacks against US interests in cyberspace. For example, GCM and GEM activities include the optimization of information flow and location and maintaining redundant GIG capabilities.

(4) (U) The synergy achieved through the layering of NetOps Effects provides defense in depth for the (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e).

c. (U) NetOps Support to (b)(1) Sec 1.7(e) NetOps Effects ensure support (b)(1) Sec 1.7(e)

d. (U) Tasks

(1) (U) CC/S/A are required to perform the essential tasks of GEM (See TAB B), GND (TAB C), and GCM (TAB D). Adhering to the responsibilities of the essential tasks (GEM, GND, and GCM) produces NetOps' desired effects of: Assured System and Network Availability, Assured Information Protection, and Assured Information Delivery in support of the overall goal of NetOps. NetOps and its essential tasks GEM, GND, and GCM include IA and can only occur when IA measures are implemented and accomplished within the GIG.

(2) (U) JTF GNO directs the operation and defense of the GIG to ensure timely and net-centric capabilities across strategic, operational, and tactical boundaries in support of the full spectrum of business, intelligence and warfighting Specific responsibilities for the JTF GNO include establishing SA, developing NetOps tactics, identifying GIG measures of effectiveness, publishing plans and orders, coordinating RA to attacks against the GIG, and conducting network threat intelligence.

4. (U) Administration and Logistics. Not used.

5. (U) Command and Control. For NetOps Command and Control, refer to Tab A (NetOps Command and Control).

Tabs

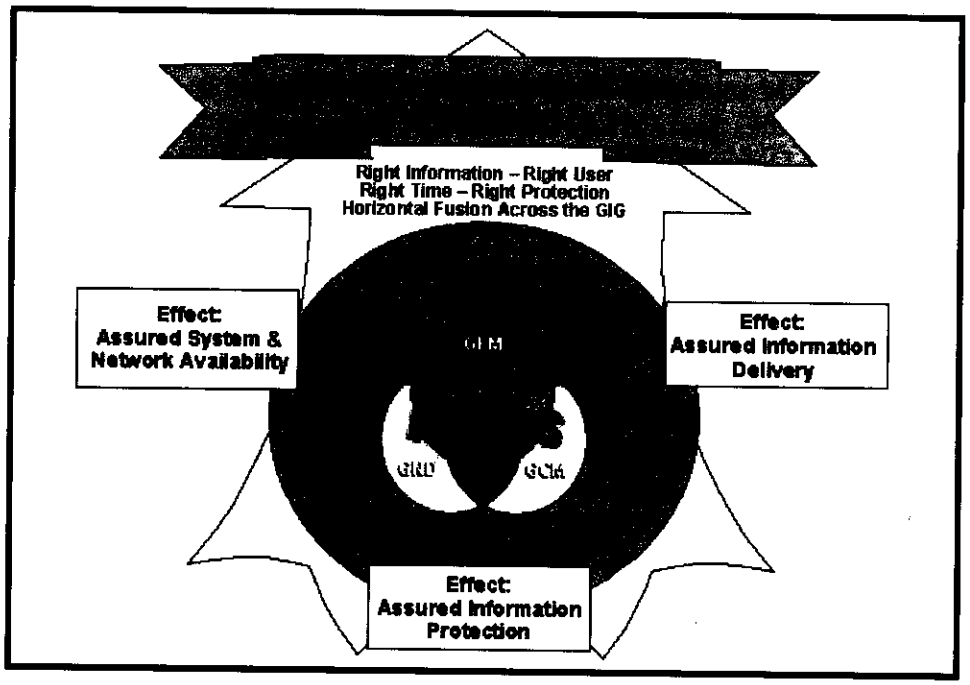
A – NetOps Command and Control (C2)
B – GIG Enterprise Management (GEM)

essential tasks. Each effect is further described in the following bullets and the relation of the essential tasks and effects are depicted below in Figure C-17-1.

(1) (U) Assured System and Network Availability is achieved through visibility and control over the system and network resources. Resources are managed and problems are anticipated and mitigated, ensuring uninterrupted availability and protection of the system and network resources. This includes providing for graceful degradation, self-healing, fail over, diversity, and elimination of critical failure points.

(2) (U) Assured Information Protection applies to information in storage/at rest, as well as passing over networks, from the time it is stored and catalogued, until it is distributed to the users, operators and decisions makers.

(3) (U) Assured Information Delivery provides information to users, operators and decision makers in a timely manner.



(U) Figure C-17-1: Relation of Essential Tasks, Effects, and NetOps

c. (U) NetOps Support (b)(1) Sec 1.7(e) The achievement of NetOps Effects ensures (b)(1) Sec 1.7(e)

(1) (U) Assured system and network availability offers digital, electronic, and physical protection to counter attacks against US interests in cyberspace. For example, GEM and GND activities include the reporting of anomalies affecting GIG health and critical infrastructure protection.

3. (U) Execution. The execution of NetOps remains the same throughout the (b)(1) Sec 1.7(e)

a. (U) Concept of Operations. NetOps is defined as the operational framework consisting of three essential tasks, SA, and C2 that CDRUSSTRATCOM, in coordination with the NetOps Community, employs to operate and defend the GIG to ensure information superiority. The GIG is a globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The three essential tasks are GIG Enterprise Management (GEM), GIG Network Defense (GND), and GIG Content Management (GCM). The synergy achieved by each integrated relationship between any two of the essential tasks (GEM, GND, and GCM) produces NetOps' desired effects of: Assured System and Network Availability, Assured Information Protection, and Assured Information Delivery in support of the overall goal of NetOps, which is to provide the right information to the edge. NetOps and its essential tasks GEM, GND, and GCM includes IA as defined and outlined in DODD 8500.1, Information Assurance, and CJCSI 6510.01D, Information Assurance and Computer Network Defense. Successful NetOps can only occur when IA measures are implemented and accomplished within the GIG. USSTRATCOM will organize its forces, identify mission essential tasks and training requirements, measure and report readiness, and direct the operation and defense of the GIG IAW the Joint CONOPS for GIG NetOps. CDRUSSTRATCOM exercises C2 through the JTF GNO. Successful operation and defense of the GIG requires an adaptive force comprised of professionals at the JTF GNO and throughout the NetOps Community. The NetOps Community is defined as the GIG providers, operators, defenders, and subscribers who possess a fundamental understanding of their responsibilities, and act synchronously to support DOD and NetOps mission partners' missions and operations. The community members include but are not limited to NetOps organizations in the CC/S/A who install, operate, maintain and defend the GIG as described in DODD 8100.1. However, it also includes major contributors to NetOps such as the OSD, Joint Staff J6, the IC Incident Response Center (IC-IRC) and (b)(1) Sec 1.7(e)

b. (U) NetOps Effects. The desired effects of NetOps are as follows: Assured System and Network Availability, Assured Information Protection, and Assured Information Delivery. Two key principles must be applied to achieve the three desired effects: essential tasks must be performed interdependently (i.e. GND cannot be performed separately from GEM as the two are synergistically coupled and are essential to evoking GCM), and JTF GNO in collaboration with the NetOps Community must perform the responsibilities associated with each essential task processes. These three effects of NetOps are derived through the synergy achieved by each integrated relationship between any two of the

m. (U) DODD 8500.1, Information Assurance (IA), 21 Nov 03

n. (U) DODD O-8530.1, Computer Network Defense, 8 Jan 01

o. ((U) DODI 8100.dd, NetOps for the GIG – DRAFT

p. (U) DODI O-8530.2, Support to Computer Network Defense (CND), 9 Mar 01

q. (U) ASD NII/DOD CIO and IC CIO MOA, Sharing Network Management and Computer Network Defense Information, 24 Jul 05

r. (U) Joint USSTRATCOM/ASD NII Memorandum, Computer Network Defense Strategy for Defense in Depth in Support of the DOD IO Roadmap, 13 Jan 05

s. (U) Joint Command and Control Functional Concept, Feb 04, p. 32

t. (U) JTF GNO OPORD 05-01 (Global Network Operations), 7 Feb 05

u. (U) JTF GNO TTX-1 VTC Minutes, 14 Nov 05

v. (U) JTF GNO TTX-2 Conference Minutes, 15 Dec 05

w. (U) JTF GNO Strategic Plan, An Adaptive Force Ensuring Information Delivery, Feb 06

x. (U) Joint Functional Component Command Space and Global Strike Concept of Operations, 1 Jan 06, DRAFT

y. (U) JFCC SGS CONOPS, 1 Jun 06 Draft NSD-42 National Policy for the Security of National Security Telecommunications and Information Systems, signed by the President on 5 Jul 90

z. (U) SD 527-1, DOD Information Operations Condition (INFOCON) System Procedures, 27 Jan 06

1. (U) Situation

a. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

b. (U) Friendly. NetOps forces. Refer to Annex A (Task Organization).

2. (U) Mission. Refer to Base Plan.

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE NE 68113-6500
28 February 2008

APPENDIX 17 TO ANNEX C TO STRATCOM CONPLAN 8039-07 (U)
(U) OPR: JTF-GNO J5
NETOPS (U)

References: Refer to Base Plan.

a. (U) SECDEF Memo, Forces For Unified Commands Memorandum, FY06 (S), 15 Feb 06

b. (U) DEPSECDEF Guidance and Policy Memo 10-8460

c. (U) USSTRATCOM Memo, Delegation of Authorities to Director, Defense Information Systems Agency (DISA), 30 Sep 03

d. (U) USSTRATCOM Memo, SECDEF Appointment of the Person Serving as Director, Defense Information Systems Agency (DISA), as Commander, Joint Task Force – Global Network Operations (JTF-GNO), 21 Jun 05

e. (U) USSTRATCOM Network Warfare Concept of Operations- Final, Mar 06

f. (U) USSTRATCOM Integrating Guidance DRAFT, 19 Dec 05

g. (U) CJCSI 6215.03, GIG Network Operations – DRAFT, Nov 05

h. (U) CJCSI 6510.01D, Information Assurance (IA) and Computer Network Defense (CND) (U), 15 Jun 04

i. (U) CJCSM 3402.01B, Alert System of the Chairman of the Joint Chiefs of Staff (U), 1 Nov 00

j. (U) DODD 8100.1, Global Information Grid Overarching Policy, 21 Nov 03

k. (U) DODD 3020.40, Defense Critical Infrastructure Program, 19 Aug 05

l. (U) DODD O-5100.30, Department of Defense Command and Control, 5

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 06 December 2032~~

Jan 06

(b) (~~S//REL USA, AUS, GBR~~) USSTRATCOM not being able to meet (b)(1) Sec 1.4(a)

(c) (U) USSTRATCOM personnel death or involvement in the death of another or death or serious illness of high-level government official.

(d) (U) A significant degradation to CI supporting a USSTRATCOM mission.

(3) (U) (b)(1) Sec 1.7(e) Report any indications of:

(a) (U) Substantial degradation in US communications capabilities, SATCOM, Terrestrial, Communications Relay System, or ground station that is part of the Communications Network.

(b) (U) Imminent or direct attacks/intrusions against the GIG and/or Coalition/Allied networks.

(4) (U) Essential Elements of Friendly Information (EEFIs). Report:

(a) (U) Discovery of a significant unmitigated vulnerability to the GIG.

(3) (U) Commanders will initiate a report through the chain of command for any of the following incidents impacting critical infrastructure supporting this OPLAN.

(a) (U) Initiation of an infrastructure incident response plan.

(b) (U) Potential or actual use of WMD against DOD assets or infrastructure.

(c) (U) Threat Information Report specifically related to infrastructure.

d. (U) Data Collection and Reporting. Collect as much information as possible for initial notification reporting, but do not delay notification to gather complete data. Submit all reports as soon as possible after an event or incident has occurred in accordance with the USSTRATCOM JTF_GNO (b)(1) Sec 1.7(e) Reporting Matrix dated 1 May 07. Use all sources, including host nation agencies, to gather data (*i.e.*, who, what, when, where, why, how).

(1) (~~S//REL USA, AUS, GBR~~) USSTRATCOM (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) notification to Commander, USSTRATCOM and senior staff. This may include (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(a) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) issues and systems (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b) (~~S//REL USA, AUS, GBR~~) Reference the GIG (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(2) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Report any changes in or events that cause changes to:

(a) (U) USSTRATCOM mission, availability of USSTRATCOM forces or unexpected loss of a USSTRATCOM asset.

(2) (U) USSTRATCOM will recommend that (b)(1) Sec 1.7(e) conduct Joint Staff Integrated Vulnerability Assessments (JSIVA), with or without a DCIP module, or Balanced Survivability Assessments (BSA) via USNORTHCOM, for CONUS based assets, other Geographic COCOMs for OCONUS based assets, and the Joint Staff. These assessments will complete gaps in information or validate dated information.

(3) (U) USSTRATCOM will request additional resources to support solutions outlined in all of USSTRATCOM's remediation plans and future characterization efforts.

4. (U) Administration and Logistics

a. (U) Administration. Refer to Base Plan.

b. (U) Logistics

(1) (U) Refer to Base Plan.

(2) (U) The Services and Agencies are responsible for funding subordinate unit CIP programs. Commanders have the inherent responsibility to implement prudent CIP measures and will immediately elevate any identified CIP concerns to their next higher headquarters or responsible command. Commanders may provide additional support through advocacy and/or funding of critical CIP issues.

5. (U) Command and Control

a. (U) Command

(1) (U) Command Relationships.

(2) (U) Command Posts. Refer to Base Plan.

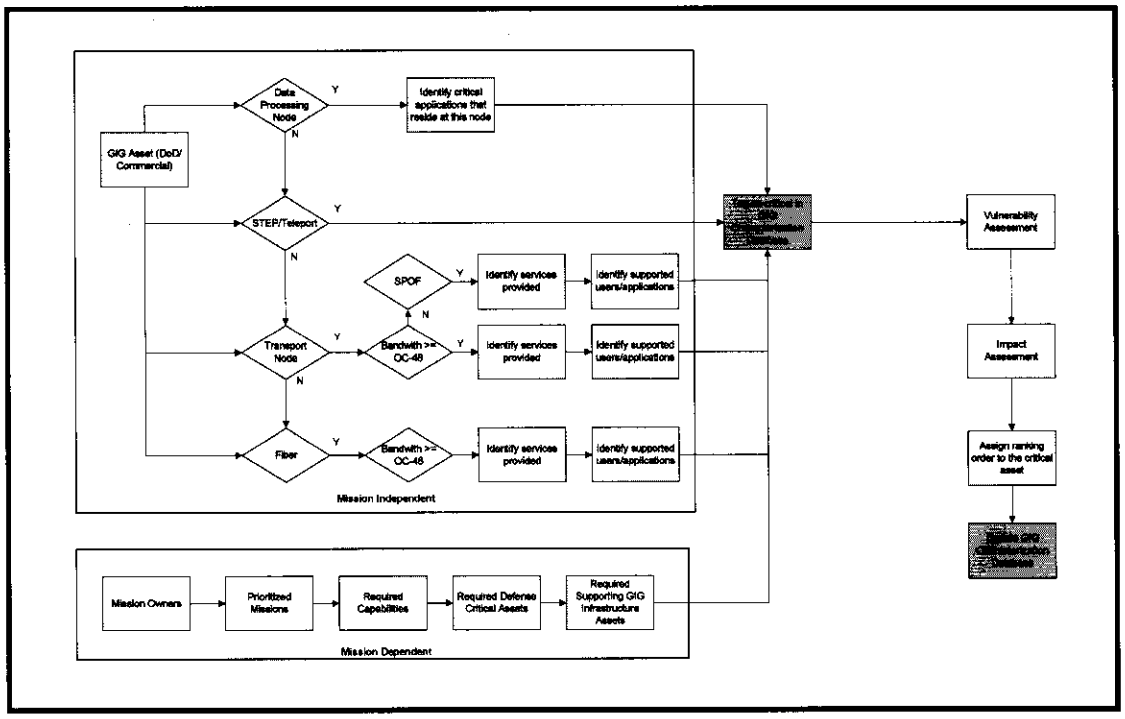
b. (U) Command, Control, Communications, and Computer (C4) Systems. See Annex K.

c. (U) Reporting Requirements

(1) (U) Refer to Base Plan.

(2) (U) All units and Commanders must immediately report any incident, threat, surveillance or suspicious activity that may adversely impact infrastructure supporting USSTRATCOM operational capability.

Figure C-16-3: The GIG Characterization Methodology (U)



(2) (U) DOD Components asset owners will remediate vulnerabilities to their critical assets/infrastructure. Remediation includes actions taken to correct known deficiencies and weaknesses once vulnerabilities have been identified. The JTF GNO will make recommendations to the CC/S/As in support of their risk management efforts. The asset owner's remediation plans will include recommendations to either accept the risk, or remediate the risk via a Doctrine-Organization- Training-Material-Leadership-Personnel-Facilities (DOTMLPF) approach. The factors to be considered are as follows:

(a) (U) Assess the ability to use material vs. non-material solutions to include alternative funding solutions if necessary.

(b) (U) Incorporate CIP into Exercise Plans.

(c) (U) Provide lessons learned to improve the GIG risk management processes.

c. (U) Coordinating Instructions

(1) (U) USSTRATCOM will coordinate (b)(1) Sec 1.7(e) to assist in the Characterization of the GIG. See Figure 2.

ranked based on their impact to the performance of the GIG. (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

DEFENSE SECTOR	*LEAD AGENCY*
Defense Industrial Base (DIB)	Defense Contract Management Agency (DCMA)
Financial Services	Defense Finance and Accounting Services (DFAS)
Global Information Grid (GIG)	(b)(1) Sec 1.7(e)
Health Affairs	Assistant Secretary of Defense (ASD) for Health Affairs (HA)
Intelligence, Surveillance, and Reconnaissance (ISR)	(b)(1) Sec 1.7(e)
Logistics	Defense Logistics Agency (DLA)
Personnel	DOD Human Resources Activity (DHRA)
Public Works	U.S. Army Corps of Engineers (USACE)
Space	USSTRATCOM
Transportation	United States Transportation Command (USTRANSCOM)

Figure C-16-2: DCIP Defense Sector Lead Agencies (U)

(7) (U) Priorities. USSTRATCOM CIP protection priorities are based on critical C4 missions in support of the NMS. GIG mission success will depend upon accurately characterizing the GIG, Identifying critical GIG assets, determining vulnerabilities, and mitigating risk.

b. (U) Tasks

(1) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
responsibility of characterizing the GIG. See Figure 3 below. This characterization process will clearly define inter/intra dependencies of DOD and non-DOD assets, single points of failure, and commercial dependencies in support of the NMS. All validated GIG task critical assets approved by the joint staff will be added to the GIG Geospatial Database that's presently maintained by the (b)(1) Sec 1.7(e) Mission Assurance Division.

(5) (U) Monitoring and Reporting (M&R). The M&R process is not solely

(b)(1) Sec 1.7(e)

Figure 1 below. The endstate is to integrate CIP into existing command reporting processes.

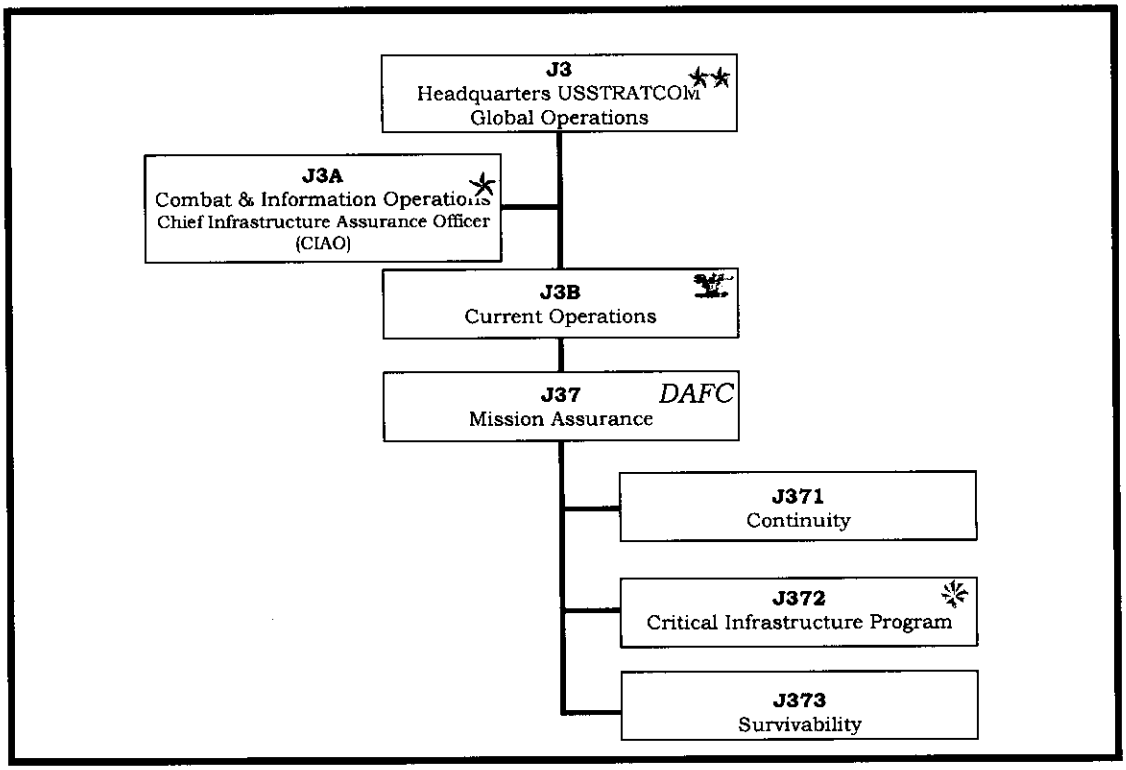


Figure C-16-1: USSTRATCOM CIP Organizational Structure (U)

(U) The USSTRATCOM's Mission Assurance Division (J37), is the office of primary responsibility to establish, resource, and execute the command's program for matters pertaining to the identification of Defense Infrastructures and the prioritization/protection of Defense *Critical* Infrastructure, including the identification and prioritization of USSTRATCOM mission essential tasks and required capabilities.

(6) (U) Criticality. The GIG critical assets are identified from both mission dependent and mission independent perspective. Mission-dependent critical assets are those deemed essential to the accomplishment of a mission. Their identification and prioritization are top down driven i.e. from mission to supporting infrastructure. Mission-independent critical assets are derived and

c. (U) Friendly: See Annex A (Task Organization). There are no friendly forces specifically assigned to protect the critical infrastructure of the United States. Rather, CIP is a national effort to establish, resource, and execute a process for matters pertaining to the identification of Defense Infrastructures and the prioritization/protection of Defense *Critical* Infrastructures. In this effort, it is important to understand that CIP and Force Protection (FP) are complementary efforts. USSTRATCOM's JTF_GNO will rely on the following organizations to enhance the success of its delegated USSTRATCOM mission to direct the operations and defense of the GIG:

(1) (U) (b)(1) Sec 1.7(e)

(2) (U) (b)(1) Sec 1.7(e)

(3) (U) (b)(1) Sec 1.7(a)

(4) (U) Counterintelligence Field Agency (CIFA)

(5) (U) Law Enforcement/Counterintelligence (LE/CI) Agency

d. (U) Assumptions. Refer to Base Plan.

2. (U) Mission. Refer to Base Plan.

3. (U) Execution. The execution of CIP remains the same throughout the (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

a. (U) Concept of Operations

(1) (U) Commander's Intent. CDRUSSTRATCOM intends to prevent or mitigate the loss or degradation of task critical assets that support assigned global missions.

(2) (U) Purpose. Identify, prioritize, and recommend protection measures to defend critical GIG assets.

(3) (U) Methods. Accurately characterize the GIG, and establish a standardized criticality methodology, and a real time situation awareness capability that will accurately support the identification of critical GIG assets.

(4) (U) Endstate. Focus scarce resources on the most critical vulnerabilities, and integrate CIP into operational planning processes.

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AFB NE 68113-6500
28 February 2008

APPENDIX 16 TO ANNEX C TO STRATCOM CONPLAN 8039 (U)
(U) OPR: JTF-GNO, J5
GIG CRITICAL INFRASTRUCTURE PROTECTION (CIP) Execution Plan (U)

(U) References:

a. (U) Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection, 17 Dec 03

b. (U) DODD 3020.40, Defense Critical Infrastructure Program (DCIP), 19 Aug 05

c. (U) DODD 3020.40, Defense Critical Infrastructure Program (DCIP), Apr 07 Draft

d. (U) Strategic Command Directive (SD) 536-1, Critical Infrastructure Program, 15 Jul 05

e. (U) Joint Concept of Operations for Global Information Grid NetOps, 4 Aug 06

f. (U) DCIP Security Classification Guide, March 2007 Draft Version 2.1

1. (U) Situation

a. (U) Background: DODD 3020.40 provides policy, and assigns responsibilities for the DCIP. DCIP was conceived at the National level as a risk management strategy to provide processes, tools, and methodologies for making economic choices about what type of protection will be employed for critical infrastructure assets to assure their continued availability. DCIP requires an understanding of mission impact to guide the prioritization of enterprise-wide protection efforts; vulnerability remediation investment strategies; operational and procedural enhancement; and contingency plan development. Protection derives from reducing or eliminating vulnerabilities. This Annex will focus on critical GIG cyber assets IAW USSTRATCOMs UCP mission which emcompasses directing GIG operations and defense capabilities.

b. (U) (b)(1) Sec 1.7(e) See Annexes B (Intelligence) (b)(1) Sec 1.7(e)

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2032~~

(b)(1) Sec 1.7(e)

simulation process itself will be used as a tool to visualize how the Operations/Campaign may flow. Additionally, modeling and simulation will be used to support analysis of collection opportunities, as well as offering COCOM staffs an opportunity to evaluate the plan for shortfalls, gaps and other complications that may not have been observed in previous collection planning efforts.

c. (U) Tasks

(1) (~~S/REL~~) JFCC ISR will (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) in support of CONPLAN 8039.

(2) (~~S//REL USA, AUS, GBR~~) JFCC GSI will coordinate and integrate operations in and through cyberspace with JFCC NW, JTF GNO, JIOWC, and as required with JFCC Space (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

d. (U) Coordinating Instructions. Refer to the Base Plan.

4. (U) Administration and Logistics. Refer to the Base Plan.

5. (U) Command and Control. Refer to the Base Plan.

allocation (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) capabilities.

(4) (U) Operations Center. JFCC ISR maintains 24/7 ISR Operations Center for situational awareness of global ISR operations. JFCC ISR's watch will monitor all (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(5) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(6) (U) Portal. The current JFCC ISR portal serves as a hub for ISR information sharing within the DOD. The information accessible within this portal consists of a collection of pages for publishing JFCC ISR specific content and multiple links to resources external to the portal. The version 2 of JFCC ISR web-based portal will be capable of supporting internal and external coordination and collaboration. The JFCC ISR Portal will be critical resource for DOD's ISR community and a vital enabler of the JFCC ISR mission.

(7) (U) Assessment

(a) (U) Assessing Collection. JFCC ISR will develop criteria for assessing collection mechanisms in order to determine the effectiveness of synchronization, resolution of tasking, asset competition, and customer satisfaction. JFCC ISR Assessment Division will, in coordination with the JFCCs, Services, IC, CSA, and COCOMs, develop, maintain, use and evaluate measures of effectiveness and mission metrics to assess ISR mission objective accomplishment. JFCC ISR will use USSTRATCOM, JFCC GSI, JFCC NW, JTF GNO, JIOWC, and combatant command inputs and planning factors as a baseline, conducting assessment process will be captures and used to inform subsequent planning and allocation efforts.

(b) (U) Modeling and Simulation Methodologies. After reviewing the plan, JFCC ISR Assessments Division will use COCOM inputs to initiate Modeling and Simulation (MOD/SIM) to support analysis of specific ISR Operations/Campaigns. While JFCC ISR will develop specialized MOD/SIM tools, the modeling and

4. (U) Re-allocate. This involves moving an asset/capability assigned against an existing requirement to the newly identified requirement. This re-allocation can be from within the requesting GCC's AOR, or from another AOR.

5. (U) Surge. This involves a specified time-frame during which selected assets/capabilities will be surged to meet the requirement.

6. (U) Utilize ISR (b)(1) Sec 1.7(e) to meet the requirement.

7. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) recommended allocation changes.

8. (~~S//REL USA, AUS, GBR~~) JFCC ISR will develop (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) allocation recommendation based on asset availability for specific requirement.

9. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) consolidate the recommendation (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) will make the final decision and assets will be allocated accordingly.

(3) (U) Support for Operations in and Through Cyberspace

(a) (~~S//REL USA, AUS, GBR~~) Operations in and through cyberspace have unique requirements in the electromagnetic spectrum. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) In this case, JFCC ISR will coordinate with JFCC NW to satisfy (b)(1) Sec 1.4(a) JFCC ISR will leverage DOD ISR (b)(1) Sec 1.4(a) right capabilities to go against the identified collection requirements.

(b) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) JFCC ISR' s flexible ISR options, if and when (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) support of operations in and through cyberspace.

(c) (U) JFCC ISR (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(d) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) JFCC ISR will provide (b)(1) Sec 1.4(a) recommendations if the current ISR

2. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

3. (~~S//REL USA, AUS, GBR~~) In a (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

4. (~~S//REL USA, AUS, GBR~~) The (b)(1) Sec 1.4(a)
continue to be improved to provide (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) timely fashion. Request for
additional ISR support, (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) requires additional coordination.

(d) (~~S//REL USA, AUS, GBR~~) Re-allocation. JFCC ISR will (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

1. (U) National Intelligence Priority.

2. (U) GCCs/USSTRATCOM (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

3. (U) Risk (associated with not gaining the information).

4. (U) Potential value of intelligence to be gathered.

(e) (U) COAs. JFCC ISR will develop potential COAs for consideration. A list of factors will be provided with each COA to facilitate decision making. Those COAs include:

1. (U) Coordination with the CC/S/As to determine if the requirement is being, or can be, met via any existing ISR operations.

2. (~~S//REL USA, AUS, GBR~~) If at all possible, (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

3. (U) Allocate. This means to allocate an asset/capability that is not currently assigned against the requirement.

(b)(1) Sec 1.4(a)

cyberspace operations forces and capabilities. Also, as required, JFCC ISR will develop and maintain a (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

appropriate entities to access. JFCC ISR is responsible for providing all ISR partners with global situational awareness of ISR activities.

(2) (U) ISR Force Management Concepts. JFCC ISR established (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

reallocation and COAs recommendations will provide the flexibility to modify existing allocation plan to better meet combatant command requirements in a timely manner.

(a) (FOUO) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(b) (FOUO) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

1. (~~FOUO~~) Requirements for this ISR (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

2. (~~FOUO~~) While supporting Geographic Combatant Commander ISR requirements, these forces enable USSTRATCOM to integrate ISR in support of strategic and global operations.

(c) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) If an immediate requirement is identified for additional ISR support (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

1. (~~S//REL USA, AUS, GBR~~) The (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.7(e)

representation within JFCC ISR.

(U)(3) ~~(S//REL USA, AUS, GBR)~~ USSTRATCOM, JFCCs and Centers. JFCC ISR will closely coordinate with USSTRATCOM, JFCC GSI and JFCC NW to support CONPLAN 8039. JFCC ISR will coordinate with other USSTRATCOM component commands to meet the CONPLAN 8039 objectives. In this effort, JFCC ISR will participate through collaborative sessions facilitated by USSTRATCOM, JFCC GSI, or other JFCCs, combatant command(s) and recommend ISR COAs if required.

(4) (U) (b)(1) Sec 1.7(e) JFCC ISR will work in conjunction with the (b)(1) Sec 1.7(e)

CONPLAN 8039.

(5) (U) Services. The Service representatives within JFCC ISR serve as the primary conduit/liaison into their respective Service for coordinating ISR issues. Coordination between JFCC ISR and JFCOM and its components will be done to address issues (b)(1) Sec 1.7(e) processes, and determination of availability and capability of Service-specific ISR assets. Additionally, each Service will receive process and disseminate data via their respective and existing ISR processes and procedures.

(6) (U) Allies and PN. To the maximum extent possible, PN ISR capabilities will be utilized when available and appropriate. (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

b. (U) Mission Execution

(1) ~~(S//REL USA, AUS, GBR)~~ (b)(1) Sec 1.4(a) JFCC ISR will coordinate with USSTRATCOM (b)(1) Sec 1.4(a) ISR (b)(1) Sec 1.4(a) JFCC ISR will monitor these operations and be prepared to assist the Unified Commanders in modifying the operation to ensure mission success. Concerning cyberspace, JFCC ISR will (b)(1) Sec 1.4(a)

networked systems and associated physical infrastructures. (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(b) (~~S//REL USA, AUS, GBR~~) Other on-going activities (i.e., Global War on Terrorism (GWOT), Contingency Operations) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(c) (~~S//REL USA, AUS, GBR~~) Other collection capabilities may be leveraged on a case-by-case basis. There may be opportunities (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(2) (U) Constraints. None Identified.

2. (U) Mission. Refer to the Base Plan.

3. (U) Execution

a. (~~S//REL USA, AUS, GBR~~) Concept of Operations. ISR operations include those processes carried out (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) The role of JFCC ISR is not to provide the analytical research of collected data, but recommend the resources to adequately respond to critical needs in the form of sensors, platforms and specific processing suites. While integrating all intelligence disciplines, JFCC ISR will ensure its focus also includes
(b)(1) Sec 1.4(a)

(1) (~~S//REL USA, AUS, GBR~~) General. JFCC ISR will coordinate and seek
(b)(1) Sec 1.4(a)

(2) (U) Organization and Mission Partners. JFCC ISR is a component
(b)(1) Sec 1.7(e)

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE, NE 68113-6500
28 February 2008

APPENDIX 9 TO ANNEX C TO USSTRATCOM CONPLAN 8039 (U)
(U) OPR: JFCC ISR
INTELLIGENCE SURVEILLANCE AND RECONNAISSANCE (ISR) (U)

(U) References:

a. (U) Draft Horizontal Command and Control Integration (HC2I), Apr 2007 (S)

b. (U) Draft Joint Functional Component Command (JFCC) ISR Concept of Operations (CONOPS), 21 Aug 06 (FOUO))

1. (U) Situation

a. (U) General

(1) (~~S//REL USA, AUS, GBR~~) The strategic goal of CONPLAN 8039 is to ensure US military freedom of action in cyberspace and to deny adversary freedom of action in cyberspace. To achieve this goal, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) when directed.

b. (U) (b)(1) Sec 1.7(e) Refer to Annex B (Intelligence) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

c. (U) Friendly. Refer to Annex A (Task Organization) and the Base Plan.

d. (U) Assumptions. Refer to the Base Plan.

e. (U) Limitations

(1) (U) Restraints

(a) (~~S//REL USA, AUS, GBR~~) Cyberspace is a domain using electronics and the electromagnetic spectrum to store, modify, and exchange data via

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (e), and (g)~~
~~Declassify on: 26 February 2032~~

(INTENTIONALLY BLANK)

commanders may use any lawful weapon or tactic available for mission accomplishment.

(3) (U) (b)(1) Sec 1.7(e) During ROE development, careful consideration must be given to (b)(1) Sec 1.7(e) anticipated operations. The ROE development cell will need to identify what actions are subject to specific ROE (e.g. reference a, Enclosure F, Paragraph 3.b.) and whether any supplemental ROE will be required (b)(1) Sec 1.7(e)

(4) (U) Self-defense. As described in reference a, unit commanders always retain the inherent right and obligation to exercise unit self-defense in response to a hostile act or demonstrated hostile intent. Unit commanders may limit individual self-defense by members of their unit. Both unit and individual self-defense includes defense of other US Military forces in the vicinity. The hostile act standard described in Enclosure A of reference a, does not apply to a subset of digital protection options under this plan, (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) Refer to Enclosure F of reference a.

b. (U) Tasks – Required Legal Reviews. It is the responsibility of the legal staffs to confirm that required legal reviews for a capability/weapon to be utilized in a cyberspace operation have been completed, as well as to do any operational legal reviews. It is the responsibility of the operators to ensure that a legal review is conducted for proposed operations.

c. (U) Coordinating Instructions. As stated above, coordination may need to take place with the Interagency and non-US forces. In addition, Enclosure F of reference a, reference b, and other DOD instructions and policies require (b)(1) Sec 1.7(e)

4. (U) Administration. Refer to Base Plan.

5. (U) Command and Control. It is possible that USSTRATCOM may be the supported commander, supporting commander, or a combination of both depending on the particular activities to be undertaken. In any of these cases, USSTRATCOM planners, operators, and attorneys must ensure that appropriate ROE are developed to carry out the missions assigned.

(SROE), but also theater ROE, existing EXORDs, and DOD authorities such as the (b)(1) Sec 1.4(a)

b. (U) Scope/Applicability. This appendix applies to all US forces and personnel conducting missions pursuant to this plan.

c. (U) (b)(1) Sec 1.7(e) Refer to Base Plan, Annex B, (b)(1) Sec 1.7(e)

d. (U) Friendly. Refer to Base Plan. Although not subject to ROE, there may be significant involvement between US forces and the Interagency to achieve overall US objectives. In some operations, non-US forces may participate in cyberspace operations under this plan. ROE for non-US forces may differ from the ROE issued to US forces. In such cases, coordination and deconfliction with the non-US force will need to take place unless classification, OPSEC, or operational considerations prevent such coordination.

e. (U) Assumptions. Refer to Base Plan.

f. (U) Legal Considerations. All operations under this plan will be conducted in compliance with US law and the law of war. Per reference b, members of the DOD Components will comply with the law of war during all armed conflicts, however such conflicts are characterized, and in all other military operations. For the legal considerations applicable to intelligence collection refer to Annex B, Intelligence.

g. (U) Concept. ROE are a means of providing guidance and instruction to military commanders and DOD components within the framework of overall political directives and the law of war. They define the degree and manner in which force may be applied and are designed to ensure its carefully controlled application in order to achieve specified objectives. Additionally, they ensure the maximum survivability of USSTRATCOM and other forces in a confrontation with adversary forces.

2. (U) Mission. Refer to Base Plan.

3. (U) Execution

a. (U) Concept of Operation

(1) (U) General. CJCS Standing ROE contained in reference a, serve as the starting point for development of ROE for an operation.

(2) (U) Lawful tactics / weapons. The SROE, reference a, are designed to be permissive in nature. Therefore, unless a specific weapon or tactic requires SecDef or combatant commander approval, or unless a specific weapon or tactic is restricted by an approved supplemental measure,

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE, NE 68113-6500
28 February 2008

APPENDIX 8 TO ANNEX C TO USSTRATCOM CONPLAN 8039 (U)
(U) OPR: USSTRATCOM HQ SJA
RULES OF ENGAGEMENT (ROE) (U)

(U) References:

a. (U) CJCSI 3121.01B, Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces, 13 Jun 05 (S)

b. (U) DOD 2311.01E, DOD Law of War Program, 9 May 06 (U)

c. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) Activities, 9 May 07 (S//NF)

1. (U) Situation

a. (~~S//REL USA, AUS, GBR~~) Purpose. The purpose of this appendix is to address rules for conducting cyberspace operations. Given that the scope and nature of contemplated operations under CONPLAN 8039 are quite diverse, this appendix contains a discussion of the issues that will need to be addressed in the ROE for a specific operation. Supplemental ROE will almost certainly have to be requested from SECDEF in order to carry out operations under this CONPLAN. As stated in the Base Plan, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) The ROE for an operation will need to enable the supported Combatant Commander and supporting Combatant Commanders to carry out cyberspace operations, including (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Authorization to carry out specific parts of an operation may depend on (b)(1) Sec 1.4(a) the (b)(1) Sec 1.4(a) operations). IO in particular tend to require higher level authorizations. The planners, operators, and attorneys who work together to develop appropriate

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2032~~

ROE will need to look not only at ref a, the Standing Rules of Engagement

(INTENTIONALLY BLANK)

(a) (U) (b)(1) Sec 1.7(e) operations are planned and executed IAW SECDEF SROE for Information Operations and the USSTRATCOM (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

4. (U) Administration and Logistics. Refer to the Base Plan.

5. (U) Command and Control. Refer to the Base Plan.

(b)(1) Sec 1.4(a) based on the situation.

(2) (~~S//REL TO USA, AUS, CAN, GBR, NZL~~) (b)(1) Sec 1.4(a) commander or head of major DOD component is the approving authority for the employment of (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) should report response actions and results to the JTF GNO as this input is critical to other response actions that may be necessary and GIG situational awareness in general. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(a) (S//REL TO USA, AUS, CAN, GBR, NZL) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b) (~~S//REL TO USA, AUS, CAN, GBR, NZL~~) (b)(1) Sec 1.4(a) System Description (b)(1) Sec 1.4(a)

(c) (S//REL TO USA, AUS, CAN, GBR, NZL) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(d) (~~S//REL TO USA, AUS, CAN, GBR, NZL~~) Significant results (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(e) (S//REL TO USA, AUS, CAN, GBR, NZL) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(3) (~~S//REL TO USA, AUS, CAN, GBR, NZL~~) (b)(1) Sec 1.4(a) The CDR USSTRATCOM is the approving authority for the employment of RA techniques (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) CC/S/A. Combatant Commands or Service component NetOps HQ request (b)(1) Sec 1.4(a) from the CDR USSTRATCOM via JTF GNO.

(4) (~~S//REL TO USA, AUS, CAN, GBR, NZL~~) (b)(1) Sec 1.4(a) The Commander, USSTRATCOM is the approving authority for (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE, NE 68113-6500
28 February 2008

TAB G TO APPENDIX 3 TO ANNEX C TO CONPLAN 8039 (U)
(U) OPR: JTF-GNO J5
RESPONSE ACTIONS (U)

(U) References. Refer to the Base Plan.

1. (U) Situation. Refer to the Base Plan. The purpose of this is to articulate definitions, boundaries and responsibilities for Response Actions (RA) in defense of the GIG.

2. (U) Mission. Refer to the Base Plan.

3. (U) Execution

a. (U) Concept of Operations. For the purpose of this plan, RAs are deliberate, authorized measures, or activities that protect and defend DOD computer systems and networks under attack or targeted for attack by adversary computer systems/networks. RAs extend DOD's layered defense-in-depth capabilities and increase DOD's ability to withstand adversary attacks. RAs consist of techniques and administrative procedures employed to halt or minimize the effects of malicious activity and/or intrusion. RAs comprise the entire set of defensive actions to protect and defend the DOD GIG. (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

b (U) Specific Guidance for RAs

(1) ~~(S//REL TO USA, AUS, CAN, GBR, NZL)~~ (b)(1) Sec 1.4(a) commander is the approving authority for the employment of response actions

(b)(1) Sec 1.4(a)

This reporting is critical to the overall defense of the GIG and situational awareness in general. CC/S/A's advise and coordinate as necessary on (b)(1) Sec 1.4(a)

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2032~~

224

225

226

227

228

229

230

231

232

233

234

235 INTENTIONALLY BLANK

(b)(1) Sec 1.4(a)

(a) (~~S//REL USA, AUS, GBR~~) Be prepared to support (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) to Appendix 3 (Information Operations) and Annex Y (Strategic Communication).

(b) (U) (b)(1) Sec 1.7(e) employed forces.

(c) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) US vital interests.

(d) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) data or the medium used to transmit or store the data.

(2) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

b. (U) Tasks. Refer to the (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

c. (U) Coordinating Instructions. Refer to the (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) and CONPLAN 8035.

4 (U) Administration and Logistics. Refer to the (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

5 (U) Command and Control

a. (U) Command Relationships

(1) (U) Roles and Responsibilities. Refer to Annex J (Command Relationships) and the Base Plan. Refer also to (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) If forces are delegated OPCON/TACON to USSTRATCOM, USSTRATCOM will further delegate TACON to JFCC NW.

(2) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Communication and Reporting Requirements. The (b)(1) Sec 1.4(a) is used for coordinating all (b)(1) Sec 1.4(a) portions of this plan. Refer to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(a) (U) (b)(1) Sec 1.7(e) threatening US vital interests.

(b) (~~S//REL USA, AUS, GBR~~) Support (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) to Appendix 3 (Information Operations) and Annex Y (Strategic Communication).

(c) (U) (b)(1) Sec 1.7(e)

(d) (U) (b)(1) Sec 1.7(e)

(e) (~~S//REL USA, AUS, GBR~~) Support Operational (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) to Appendix 3 (Information Operations).

(f) (U) Maintain the capability to support deterrence/follow-on operations against other potential adversaries.

4. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

considered. Refer to (b)(1) Sec 1.7(e) to Appendix 3 (Information Operations) and Annex Y (Strategic Communication).

2. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) USSTRATCOM will lead a collaborative effort across the USSTRATCOM Staff, Functional Components, Service Components, combatant commanders, Joint Staff, and a Joint
(b)(1) Sec 1.4(a)

(a) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(b) (U) (b)(1) Sec 1.7(e)

(c) (~~S//REL USA, AUS, GBR~~) Support (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) to Appendix 3 (Information Operations) and Annex Y (Strategic Communication).

(d) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(e) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(f) (~~S//REL USA, AUS, GBR~~) Support Operational (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) to Appendix 3 (Information Operations).

3. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(1) (~~S//REL USA, AUS, GBR~~) USSTRATCOM will (b)(1) Sec 1.4(a) IAW references (a) through (e) above, Plan Summary, and Base Plan.

(a) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) operations, USSTRATCOM will (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

1. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(a) (U) Identify threats to US interests and assess (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(b) (U) (b)(1) Sec 1.7(e) interagency partners, allies, and GCCs. Identify (b)(1) Sec 1.7(e) in support of plan activities that will (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(c) (U) Establish force posture and conditions tailored to (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(d) (U) Use of (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) will be

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE, NE 68113-6500
28 February 2008

TAB F TO APPENDIX 3 TO ANNEX C TO USSTRATCOM CONPLAN 8039 (U)

(U) OPR: JFCC NW

(b)(1) Sec 1.7(e) (U)

(U) References: Refer to the Base Plan.

a. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) United States Strategic Command (USSTRATCOM) and Delegation of Authority," 14 Aug 2003 (S//NF)

b. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) Headquarters Commands to USSTRATCOM," 1 Oct 2003 (S//NF)

c. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) Jan 2004 (With Modifications 1, 2, and 3) (U)

d. (U) SECDEF Memorandum, Subject: "Appointment of the Commander, JFCC NW," 12 Jul 2005 (S)

e. (U) USSTRATCOM Operational Order (OPORD) 07-01, 1 Nov 2006

1. (U) Situation

a. (U) (b)(1) Sec 1.7(e) Refer to Annex B (Intelligence) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

b. (U) Friendly. Refer to Annex A (Task Organization), the Base Plan and (b)(1) Sec 1.7(e)

c. (U) Assumptions. Refer to the Base Plan (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

2. (U) Mission. Refer to the Base Plan.

3 (U) Execution

a. (U) Concept of Operations

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2032~~

b. (~~S//REL USA, AUS, GBR~~) Coordinating Instructions. Planners should compare and evaluate the merit of (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Refer to the Base Plan for an example of a (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) will be deconflicted by USSTRATCOM.

4. (U) Administration and Logistics. Refer to the Base Plan.

5. (U) Command and Control. Refer to the Base Plan, Annex J (Command Relationships).

(b)(1) Sec 1.4(a)

(4). (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) through cyberspace can be used to (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(5). (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) Consider the activities below as representative activities that may be best achieved through (b)(1) Sec 1.4(a)

(a). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(b).) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) through the cyberspace domain.

(c). (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) through the cyberspace domain.

(d). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(e). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(f). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) USSC

(g). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(h). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(i). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

the mission space for command and control of forces; some use the internet to conduct recruiting and develop the financial support that is the lifeblood of modern terrorism, others use it as a means to subvert regimes and governments; others use it in active, opposing "fire fights," i.e., combat in cyberspace to deny freedom of action to the US.

c. (U) Assumptions. Refer to the Base Plan.

2. (U) Mission. Refer to the Base Plan.

3. (U) Execution. Refer to the Base Plan.

a. (U) Concept of Operations

(1). (U) Purpose

(a). (U) The purpose of this Tab is to provide a common level of understanding of the requirement to (b)(1) Sec 1.7(e) planning operations in and through cyberspace.

(b). (U) Additionally, this Tab illustrates (b)(1) Sec 1.7(e) that can be integrated into operations in and through cyberspace and generate an effect in the cyberspace domain. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(2). (~~S//REL USA, AUS, GBR~~) General. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) cyberspace operations. Availability of (b)(1) Sec 1.4(a) within cyberspace affords a combatant commander a wide variety of (b)(1) Sec 1.4(a) that can (b)(1) Sec 1.4(a)

(3). (S//REL USA, AUS, GBR)) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE, NE 68113-6500
28 February 2008

TAB E TO ANNEX C TO USSTRATCOM CONPLAN 8039 (U)

(U) OPR: JFCC NW J52

(b)(1) Sec 1.7(e) (U)

(U) References: Refer to the Base Plan and Appendix 3 (Information Operations) to Annex C (Operations).

1. (U) Situation. Refer to the Base Plan.

a. (U//~~FOUO~~) General. Our Adversaries are using cyberspace to execute command and control, to enhance logistics and acquisition, to disseminate their ideology of violence, solicit and gather the finances for operations, train the present cadre of insurgents in traditional and modern TTPs, and radicalize the next generation of terrorists. One way to effectively disrupt their freedom of maneuver in these efforts is by (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(1). (U//~~FOUO~~) For the purpose of this document, (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
actions that affect adversary information.

(2). (U//~~FOUO~~) Opportunities to neutralize, counter, or prosecute adversary operations in and through cyberspace will emerge and disappear within minutes, at best, and seconds, at worst. While (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

b. (U//~~FOUO~~) Adversary. (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) (adversaries) targeting the USG with multiple objectives, operating at different levels of competence and capability, in struggles of differing philosophies and ends – all occurring simultaneously. Some adversaries are content to intrude on and exfiltrate data in mass; others use

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2032~~

(INTENTIONALLY BLANK)

c. (U) Coordinating Instructions

(1) (~~S//REL~~) (b)(1) Sec 1.4(a) Respective combantant command (b)(1) Sec 1.4(a) When required, (b)(1) Sec 1.4(a)

(2) (S//REL) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(3) (U) USSTRATCOM Component Commands will integrate planning efforts to achieve CDRUSSTRATCOM and combatant command objectives and desired effects.

(4) (~~S//REL~~) CDRUSSTRATCOM will coordinate with combatant commanders in order to develop, and provide to those commands, IO capabilities that can be used to achieve objectives (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

4. (U) Administrative and Logistics. Refer to the Base Plan.

5. (U) Command and Control. Refer to the Base Plan and Annex J (Command Relationships).

planning and employment with all affected COCOMs and DOD Components.

(b). (~~S//REL~~) Coordinate (b)(1) Sec 1.4(a) with affected Combatant Commands, DOD Components, (b)(1) Sec 1.4(a)

(c). (~~S//REL~~) Coordinate with all applicable (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(d). (~~S//REL~~) USSTRATCOM components and supported COCOMs will (b)(1) Sec 1.4(a)

(e). (~~S//REL~~) USSTRATCOM (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(f). (~~S//REL~~) USSTRATCOM and subordinate Joint Combatant Commands/JTFs will coordinate necessary action for supported Combatant Commands/Services/Agencies (CC/S/A) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(2) (U) Combatant Commands

(a). (~~S//REL~~) Coordinate (b)(1) Sec 1.4(a) ISR resources (b)(1) Sec 1.4(a) and USSTRATCOM as required.

(b). (~~S//REL~~) Coordinate (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) surveillance assets as required in accordance with all applicable (b)(1) Sec 1.4(a)

(c). (~~S//REL~~) Develop and/or manage the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(d). (~~C//REL~~) Maintain, update, and provide access to the combatant command (b)(1) Sec 1.4(a)

(e). (~~S//REL~~) Conduct (b)(1) Sec 1.4(a) surveillance to help ensure freedom of action in cyberspace to USG. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE, NEBRASKA 68113-6500
28 February 2008

TAB D TO APPENDEX C TO USSTRATCOM CONPLAN 8039 (U)

(U) OPR: JIOWC

(b)(1) Sec 1.7(e) (U)

(U) References: Refer to Base Plan.

a. (U) (b)(1) Sec 1.7(e) 31 Jul 2002 (S)

b. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) Feb 1996 (U)

c. (U) (b)(1) Sec 1.7(e) 7 Apr 2000 (U)

d. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) 1 Oct 1993 (FOUO)

1. (U) Situation. Refer to Base Plan.

2. (U) Mission. Refer to Base Plan.

3. (U) Execution

a. (~~S//REL~~) Concept of Operations. For the purpose of CONPLAN 8039,
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) These and Intelligence, Surveillance, and Reconnaissance (ISR) assets conduct operations globally to ensure freedom of action in cyberspace for the US, (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) IAW applicable combatant command standing rules of engagement (ROE).

b. (U) Tasks

(1) (U) USSTRATCOM

(a). (~~S//REL~~) Coordinate (b)(1) Sec 1.4(a)

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2032~~

(2) (U//~~FOUO~~) A strict "need-to-know" policy must be announced, enforced, and maintained throughout the entire operation. The need-to-know policy should cover classified and unclassified information. While all personnel must be familiar with the critical information list, personnel do not have a need-to-know specific facts comprising critical information for areas of the plan in which they are not involved. Limiting information distribution will dramatically reduce the chances for accidental compromise of unclassified, but sensitive information that is critical to the success of the operation.

(3) (U//~~FOUO~~) Initiation and termination of OPSEC measures and related activities will be coordinated through the OPSEC Working Group.

(4) (U//~~FOUO~~) Dissemination of the critical information list as widely as possible within security and OPSEC guidelines is essential to OPSEC awareness.

(5) (U//~~FOUO~~) Provisions of OPSEC support to this plan should be coordinated with the PAO. (b)(1) Sec 1.7(e)

(6) (U) OPSEC Concerns. Personnel are encouraged to contact the USSTRATCOM OPSEC Officer to report OPSEC concerns, request guidance, and to provide suggestions for process improvement.

4. (U) Administration and Logistics

a. (U) Administration. Command OPSEC program officers/managers must be appointed in writing. Identify in writing these OPSEC officers/managers to the STRATCOM J39/JFCC GSI J39 OPSEC officer.

b. (U) Logistics. Not used.

5. (U) Command and Control

a. (U) OWG. An OWG comprised of representatives from all supporting Combatant Commands/Joint Force Commands supporting this plan will be convened as necessary. Reporting of OPSEC disclosures to the OWG will be made for the purpose of ensuring the currency of OPSEC awareness as it pertains to this plan.

b. (U) OPSEC Procedures. Conduct periodic reviews and evaluations of OPSEC procedures in order to improve the USSTRATCOM OPSEC Program.

(b) (U//~~FOUO~~) In coordination with J6, update monitoring priorities and key word lists.

(c) (U//~~FOUO~~) Attend all planning group meetings / discussions to include (b)(1) Sec 1.7(e)

(2) (U//~~FOUO~~) J2

(a) (U//~~FOUO~~) Provide an assessment of the effectiveness of OPSEC countermeasures.

(b) (~~S//REL USA, AUS, GBR~~) Utilize the OPSEC process to enable other (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(3) ~~(C)~~ J6

(a) (U//~~FOUO~~) Identify secure/encrypted communications shortfalls based upon CONPLAN operations.

(b) (~~C//REL USA, AUS, GBR~~) Develop a communications plan that (b)(1) Sec 1.4(a)

(4) (U//~~FOUO~~) PAO. Coordinate PA Guidance with OPSEC Working Group in order to prevent disclosures.

(5) (~~C//REL USA, AUS, GBR~~) Force Protection. Coordinate facility (b)(1) Sec 1.4(a)

(6) (U//~~FOUO~~) Division Chiefs (or OWG members). Periodically remind staff personnel of USSTRATCOM critical information and indicators, vulnerabilities, and adversary intelligence collection capabilities.

c. (U) Coordinating Instructions

(1) (U//~~FOUO~~) To protect against collection from adversaries, USSTRATCOM personnel must be cognizant when using unsecured means of communications such as the NIPRNET, facsimile, cell phones, Defense Switching Network (DSN) telephones, and common telephones. Anytime personnel are communicating over an unsecure or unencrypted means of communication they must not disclose critical or sensitive information pertaining to CONPLAN 8039.

5. (U) Details of military ties, agreements, arrangements between the DOD, the interagency, commercial industries, and partner nations.

6. (U) Details of security measures or procedures with other federal, state, or local agencies. Vulnerabilities, discovered through regular cyberspace assessments, and those corrective measures recommended.

7. (U) Capabilities, facility and network diagrams, infrastructure layouts, connectivity information, status/readiness of cyberspace assets, alert status/procedures of forces supporting this CONPLAN.

8. (U) Details and vulnerabilities of a Combatant Commander's C4ISR architecture and physical security infrastructure.

9. (U) Operational and technical details, including Tactics, Techniques, and Procedures (TTP), of cyberspace operations.

d. (U) Assumptions. Refer to Base Plan.

2. (U) Mission. Refer to Base Plan.

3. (U) Execution

a. (U) Concept of Operations. The purpose of OPSEC is to prevent adversaries from obtaining friendly critical information. While OPSEC should be practiced at the same rigor whether in garrison, during training, or deployed conducting operations, leaders at all levels are encouraged to remind their personnel of the importance of OPSEC during the planning and execution of this CONPLAN and to apply OPSEC TTPs to protect critical information and indicators regarding force intentions, capabilities, and vulnerabilities. The OPSEC process will be integrated into this plan, and its supporting plans and operations, to the fullest extent possible. Based on identification of critical information, analysis of the threat and friendly vulnerabilities, OPSEC officers/managers/planners will assess risk to mission and then implement appropriate countermeasures to increase overall mission effectiveness.

b. (U) Tasks

(1) (U//~~FOUO~~) USSTRATCOM OPSEC Officer

(a) (U//~~FOUO~~) Use the OPSEC Working Group (OWG) meeting to evaluate CILs and countermeasures and promulgate the OPSEC plan. The OWG members will then increase OPSEC awareness within their respective directorate to decrease the chance of critical information disclosure.

(d) (U) Assess Risk. A determination of how much damage to the cyberspace mission and commander's intent will be caused by the loss/disclosure of the critical information.

(e) (U) Implement Countermeasures. Anything that effectively negates an adversary's ability to gather or exploit friendly critical information or that renders the possession of the critical information useless. While not a formal step of the OPSEC Process, (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) the OPSEC planner to monitor utility of implemented countermeasures and, if required, re-initiate the cyclic nature of the OPSEC process to improve on the actions taken.

(3) (U) Critical Information

(a) (U) In any operation, it is vital to achieve 'essential secrecy' which is the condition achieved as a result of denying adversaries friendly forces critical information. Because of the requirements to share operational information across many agencies and to other governments, care must be taken to emphasize the need to protect critical information.

(b) (U) Critical Information is the specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to cause a delay, disruption, total failure, or unacceptable consequences for friendly mission accomplishment.

(c) (U) Each C/S/A supporting this plan will develop a Critical Information List (CIL). Once developed, the CIL will be used to support the 5-step OPSEC process. The following are generalized Critical Information items that pertain to this CONPLAN. Actual words and/or phrases that address or provide specifics covered below must not be discussed over non-secure means or in public spaces in order to protect critical information from disclosure and adversary exploitation.

1. (U) Association of the operational execution of this CONPLAN with any specific target or country.

2. (U) Association of this CONPLAN with exercises, operational rehearsals, or other mission-specific training that supports this CONPLAN.

3. (U) Association of abbreviations, acronyms, nicknames, or code words with this CONPLAN or locations.

4. (U) Movement/billeting of forces and senior decision makers when conducted in support of this plan.

(3) (U) Responsibility for OPSEC. OPSEC is a command responsibility. At each level of command, the operations officer (or equivalent), has staff responsibility for coordinating overall OPSEC planning. Every individual involved with or supporting CONPLAN 8039 must assist in safeguarding classified and unclassified information deemed sensitive or critical to the success of this CONPLAN.

b. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

c. (U) Friendly Forces. Refer to Base Plan and Annex A (Task Organization).

(1) (U) Friendly Operations. Adversaries can exploit OPSEC vulnerabilities and correlate information obtained by various collection and exploitation methods. Therefore, we must operate in such a manner as to deny friendly information necessary for adversaries to accurately estimate the military situation/friendly capability, and simultaneously contribute to adversely affecting their decision cycles.

(2) The OPSEC process. OPSEC is a continuous analytical process which focuses on identifying, controlling, and protecting evidence associated with any operation. OPSEC is not a physical, personnel, or information security system; nor is it a collection of rules or instructions. Like the overall integration of IO, OPSEC is a function of planning; this planning must apply appropriate countermeasures to achieve desired effects during execution of operations. IAW reference (b), all Combatant Commands and supporting joint forces will use the five-step OPSEC process:

(a) (U) Identify Critical Information. That information, if exploited by an adversary, would significantly impede friendly operations or prevent mission accomplishment. Combatant Commands should provide their critical information lists to USSTRATCOM and other pertinent Combatant Commands, to facilitate protection of sensitive information.

(b) (U) Analyze the Threat. A formal assessment of the adversary's capability and intent to exploit any critical information. Combatant Commands should task supporting intelligence elements to provide analysis tailored for OPSEC planners that focus on cyberspace threats and as appropriate, state and non-state threat collection capabilities and intentions. (b)(1) Sec 1.7(e) related information that most be considered by personnel when planning for, exercising, or conducting cyberspace operations.

(c) (U) Analyze Vulnerabilities (and specific signatures / indicators). A determination of how susceptible cyberspace operations related critical information is to loss/disclosure.

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AFB, NE 68113-6500
28 February 2008

TAB C TO APPENDIX 3 TO ANNEX C TO US STRATEGIC COMMAND CONPLAN 8039 (U)
(U) OPR: JIOWC/J36
OPERATIONS SECURITY (U)

(U) References. Refer to Base Plan and Appendix 3 (Information Operations) to Annex C (Operations).

a. (U) CJCSI 3213.01B, Joint Operations Security, 17 Dec 2003 (U)

b. (U) Joint Pub 3-13.3, Joint Doctrine for Operations Security, 29 Jun 2006 (U)

c. (U) CJCSI 6510.01D, Information Assurance and Computer Network Defense, 15 Jun 2004 (U)

1. (U) Situation. Refer to Base Plan.

a. (U) General

(1) (~~S//REL USA, AUS, GBR~~) Purpose. This Tab provides planning guidance for integrating OPSEC into (b)(1) Sec 1.4(a) CONPLAN 8039 (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(2) (U) Overview. OPSEC is the process of denying adversaries information about friendly intentions and capabilities by identifying, controlling, and protecting indicators associated with planning and conducting of operations and other activities. When applied, OPSEC measures prevent an adversary's timely exploitation of critical friendly information relating to operational plans, special technologies, capabilities, and relationships. OPSEC measures include protection of primarily unclassified information that can model or profile friendly intentions and capabilities through analysis, compilation, and integration of multiple-source information including that available through open sources and international media coverage.

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2032~~

PAGE INTENTIONALLY BLANK

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE, NE 68113-6500
28 February 2008

TAB B TO APPENDIX 3 TO ANNEX C TO USSTRATCOM CONPLAN 8039 (U)
(U) OPR: HQ USSTRATCOM J39
(b)(1) Sec 1.7(e) (U)

(U) References: Refer to the Base Plan.

1. (U) Situation. Refer to the Base Plan.

2. (U) Mission. Refer to the Base Plan.

3. (~~S//REL USA, AUS, GBR~~) Execution. Information concerning (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) in CONPLAN 8039 is handled in (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) is required.

4. (U) Administration and Logistics. Refer to the Base Plan.

5. (U) Command and Control. Refer to the Base Plan.

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2032~~

INTENTIONALLY BLANK

5. (~~S//REL USA, AUS, GBR~~) Command and Control. CDRUSSTRATCOM is the supported commander for planning and may be designated the supported commander for execution. As required, (b)(1) Sec 1.4(a) will provide the supported commander the necessary (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) The supported commander will identify (b)(1) Sec 1.4(a)

a. (~~S//REL USA, AUS, GBR~~) Headquarters Locations and movements. As required, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

b. (~~S//REL USA, AUS, GBR~~) Supporting (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

c. (U) C4 support requirements and responsibilities for (b)(1) Sec 1.7(e) liaison officers are situation dependent based on (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) computer networks.

(g) (~~S//REL USA, AUS, GBR~~) Confirm capabilities and (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(h) (~~S//REL USA, AUS, GBR~~) As required, assist in the identification and staffing of (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(4) (U) (b)(1) Sec 1.7(e)
when requested.

4. (U) Administration and Logistics. The requirements below reflect those necessary for sustainment in the event (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) supported commander.

a. (U) Administration. Not used.

b. (U) Logistics

(1) (U) ICW USSTRATCOM, and (b)(1) Sec 1.7(e) the affected GCC will
(b)(1) Sec 1.7(e)
requirements.

(2) (U) USSTRATCOM ICW (b)(1) Sec 1.7(e) and the affected GCC will coordinate the (b)(1) Sec 1.7(e) equipment and materials.

(3) (U) USSTRATCOM ICW (b)(1) Sec 1.7(e) and the affected GCC will coordinate fiscal matters relating to special funds.

(4) (U) USSTRATCOM ICW (b)(1) Sec 1.7(e) and the affected GCC will coordinate (b)(1) Sec 1.7(e)

(5) (U) USSTRATOM will coordinate movement of personnel and equipment to (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(e) (U) Coordinate (b)(1) Sec 1.7(e)

(2) (U) (b)(1) Sec 1.7(e)

(a) (~~S//REL USA, AUS, GBR~~) Plan, develop, coordinate, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b) (b) (~~S//REL USA, AUS, GBR~~) ICW affected GCCs, request support from (b)(1) Sec 1.4(a) as required.

(c) (~~S//REL USA, AUS, GBR~~) Coordinate (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) with GCCs.

(d) (~~S//REL USA, AUS, GBR~~) ICW (b)(1) Sec 1.4(a) and the affected GCC, (b)(1) Sec 1.4(a)

(e) (~~S//REL USA, AUS, GBR~~) Coordinate with (b)(1) Sec 1.4(a) affected GCCs, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(3) (U) Commander (b)(1) Sec 1.7(e)

(a) (~~S//REL USA, AUS, GBR~~) Prepare (b)(1) Sec 1.4(a) in support of cyberspace operations.

(b) (~~S//REL USA, AUS, GBR~~) Conduct (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(c) (~~S//REL USA, AUS, GBR~~) Conduct (b)(1) Sec 1.4(a)

(d) (~~S//REL USA, AUS, GBR~~) Provide copies of all cyberspace related products to (b)(1) Sec 1.4(a) and affected GCCs.

(e) (~~S//REL USA, AUS, GBR~~) Determine critical requirements shortfalls (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(f) (~~S//REL USA, AUS, GBR~~) Develop and provide detailed (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

conventional missions and units as necessary. Commander, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(d) (~~S//REL USA, AUS, GBR~~) CDRUSSTRATCOM/Geographic Combatant Commanders. Be prepared to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) as requested and required.

(3) (U) Authorities

(a) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Geographic Combatant Commander's are the approval authority (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(c) (~~S//REL USA, AUS, GBR~~) The designated supported commander for execution is delegated (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(d) (~~S//REL USA, AUS, GBR~~) Geographic Combatant Commanders. In coordination with (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

e. (U) Tasks

(1) (U) GCCs

(a) (~~S//REL USA, AUS, GBR~~) Integrate cyberspace (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) cyberspace operations strategy.

(c) (U) Accept OPCON or TACON (b)(1) Sec 1.7(e) to conduct operations.

(d) (U) Be prepared to provide Service-unique capability to support (b)(1) Sec 1.7(e)

4 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(f) (U) USG National Goal 6: Defending US citizens and interests at home and abroad.

1 (U) (b)(1) Sec 1.7(e)

2 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

b. (U) End State. Refer to the Base Plan.

c. (U) Situation Monitoring and Measures of Effectiveness. Intelligence (b)(1) Sec 1.7(e) security monitoring, and operational feedback mechanisms to support this CONPLAN and determine measures of effectiveness will be determined for each situation, permissive or otherwise.

d. (U) Control

(1) (~~S//REL USA, AUS, GBR~~) Approval Process. The (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) and cyberspace (b)(1) Sec 1.4(a) USSTRATCOM thru coordination with the (b)(1) Sec 1.4(a) USSTRATCOM recommends cyberspace (b)(1) Sec 1.4(a) submits cyberspace (b)(1) Sec 1.4(a) for approval. Once cyberspace (b)(1) Sec 1.4(a) are approved CDRUSSTRATCOM is the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) In all other cases, the GCC is delegated product approval authority.

(2) (U) Responsibilities

(a) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) guidance and programs approval authority.

(b) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) approval and dissemination authority to the designated Supported Commander (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(c) (~~S//REL USA, AUS, GBR~~) Commander, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

3 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(c) (U) USG National Goal 3: Defeat terrorist organizations.

1 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

3 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

4 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(d) (U) USG National Goal 4: Deny sponsorship/support/sanctuary to terrorist organizations.

1 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

3 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

4 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(e) (U) USG National Goal 5: Diminish the underlying causes of terrorism.

1 (U) (b)(1) Sec 1.7(e)

2 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

3 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

3. (S//REL USA, AUS, GBR) US (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

4. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

5. (~~S//REL USA, AUS, GBR~~) The victims (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(b) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(d) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) The most significant (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(6) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(a) (U) USG National Goal 1: Deter aggression and counter coercion.

1 (U) (b)(1) Sec 1.7(e)

2 (U) (b)(1) Sec 1.7(e)
community.

(b) (U) USG National Goal 2: Dissuade/Defeat potential adversaries.

1 (U) (b)(1) Sec 1.7(e)

2 (U) (b)(1) Sec 1.7(e)

(2) (~~S//REL USA, AUS, GBR~~) Guidance. CDRUSSTRATCOM thru coordination with (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) activities. Initiate required actions to deploy forces required in support of USSTRATCOM CONPLAN 8039.

(3) (U) (b)(1) Sec 1.7(e) will be developed and included in the appropriate appendices to (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(4) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) CDRUSSTRATCOM thru coordination with CDRUSSOCOM will develop and publish in (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(5) (U) (b)(1) Sec 1.7(e)

(~~S//REL USA, AUS, GBR~~) Operational Guidance. OPE will be used to provide predictive analysis (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(a) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

1. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) to those goals.

(b)(1) Sec 1.4(a)

(5) (~~S~~) Use (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

g. (U) Assumptions. Refer to the Base Plan.

(1) (~~S~~) Interagency information (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(2) (S) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2. (U) Mission. Refer to the Base Plan.

3. (U) Execution

a. (U) Concept of Operations. The purpose of (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(1) (~~S//REL USA, AUS, GBR~~) Overview. Advise the CJCS, USSTRATCOM, and GCCs on cyberspace information measures, themes, and
(b)(1) Sec 1.4(a)

(k) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(l) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(m) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(n) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(o) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(p) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(4) (U) Command Systems. Refer to Annex B (Intelligence) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

e. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

f. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Tasks

(1) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(2) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) decision-making process.

(3) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(4) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

(2) (U) (b)(1) Sec 1.7(e) US military operations ISO this plan.

d. (U) (b)(1) Sec 1.7(e) Refer to the Base Plan, Annex B (Intelligence), (b)(1) Sec 1.7(e)

(1) (U) Decision Maker and Staff. Refer to Annex B (Intelligence) and (b)(1) Sec 1.7(e)

(2) (U) Intelligence Systems. Refer to Annex B (Intelligence) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(3) (U) Target Audiences

(a) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(c) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(d) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

(e) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

(f) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

(g) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) theater of operations.

(h) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(i) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) operations in and through cyberspace within their jurisdiction.

(j) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

1. (U) Situation

a. (~~S//REL USA, AUS, GBR~~) Overview. Cyberspace can play a role in the conduct (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) via the Global Information Grid (GIG). (b)(1) Sec 1.4(a) is responsible for the development and approval (b)(1) Sec 1.4(a) the cyberspace community can support as one of many methods (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

b. (U) US and Allied Perspective

(1) (U) Refer to the Base Plan and Annex A (Task Organization).

(2) (U) US Department of State (DOS)

(a) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) prior to the initiation of cyberspace activities.

(b) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Furnishes advice (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) communications capabilities. The Office may release select (b)(1) Sec 1.4(a) assets to the appropriate combatant command's control IAW (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(3) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(4) (~~S//REL USA, AUS, GBR~~) Under Secretary of Defense - Policy (USD-P) . Will delegate (b)(1) Sec 1.4(a) CDRUSSTRATCOM upon request and implementation of CONPLAN 8039.

(5) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) US agencies per existing agreements.

c. (U) Neutral Perspective

(1) (U) Refer to the Base Plan, Annex B (Intelligence), (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AFB, NE 68113-6500
28 February 2008

TAB A TO APPENDIX 3 TO ANNEX C TO USSTRATCOM CONPLAN 8039 (U)
(U) OPR: JIOWC/J36
(b)(1) Sec 1.7(e) (U)

(U) References. Refer to the Base Plan.

a. (U) Executive Order 12333, 4 December 1981, "United States Intelligence Activities"

b. (U) (b)(1) Sec 1.7(e)

c. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) S)

d. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) (FY) 2002."

e. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
FY 2002."

f. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

g. (U) Joint Pub 3-57.1, 14 April 2003, "Joint Doctrine for Civil Affairs."

h. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

i. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2032~~

(b)(1) Sec 1.4(a)
Operations.

c. (~~S//REL USA, AUS, GBR~~) Determination of command relationships (TACON / OPCON) of forces shall be provided in published WARNORD(S)/EXORD(S) or the applicable (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

d. (U) External Agency Support. During exercises and contingencies, USSTRATCOM components and agencies such as, but not limited to JIOWC, JFCC NW, JTF_GNO, DISA, the JWAC, and Joint COMSEC Monitoring Agency, may deploy to USSTRATCOM AOR or a supporting location as required.

Tabs:

A - (U) (b)(1) Sec 1.7(e)
B - (U) Electronic Warfare
C - (U) Operations Security
D - (U) (b)(1) Sec 1.7(e)
E - (U)
F - (U)
G - (U) Response Actions

4. (~~S//REL USA, AUS, GBR~~) USSTRATCOM. Develop and conduct (b)(1) Sec 1.4(a)

5. (~~S//REL USA, AUS, GBR~~) USSTRATCOM. Facilitate (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

6. (U) JFCC GSI. (b)(1) Sec 1.7(e) IO capabilities as needed.

c. (U) (b)(1) Sec 1.7(e) Activities in this (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) action in cyberspace.

d. (U) Coordinating Instructions

(1). (U) IO will be conducted through centralized planning and decentralized execution. JFCC GSI J39 will establish IO objectives and associated tasks. JFCC GSI J39 will coordinate IO plans and objectives with supporting commands, components, and support agencies.

(2) (U) Supporting elements will give daily IO Situational Reports through the USSTRATCOM GOC providing the status of execution of supporting tasks in support of IO objectives.

4. (U) Administration and Logistics. Refer to Base Plan.

a. (U) Forces utilized in this CONPLAN include deployable or fixed assets operating in CONUS or from sites located throughout the world and are controlled as separate forces. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) AOR. During a contingency, USSTRATCOM Service components will ensure all mission-critical cyberspace forces (fixed and mobile), are fully supported and capable of performing their mission.

5. (U) Command and Control

a. (U) Refer to Annex K (Command Control, Communications and Computer Systems), (b)(1) Sec 1.7(e)

b. (~~S//REL USA, AUS, GBR~~) Special IO Communication and Reporting Requirements. (b)(1) Sec 1.4(a)

6. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

7. (U) (b)(1) Sec 1.7(e)

8. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

9. (U) (b)(1) Sec 1.7(e)

10. (U) (b)(1) Sec 1.7(e)

11. (U) (b)(1) Sec 1.7(e)

12. (U) (b)(1) Sec 1.7(e)

13. (U) Support activities establishing (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

14. (~~S//REL USA, AUS, GBR~~) Objective Balancing. When (b)(1) Sec 1.4(a)

b. (U) (b)(1) Sec 1.7(e) Tasks

1. (U) Supporting CDRs. Employ IO options in support of USSTRATCOM (b)(1) Sec 1.7(e) objectives as directed. Maintain sufficient strategic reserve. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

2. (~~S//REL USA, AUS, GBR~~) JTF GNO. Coordinate with supporting commanders, Service and functional components (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

3. (~~S//REL USA, AUS, GBR~~) JIOWC. Facilitate interagency coordination and integration (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) considered and made available to decision makers.

(b)(1) Sec 1.4(a)

5. (~~S//REL USA, AUS, GBR~~) JFCC GSI. Through the use of collaborative tools, (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

c. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Activities in this
(b)(1) Sec 1.4(a)
cyberspace.

(5) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) The intent of this
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) operations if necessary. IO efforts (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

a. (U) (b)(1) Sec 1.7(e) Strategic IO objectives. The following objectives
(b)(1) Sec 1.7(e)

1. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

3. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

4. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

5. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(4). (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) The intent of this (b)(1) Sec 1.4(a)

a. (U) (b)(1) Sec 1.7(e) Strategic IO objectives

1. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) to other operations through cyberspace will be covered in (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

2. (~~S//REL USA, AUS, GBR~~) Objective Balancing. When executing (b)(1) Sec 1.4(a)

b. (U) (b)(1) Sec 1.7(e) Tasks

1. (U) Supporting CDRs. (b)(1) Sec 1.7(e) USSTRATCOM cyberspace objectives as directed. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

2. (~~S//REL USA, AUS, GBR~~) JTF-GNO. IAW published IA/CND Plans coordinate with supporting commanders, Service and functional components to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) essential elements of friendly information.

3. (~~S//REL USA, AUS, GBR~~) JFCC GSI/JFCC NW. Coordinate (b)(1) Sec 1.4(a)

4. (~~S//REL USA, AUS, GBR~~) JIOWC. Facilitate interagency coordination and integration (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)
actors.

2. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) OPLAN.

3. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) adversaries.

4. (U) Utilize IO to maximize effectiveness of force deployment,
(b)(1) Sec 1.7(e)

b. (U) (b)(1) Sec 1.7(e) Tasks

1. (U) Supporting CDRs. Employ IO options in support of USSTRATCOM cyberspace objectives as directed. (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

2. (~~S//REL USA, AUS, GBR~~) JTF-GNO. IAW published IA/CND Plans coordinate with supporting commanders, Service and functional components to (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) essential elements of friendly information.

3. (~~S//REL USA, AUS, GBR~~) JFCC GSI/JFCC NW. Coordinate
(b)(1) Sec 1.4(a)

4. (~~S//REL USA, AUS, GBR~~) JIOWC. Facilitate interagency coordination and integration (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(U) 5. (~~S//REL USA, AUS, GBR~~) JFCC GSI. Collaborate with the effected GCC(s) and applicable agencies.

6. (~~S//REL USA, AUS, GBR~~) Objective Balancing. When executing
(b)(1) Sec 1.4(a)

c. (U) (b)(1) Sec 1.7(e) Activities in this (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) cyberspace mission(s).

1. (U) JTF GNO. Coordinate with supporting commanders, Service and functional components to develop robust IA to protect our critical information systems.

2. (~~S//REL USA, AUS, GBR~~) JFCC GSI/JFCC NW. Identify, prioritize, and obtain (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) reflected in validated national collections requirements.

3. (U) JFCC GSI/JIOWC. Facilitate interagency coordination and integration of appropriate (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) Through the use of collaborative tools, integrate planning actions (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

4. (U) USSTRATCOM. Support US declaratory policy by preparing CDRUSSTRATCOMs positions. Adjust force posture. Adjust themes and messages.

(c). (U) (b)(1) Sec 1.7(e) Activities (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) in support of cyberspace mission(s).

(3) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) The intent of (b)(1) Sec 1.4(a)

a. (U) (b)(1) Sec 1.7(e) Strategic IO objectives. Continue ongoing objectives (b)(1) Sec 1.7(e) following strategic objectives:

1. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(c) (U) (b)(1) Sec 1.7(e) End State. Activities in this (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) CDRUSSTRATCOM to present available IO COAs in support of cyberspace mission(s) (b)(1) Sec 1.7(e)

(2) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) force posture or execution of the identified options. IO actions conducted (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) actions lead to achievement of US strategic objectives.

(a). (U) (b)(1) Sec 1.7(e) Strategic IO Objectives. (b)(1) Sec 1.7(e) strategic objectives. Strategic Communication (SC) themes and messages will be situation dependant (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) consequences to the current adversarial government once their forces are neutralized.

1. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

2. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

3. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

4. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) integrated to best achieve the commander's objectives.

5. (~~S//REL USA, AUS, GBR~~) Objective Balancing. When executing (b)(1) Sec 1.4(a)

(b). (U) (b)(1) Sec 1.7(e) Tasks

(b)(1) Sec 1.4(a) Develop and manage IO COAs derived from the (b)(1) Sec 1.4(a)

3. (~~S//REL USA, AUS, GBR~~) JFCC GSI/JFCC NW. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) necessary to accomplish detailed planning of IO options.

4. (~~S//REL USA, AUS, GBR~~) JFCC GSI/JFCC NW. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Develop baseline force structure.

5. (U) JTF-GNO. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) USSTRATCOM information systems. Coordinate with supporting commanders, Service and functional components to develop robust IA and OPSEC plans to protect our critical information systems and essential elements of friendly information.

6. (~~S//REL USA, AUS, GBR~~) JFCC GSI/JTF GNO. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

7. (~~S//REL USA, AUS, GBR~~) JFCC GSI/Supporting CDRs. Develop IO options (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

8. (U) JIOWC. Facilitate interagency coordination and integration of appropriate IO themes, and responses to support objectives (b)(1) Sec 1.7(e) Provide Combatant Commanders with IO support teams, integrate and coordinate (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

9. (U) USSTRATCOM, Services and Agencies

a. (U) Identify and assist in development of IO capabilities necessary to meet validated requirements.

b. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) of these issues.

c. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) maintain situational awareness.

b. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

c. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

9. (~~S//REL USA, AUS, GBR~~) Incorporate IO capabilities, as they become available (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

a. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Develop and implement IO options which when (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

b. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

10. (~~S//REL USA, AUS, GBR~~) Objective Balancing. When executing (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(b). (U) (b)(1) Sec 1.7(e) Tasks

1. (U) USSTRATCOM. (b)(1) Sec 1.7(e) USSTRATCOM staff and components, supporting commands and agencies are adequately trained in the IO disciplines needed to meet (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) Assess and identify IO capabilities against potential adversaries (b)(1) Sec 1.7(e) Support US declaratory policy by preparing CDRUSSTRATCOM positions. Establish IO requirements for CDRUSSTRATCOM-directed objectives.

2. (~~S//REL USA, AUS, GBR~~) JFCC GSI. (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) Key to success is working with supporting and component commands, Combatant Commanders and outside agencies on the integration and synchronization of the following strategic objectives:

(a). (U) (b)(1) Sec 1.7(e) IO Strategic Objectives

1. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) US is capable of (b)(1) Sec 1.4(a) networks.

2. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

3. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) adversaries.

4. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) adversaries.

5. (~~S//REL USA, AUS, GBR~~) Ensure friendly forces have (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

6. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) infrastructures.

7. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

8. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

a. (~~S//REL USA, AUS, GBR~~) C4I Systems. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(a). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(b). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(2). (U) (b)(1) Sec 1.7(e)
Example actions may include:

(a). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(b). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(3) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) Example actions may include:

(a). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(b). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

c. (U) (b)(1) Sec 1.7(e)

(1). (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) The strategy of this
(b)(1) Sec 1.4(a)

(b)(1) Sec 1.7(e) effects. It is important to note that IO plans that incorporate (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(b). (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) on the supporting information infrastructure. The DOD's (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Refer to Plan Summary, Base Plan and Annex C for more detailed descriptions of defense types.

(c). (~~S//REL USA, AUS, GBR~~) End State. Refer to the Base Plan and Annex C (Operations). (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) and appropriate legal, informational, military, diplomatic or economic measures are taken (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) US resumes normal cyber operations. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) DOD is postured to support homeland security, critical infrastructure protection, and civil support. US, allies, and coalition partners have freedom of action to operate in cyberspace.

(d). (U) Cyber Engagement Criteria. Refer to the Base Plan.

b. (U) Strategic Objectives/IO Tasks. General IO tasks will be covered in Tabs A through G of Appendix 3 (Information Operations). All types of cyber defense will be utilized (b)(1) Sec 1.7(e)

(1). (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) Example actions may include:

IO (b)(1) Sec 1.4(a) Additionally, USSTRATCOM (b)(1) Sec 1.4(a)

(2) (~~S//REL USA, AUS, GBR~~) The commander's IO efforts will (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) by employing assigned IO assets to protect USSTRATCOM information from (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) while ensuring readiness, reliability, and continuity of the DOD GIG and the critical information infrastructure. IO (b)(1) Sec 1.4(a)

(a). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

1. (U) COAs. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) The primary method of supporting the mission is through the development of integrated IO courses of action (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) courses of action underscore the importance of contingency planning and early response to a crisis. Given clearly stated objectives and effectively integrated IO capabilities, this has the potential to change the course of threatening events. Finally, when deterrence fails, IO (b)(1) Sec 1.7(e) COA. Refer to Figure C-3-1.

2. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) Specific implementation supporting (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) to Appendix 3 (Information Operations) to Annex C (Operations). (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) This appendix provides guidance for the planning, integration and implementation of current IO capabilities and development of future IO capabilities to support the planning, deployment and employment of US forces for dominance in cyberspace. (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

a. (U) Adversary. Refer to Annex B (Intelligence) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

b. (U) Friendly. Refer to the Base Plan.

(1) (U) The US and our allies are increasingly reliant on automated communications and information-based decision-making systems. These systems are vital to US warfighting capabilities. The US requires an integrated and synchronized approach to maintaining information superiority.

(2) (U) Essential Elements of Friendly Information. Refer to the Base Plan.

c. (U) Assumptions. Refer to the Base Plan.

2. (U) Mission. Refer to the Base Plan.

3. (U) (b)(1) Sec 1.7(e)

a. (~~S//REL USA, AUS, GBR~~) Concept of Operations. This appendix provides USSTRATCOM with (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) US vital interests and contribute to conflict termination on terms favorable to the US.

(1) [~~S//REL~~] This appendix provides a variety of preplanned courses of action (COA) that support CDRUSSTRATCOM objectives outlined in the Base Plan. (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) US and coalition forces. USSTRATCOM will coordinate, integrate, and synchronize DOD IO in support of assigned cyberspace missions, identify IO requirements and capabilities for cyber operations and, when directed, plan and or execute

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE, NEBRASKA 68113-6500
28 February 2008

APPENDIX 3 TO ANNEX C TO CDRUSSTRATCOM CONPLAN 8039 (U)
(U) OPR: JFCC GSI J39
INFORMATION OPERATIONS (U)

(U) References: Refer to Base Plan.

a. (U) CJCSI 3210.01B, Joint Information Operations Policy, 5 January 07 (S)

b. (U) DODD-3600.O1 Information Operations, 14 Aug 06 (U)

c. (U) Joint Pub 3-13.1 Joint Doctrine for Electronic Warfare, 25 Jan 2007 (U)

d. (U) Joint Pub 3-13, Information Operations, 13 Feb 2006 (U)

e. (U) (b)(1) Sec 1.7(e) 13 Jul 06 (U)

f. (U) (b)(1) Sec 1.7(e) 01 Aug 2007 (S)

g. (U) CJCSI 3210.03B, Joint Electronic Warfare Policy, 31 Jul 02 (S)

h. (U) JP 3-13.3 Joint Doctrine for Operations Security, 29 Jun 06 (U)

i. (U) (b)(1) Sec 1.7(e) 5 Sep 2003 (U)

k. (U) JP 3-09, Doctrine for Joint Fire Support, 13 Nov 2006 (U)

k. (U) JP 3-61, Joint Doctrine for Public Affairs, 9 May 2005 (U)

l. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) Jan 2006 (S//NF)

1. (~~S//REL USA, AUS, GBR~~) Situation. This appendix describes IO activities supporting USSTRATCOM's CONPLAN 8039. IO integrates the core capabilities of OPSEC, (b)(1) Sec 1.4(a) and CNO to achieve CDRUSSTRATCOM effects and objectives (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) to fulfill this plans objectives.

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2032~~

When employed successfully, IO (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(8) (U) Tasks. Refer to Base Plan for additional tasks and (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) For CONPLAN 8039 taskings, significant interagency support may be required. Access to the interagency will be through the Joint Staff or appropriate liaison elements. Refer to Annex V (Interagency Coordination) for further discussion. This CONPLAN will not explicitly task the interagency partners.

(9) (U) Coordinating Instructions. Refer to Base Plan.

4. (U) Administration and Logistics. Refer to the Base Plan.

5. (U) Command and Control. Refer to the Base Plan and Annex J (Command Relationships).

OFFICIAL

s/
Mark H. Owen
Brigadier General, USAF
Director, Plans and Policy

KEVIN CHILTON
General, USAF
Commander

Appendixes:
- 3 -- Information Operations
- 8 -- Rules of Engagement
- 9 -- Intelligence, Surveillance and Reconnaissance
- 16 -- Critical Infrastructure Protection
- 17 -- Network Operations
- 18 -- Time Sensitive Planning
- 19 -- Effect Assessment Guidance
- 20 -- (b)(1) Sec 1.7(e)

2. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
operations favor: (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) Refer to (b)(1) Sec 1.4(a) should consider the impact that a
(b)(1) Sec 1.4(a)

(d). (U) (b)(1) Sec 1.7(e)

1. (~~S//REL USA, AUS, GBR~~) Commander's Intent. (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
operations favor: (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(e). (U) (b)(1) Sec 1.7(e)

1. (~~S//REL USA, AUS, GBR~~) Commander's Intent. (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
operations favor: (b)(1) Sec 1.4(a) The
planner should consider (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(f). (U) (b)(1) Sec 1.7(e)

1. (~~S//REL USA, AUS, GBR~~) Commander's Intent. Provide
(b)(1) Sec 1.4(a)

2. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
operations favor (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(U)(e) ~~(S//REL USA, AUS, GBR)~~ Intelligence, Surveillance, and Reconnaissance (ISR) Operations. Refer to Appendix 9 (Intelligence, Surveillance and Reconnaissance) to Annex C (Operations).

(f) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(7) (U) Cyberspace (b)(1) Sec 1.7(e)

(a). (U) (b)(1) Sec 1.7(e)

1. (~~S//REL USA, AUS, GBR~~) Commander's Intent. Support US government efforts to (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
US national interests if attributed.

(b). (U) (b)(1) Sec 1.7(e)

1. (~~S//REL USA, AUS, GBR~~) Commander's Intent. (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) US national interests if attributed.

(c). (U) (b)(1) Sec 1.7(e)

1. (~~S//REL USA, AUS, GBR~~) Commander's Intent. (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

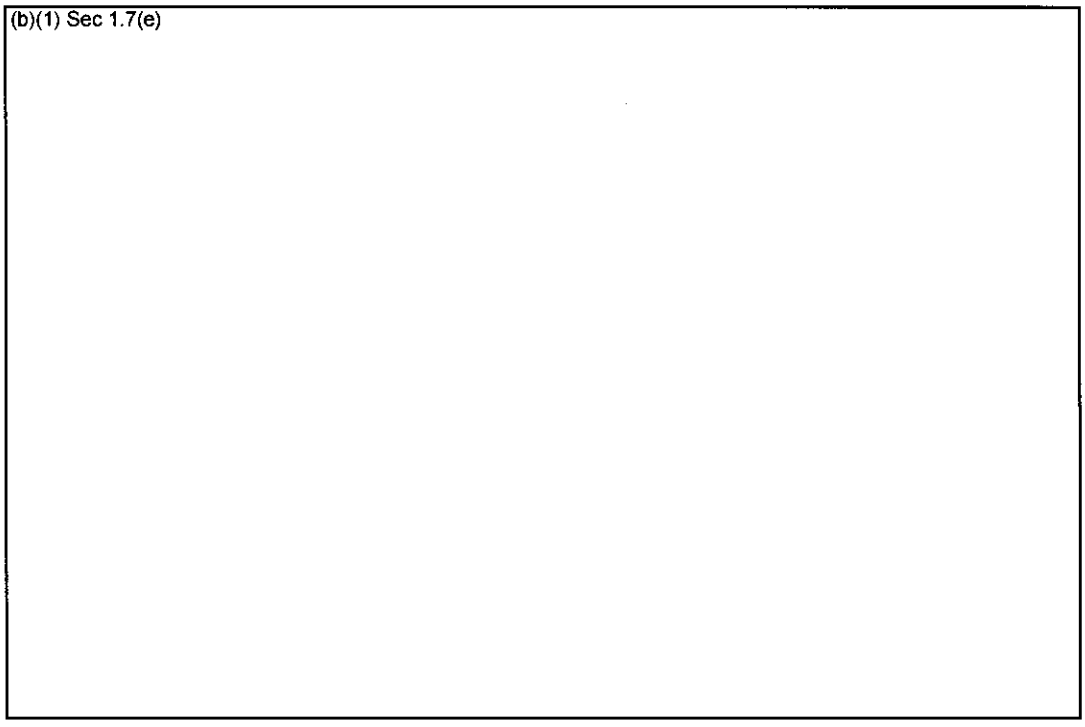


Figure 6: (U) Sample (b)(1) Sec 1.7(e) Activities

(6). (U) Supporting capabilities. In addition to USSTRATCOM's cyberspace capabilities, supporting capabilities will be synchronized to achieve (b)(1) Sec 1.7(e) within (b)(1) Sec 1.7(e) While each plan (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) there are capabilities that should be considered in any plan.

(a) (U) Strategic Communication. Refer to Annex Y (Strategic Communication)

(b) (U) (b)(1) Sec 1.7(e) Refer to Appendix 3 (b)(1) Sec 1.7(e) to Annex A (Task Organization) for general (b)(1) Sec 1.7(e) guidance (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(c) (U) Information Operations (IO). Refer to Appendix 3 (Information Operations) of Annex C (Operations) for detailed discussion of the integration of each core IO capabilities in support of CONPLAN 8039.

(d) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Refer to Annex (b)(1) Sec 1.4(a)

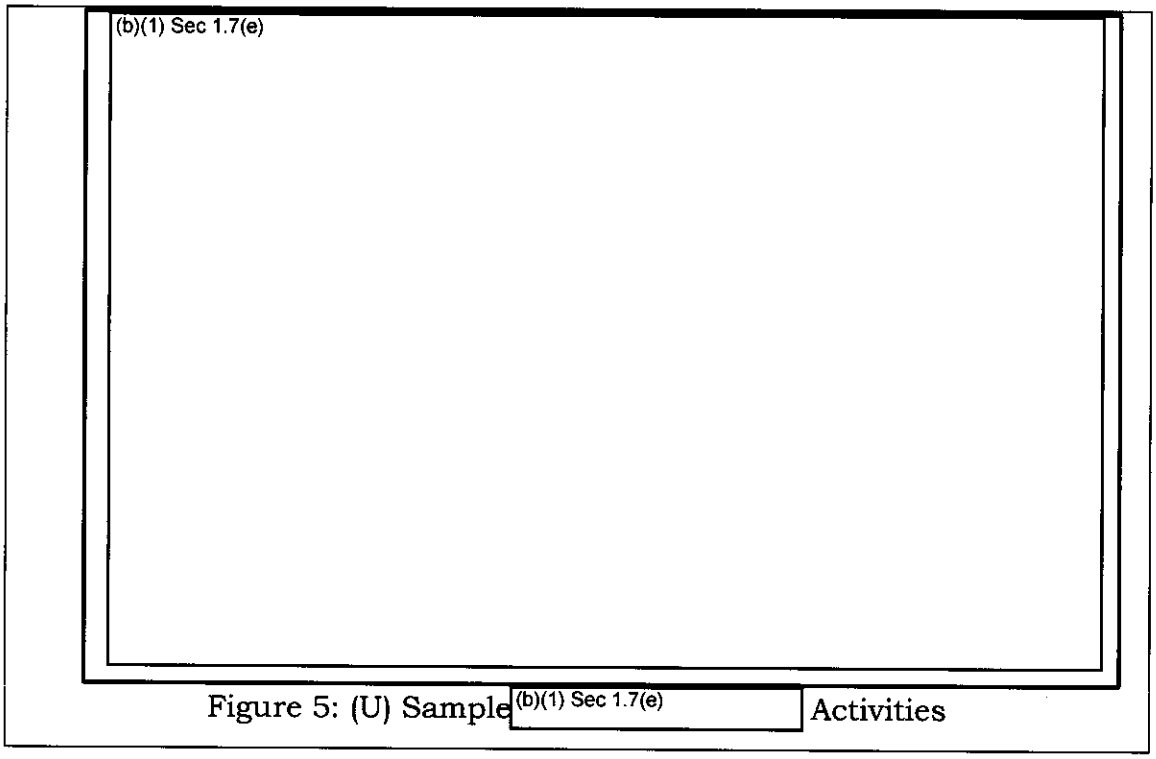


Figure 5: (U) Sample (b)(1) Sec 1.7(e) Activities

(d) (U) (b)(1) Sec 1.7(e) in support of operations in and through cyberspace includes (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) including other aspects of IO. See Figure 6 below for sample (b)(1) Sec 1.7(e) to Appendix 3 (Information Operations) to Annex C (Operations) for additional discussion.

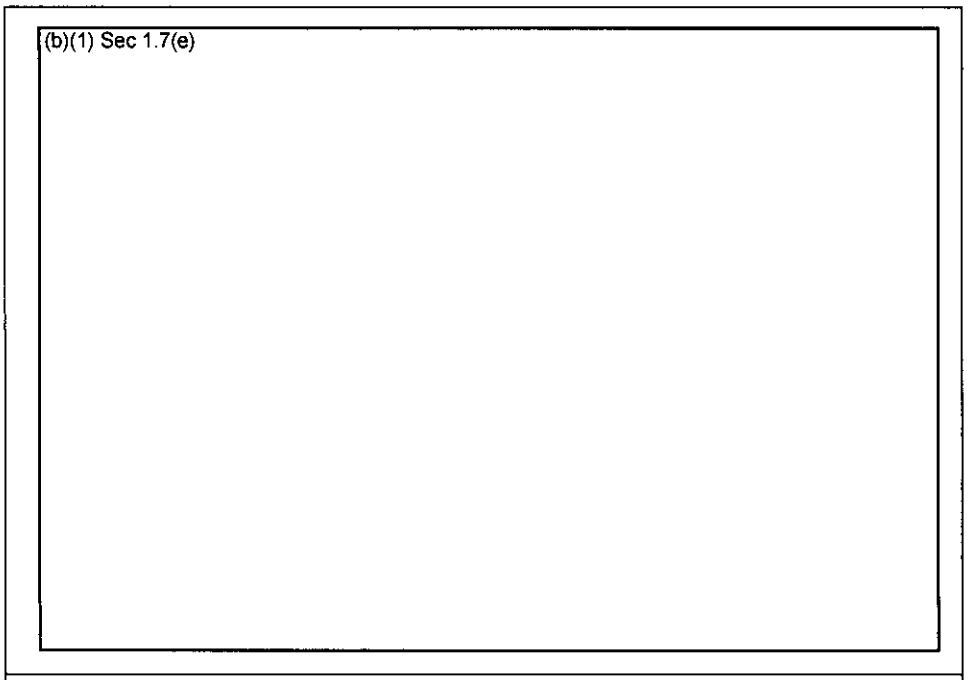


Figure 4: (U) Sample cyberspace activities supporting (b)(1) Sec 1.7(e)

153

154 (c) (U) (b)(1) Sec 1.7(e) can come from any
155 (b)(1) Sec 1.7(e)
156
157
158
159
160
161
162 (b)(1) Sec 1.7(e) to Appendix 3 (Information Operations) to Annex C
163 (Operations) for additional discussion.

164

3 as a construct for a notional adversary. This process should be followed (b)(1) Sec 1.7(e) designated in (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

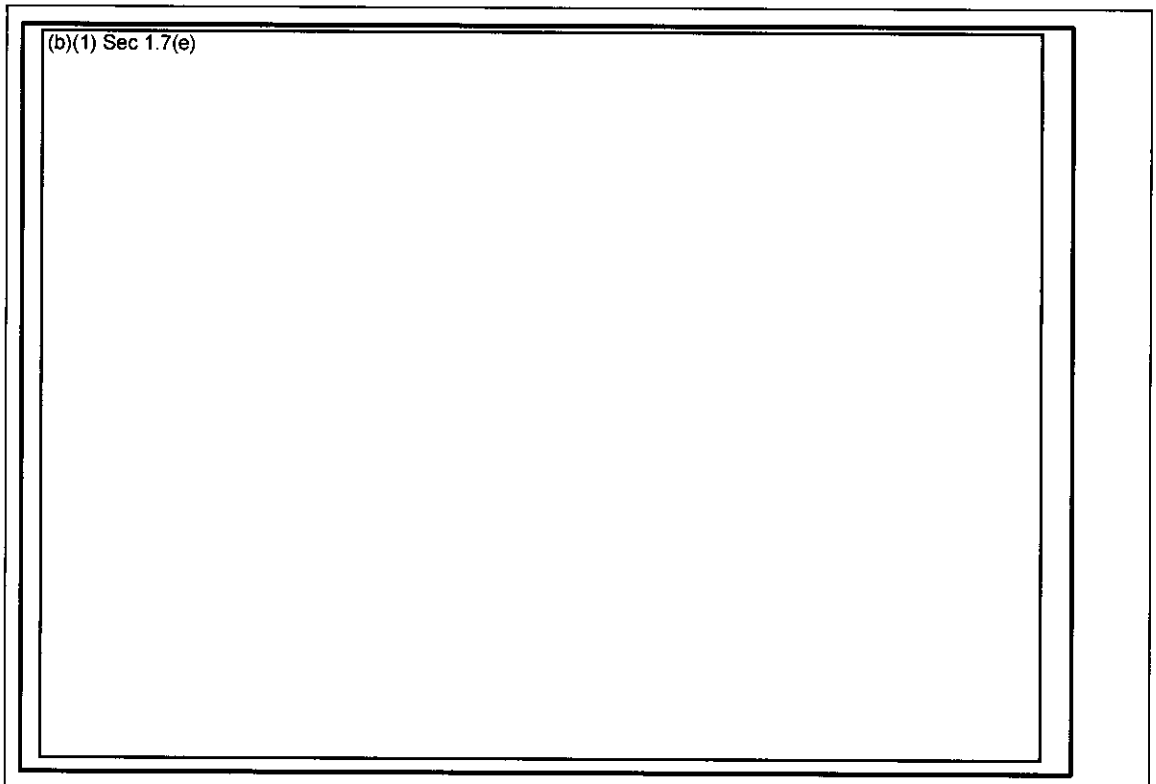


Figure 3: (U) Sample cyberspace activities supporting (b)(1) Sec 1.7(e)

(b). U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

other command plans as applicable. Consider Figure 4 as a construct where other commanders (or other USSTRATCOM plans) are supported.

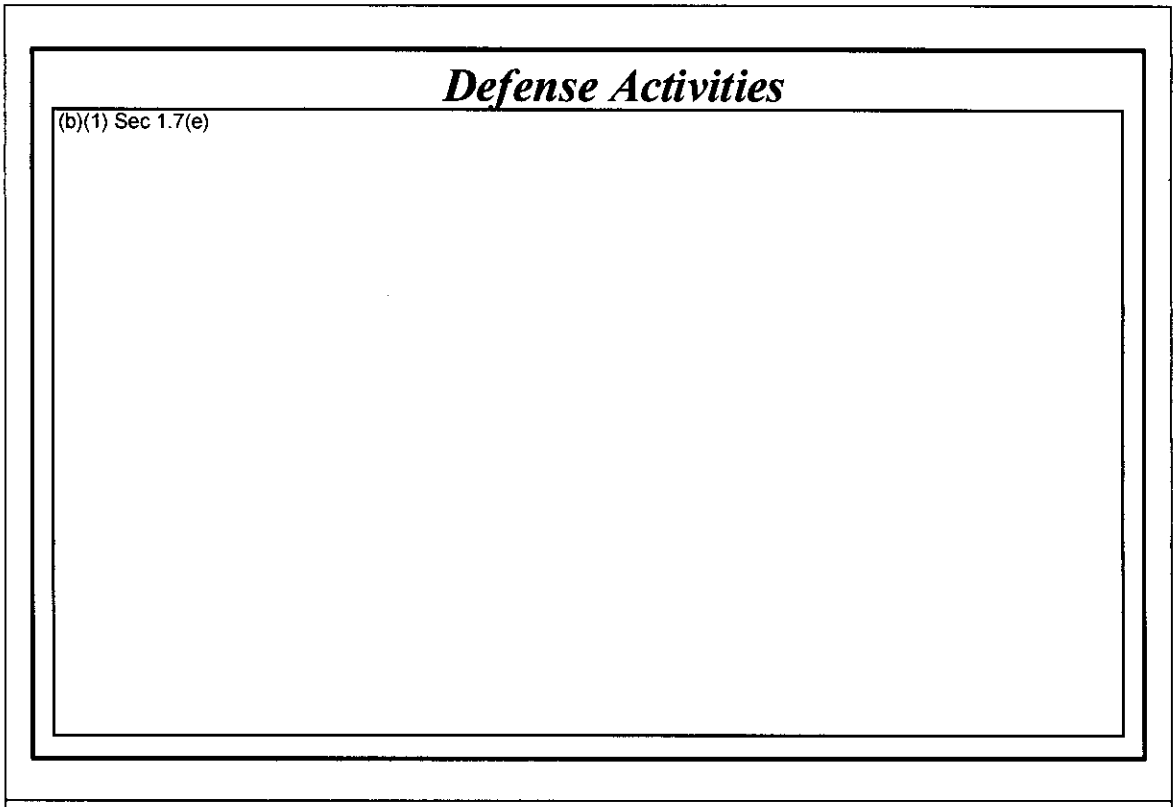


Figure 2: (U) Sample Defense Activities

(5) Offensive Operations in and through cyberspace. USSTRATCOM will provide a range of offensive capabilities in the cyberspace domain to achieve (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) can be supported by or in support of (b)(1) Sec 1.7(e) environments. Specific activities should be planned (b)(1) Sec 1.7(e) operations. See (b)(1) Sec 1.7(e) for (b)(1) Sec 1.7(e) see (b)(1) Sec 1.7(e) to Appendix 3 (Information Operations) to Annex C (Operations). For purposes of this CONPLAN, in accordance with (b)(1) Sec 1.7(e) are described as below in (b)(1) Sec 1.7(e)

(a) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) will be integrated across each of their military functions. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) Consider Figure

121

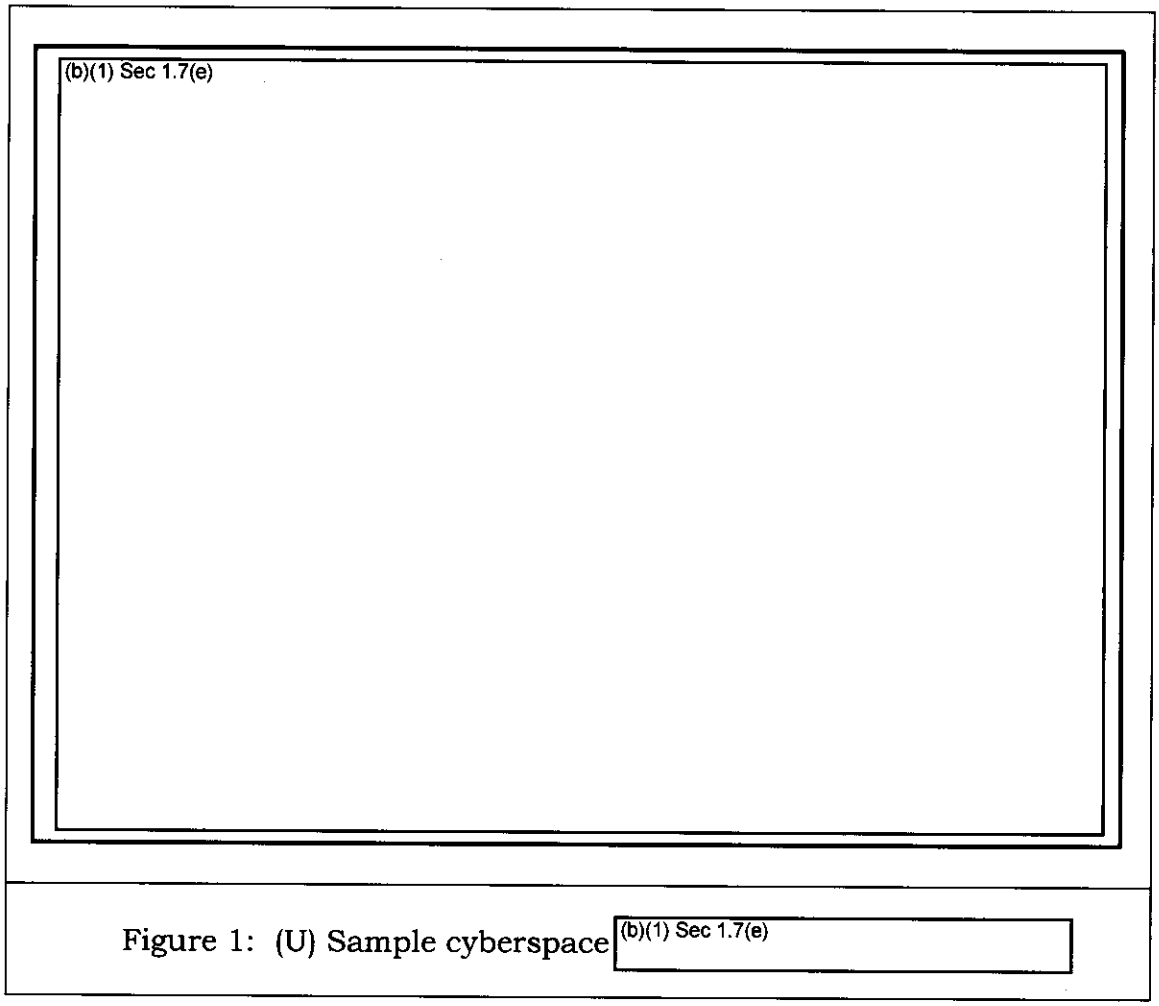


Figure 1: (U) Sample cyberspace (b)(1) Sec 1.7(e)

122

the effects that they could create across all sub-areas of cyberspace (A through E as outlined in Figure 1 of the Base Plan). USSTRATCOM will plan and conduct operations in cyberspace, to achieve CONPLAN 8039 objectives. The desired effects list found in paragraph 3b(3)(c)2d assist Combatant Commands in establishing a framework to (b)(1) Sec 1.7(e) with specific tasks that cyber forces will execute. The (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(3) (U) Offense Defense Mix. To achieve cyberspace superiority, forces require situational awareness, robust defense in depth of our cyberspace systems, the ability (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) commander's intent. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) These activities are not conducted (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) improve their defenses. Offensive and defensive capabilities will be merged in CONPLAN 8039 to establish cyberspace superiority at times and places critical to the accomplishment (b)(1) Sec 1.7(e)

(4) (U) Defensive Operations in cyberspace. CONPLAN 8039 describes cyberspace defense as those actions taken in cyberspace to protect, defend, monitor, analyze, detect and respond to unauthorized attacks against the DOD GIG, and as directed, other US cyberspace. For purposes of this CONPLAN, in accordance with (b)(1) Sec 1.4(a) guidance, defensive operations are described as below.

(a).(U//~~FOUO~~) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) cyberspace. (b)(1) Sec 1.7(e) planners will consider (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) Planners will also consider friendly (b)(1) Sec 1.7(e) cyberspace. Consider Figure 1 as a construct to ensure (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) This process of developing operations in and through cyberspace (b)(1) Sec 1.7(e) military functions should be followed for a (b)(1) Sec 1.7(e) designated in (b)(1) Sec 1.7(e) Figure 2 describes (b)(1) Sec 1.7(e)

obligations to which the US is a party, LOAC, customary international law, ROEs, and national policies.

2. (U) Mission. Refer to Base Plan.

3. (U) Execution

a. (~~S//REL USA, AUS, GBR~~) Conduct of Operations. Operations in and through cyberspace (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) CDRUSSTRATCOM will provide strategic direction to CC/S/As for (b)(1) Sec 1.4(a) in and through cyberspace. CDRUSSTRATCOM may establish a (b)(1) Sec 1.4(a) to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) USSTRATCOM's JFCC GSI, JFCC NW) and JTF GNO will coordinate all requests from CC/S/As, prioritize these requests and coordinate for support from the applicable CC/S/As as needed. US military operations in cyberspace will be conducted as necessary to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) when directed.

(1) (U) Commander's Intent. USSTRATCOM conducts operations in and through cyberspace by providing cyberspace effects under two scenarios:

(a) When CDRUSSTRATCOM is the supported commander for planning within the context of other STRATCOM plans (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) In this case, cyberspace effects will also (b)(1) Sec 1.7(e) Additionally, when supported, CDRUSSTRATCOM will provide cyberspace effects to (b)(1) Sec 1.7(e) cyberspace threats.

(b) When USSTRATCOM is a supporting commander for another combatant commander, effects and activities in support of other plans will be derived via the applicable combatant commander plan. For timing and tempo of operations, USSTRATCOM-assigned forces will follow the phasing or planned construct resident in that plan.

(2) (U) Priority Effects. Refer to the Base Plan. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) Therefore all operations in and through cyberspace must be considered for

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AFB NE 68113-6500
28 February 2008

ANNEX C TO USSTRATCOM CONPLAN 8039 (U)
(U) OPR: JFCC NW J5
OPERATIONS (U)

(U) References: Refer to Base Plan.

1. (U) Situation

a. (~~S//REL USA, AUS, GBR~~) General.

(1) (~~S//REL USA, AUS, GBR~~) CONPLAN 8039 describes the process for planning and (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) This annex discusses the concept of operations for (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) command relationships and military operations relative to CDRUSSTRATCOM mission to conduct DOD operations in and through cyberspace. This annex discusses (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Plans concerning (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) of this plan.

(2) (U) (b)(1) Sec 1.7(e) in cyberspace are currently centered on (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) However (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

b. (U) Area of Concern. See Base Plan.

c. (U) (b)(1) Sec 1.7(e) See Base Plan

d. (U) Adversary Capabilities. See Base Plan

e. (U) Friendly Force Capabilities. See Base Plan. .

(1) (U) Assumptions. See Base Plan.

(U) f. (~~C//REL~~) Legal Considerations. See Appendix 8 (Rules of Engagement). Legal review is required in the planning and execution of operations in and through cyberspace to ensure compliance with the US Constitution, applicable US statutes, international treaty/agreement

(INTENTIONALLY BLANK)

(2) (U) The USSTRATCOM/J3 approves requests and (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) as recommended by the USSTRATCOM/ J2.

(3) (U) The USSTRATCOM (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(4) (U) Components will secure and maintain (b)(1) Sec 1.7(e) identified in paragraph 1.

c. (U) Coordinating Instructions. DIRLAUTH is authorized between all coordinating units and the Headquarters USSTRATCOM staff.

4. (U) Administration and (b)(1) Sec 1.7(e) administrative processing of (b)(1) Sec 1.7(e)

a. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

b. (U) Administration. Administrative control (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) and proper reporting are vital parts of the process. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) is initially published for National-level consumption and archived at the (b)(1) Sec 1.7(e) Contents of the initial report consist of lead examiner, date of report, (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

5. (U) Command and Control. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) would notify their higher headquarters to inform them of (b)(1) Sec 1.7(e) They would then immediately implement (b)(1) Sec 1.7(e) and administrative procedures.

Kevin P. Chilton
General, USAF
COMMANDER

2. (U) Mission. Refer to Basic Plan.

3. (U) Execution

a. (U) Concept of Operations. Summarize the general concept governing (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) The following topics are covered specifically in Tabs to this Appendix.

(1) (~~S//REL USA, AUS, GBR~~) Upon execution of CONPLAN 8039, CDRUSSTRATCOM will (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) for USSTRATCOM. USSTRATCOM subordinate commanders will report the (b)(1) Sec 1.4(a) to USSTRATCOM/ J2 for (b)(1) Sec 1.4(a) USSTRATCOM/ J2 (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) to satisfy CDRUSSTRATCOM intelligence requirements.

(2) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) through (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) through legal channels.

(3) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) are of great value to USSTRATCOM's IO mission and force protection operations. In addition, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) may provide significant information for USSTRATCOM and President and Secretary of Defense. (b)(1) Sec 1.4(a)

b. (U) Tasks. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) List the assigned tasks to each element of the supported and supporting commands. At a minimum address tasks for J-2, J-3, (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) and component commands.

(1) (U) The USSTRATCOM/J2 is responsible for leadership, oversight, and policy of (b)(1) Sec 1.7(e) The USSTRATCOM/J2 prioritizes (b)(1) Sec 1.7(e) requirements, operationally controls the (b)(1) Sec 1.7(e) intelligence.

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AFB NE 68113-6500
26 February 2008

APPENDIX 9 TO ANNEX B TO CDRUSSTRATCOM CONPLAN 8039-07 (U)
(U) OPR: HQ USSTRATCOM J2
(b)(1) Sec 1.7(e) USSC (U)

(U) References:

a. (U) (b)(1) Sec 1.7(e) " 18 Sep 86, (C).

b. (U) (b)(1) Sec 1.7(e) " 30 Jun 97 (U).

c. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) " Aug 87 (U).

d. (U) Joint Pub 2-01, Intelligence Support to Joint Operations, 20 Nov 96, (U).

1. (~~S//REL USA, AUS, GBR~~) Situation. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) discovery. The information obtained assists in (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) They also provide key information for the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) It is therefore vital (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

a. (U) (b)(1) Sec 1.7(e) Refer to Annex B of the Base Plan (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

b. (~~S//REL USA, AUS, GBR~~) Friendly. USSTRATCOM/ J2 will provide guidance and support (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

c. (U) Assumptions. Some (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2032~~

(PAGE INTENTIONALLY LEFT BLANK)

(3) (U) USSTRATCOM Collection Managers can select alternate product delivery methods within (b)(1) Sec 1.7(e)

5. (U) Command and Control. Refer to Annex B (Intelligence)

Kevin P. Chilton
General, USAF
COMMANDER

(c) (U) Provide immediate information on and assessments (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(d) (U) Provide updates and status concerning changes that affect the (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) to facilitate the most responsive tasking of assets in support of Commander, USSTRATCOM.

(e) (U) (b)(1) Sec 1.7(e) support of USSTRATCOM collection requirements.

(3) (U) (b)(1) Sec 1.7(e) through the (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) USSTRATCOM standing requirements validated by (b)(1) Sec 1.7(e) Refer to reference b.

(4) (U) USSTRATCOM JFCC ISR. Ensure proper national-level coordination and approval of appropriate (b)(1) Sec 1.7(e) requirements in support of this CONPLAN.

(5) (U) USSTRATCOM (b)(1) Sec 1.7(e) Assist in monitoring the progress of (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) requirements and product reporting.

c. (U) Coordinating Instructions. Refer to references a through i.

4. (U) Administration and Logistics

a. (U) Logistics. Not applicable.

b. (U) Reporting

(1) (U) (b)(1) Sec 1.7(e) task appropriate processing and (b)(1) Sec 1.7(e) to satisfy validated USSTRATCOM requirements. This will be accomplished through (b)(1) Sec 1.7(e)

(2) ~~(S//REL USA, AUS, GBR)~~ (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) product format or posting location. Refer to references b and g.

(1) (U) Collection Management. USSTRATCOM/J2 will provide (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) support to HQs staff elements only. USSTRATCOM JFCCs, Centers, components, and subordinate commands will assume (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) functions for their organizations while keeping HQ informed. JFCC ISR will closely collaborate with USSTRATCOM/J2 to maintain awareness of requirements and to ensure synchronization with DOD ISR. Ultimately, reporting agencies will be responsible to the Command and its subordinate JFCCs.

(2) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) The DOD architecture for (b)(1) Sec 1.4(a) distributed throughout the DOD. (b)(1) Sec 1.4(a) support USSTRATCOM missions are executed by other organizations, to include (b)(1) Sec 1.4(a)

b. (U) Tasks

(1) (U) USSTRATCOM Collection Managers

(a) (U) USSTRATCOM/J23 Collection Managers submit (b)(1) Sec 1.7(e) requirements (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) Refer to reference c.

(b) (U) USSTRATCOM JFCCs, Centers, components and subordinate Command Collection Managers will also submit (b)(1) Sec 1.7(e) requirements through (b)(1) Sec 1.7(e) while keeping HQ informed. Refer to reference i.

(c) (U) Users without (b)(1) Sec 1.7(e) can submit requirements by e-mail, message, or telecom to (b)(1) Sec 1.7(e)

(2) (U) (b)(1) Sec 1.7(e)

(a) (U) Provide timely, responsive processing and validation of USSTRATCOM Commander's, (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) validation. (b)(1) Sec 1.7(e) execute requirements validation and tasking for time critical requirements and special circumstances after normal working hours and on weekends. Refer to reference e.

(b) (U) Provide status to USSTRATCOM/J23 Intelligence Capabilities Branch of all Commander, USSTRATCOM, (b)(1) Sec 1.7(e) requirements. Assist in the coordination of (b)(1) Sec 1.7(e) requirements with other Unified Commands, National Agencies, and Services. Refer to reference e.

collection requirements. NOTE: (b)(1) Sec 1.4(a) as outlined in reference b. and is not included in this appendix.

a. (U) (b)(1) Sec 1.7(e) Refer to Annex B (Intelligence)

b. (U) Friendly

(1) (U) (b)(1) Sec 1.7(e) is responsible for (b)(1) Sec 1.7(e) balancing competing priorities of military and national needs as detailed in reference b.

(2) (U) (b)(1) Sec 1.7(e) and prioritizes collection requirements in line with the (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(3) (U) (b)(1) Sec 1.7(e) will provide timely/responsive processing and validation of Commander, USSTRATCOM, (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) Combatant Command intelligence requirements. (b)(1) Sec 1.7(e) requirements to the (b)(1) Sec 1.7(e) for validation. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(4) (U) (b)(1) Sec 1.7(e) provide Commander, USSTRATCOM, and the Commanders of JFCCs with (b)(1) Sec 1.7(e) consultation, and support in planning activities.

(5) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) will conduct the (b)(1) Sec 1.7(e) support mission and provide (b)(1) Sec 1.7(e)

c. (U) Assumptions. Refer to Base Plan.

2. (U) Mission. Refer to Base Plan.

3. (U) Execution. Refer to Annex B (Intelligence)

a. (U) Concept of Operations

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AFB NE 68113-6500
26 February 2008

APPENDIX 8 TO ANNEX B TO CDRUSSTRATCOM CONPLAN 8039 (U)
(U) OPR: HQ USSTRATCOM/J2
(b)(1) Sec 1.7(e) (U)

(U) References:

a. (U) Intelligence Community Directive-1, Policy Directive for Intelligence Community Leadership, 1 May 2006 (U).

b. (U) (b)(1) Sec 1.7(e) 22 Jul 05 (S//TK).

c. (U) (b)(1) Sec 1.7(e) (TS//SCI).

d. (U) (b)(1) Sec 1.7(e) 18 February 1997 (U).

e. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) 9 Feb 93 (U).

f. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) 1 December 2005 (U).

g. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) 9 June 2006 (S).

h. (U) D-R-A-F-T Department of Defense Directive, SUBJECT: (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) within the Department of Defense, Apr 05 (U).

i. (U) Implementation Directive: Joint Functional Component for Intelligence, Surveillance, and Reconnaissance (JFCC ISR), 24 Jan 2005 (U).

1. (~~S//REL USA, AUS, GBR~~) Situation. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Given the current intelligence tasks in the (b)(1) Sec 1.4(a) to the overall plan. As such, this appendix provides a general overview of the (b)(1) Sec 1.4(a) organization, general responsibilities, and procedures for (b)(1) Sec 1.4(a)

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2032~~

(3) (U) USSTRATCOM JFCC ISR. Ensure proper national-level coordination and approval of appropriate (b)(1) Sec 1.7(e) support of this CONPLAN.

c. (U) Coordinating Instructions. Refer to references.

4. (U) Administration and Logistics

a. (U) Logistics. Not applicable.

b. (U) Reporting

(1) (U) Originating Collection Management office will task appropriate processing and (b)(1) Sec 1.7(e) to satisfy validated USSTRATCOM requirements. (b)(1) Sec 1.7(e)

(2) (S//REL) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

5. (U) Command and Control. Refer to Annex B (Intelligence).

a. Command Relationships. Refer to Annex B (Intelligence).

b. Communications. Refer to Annex B (Intelligence).

Kevin P. Chilton
General, USAF
COMMANDER

USSTRATCOM missions are or may be executed by, but not limited to, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

b. (U) Tasks

(1) (U) USSTRATCOM Collection Managers

(a) (U) USSTRATCOM/J2 Collection Managers submit (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) JWICS (ref c).

(b) (U) USSTRATCOM JFCCs, Centers, components, and subordinate command Collection Managers will also submit (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) while keeping HQ informed (ref i).

(c) (U) Users without (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) e-mail, message, or telecom to USSTRATCOM/J2 Collection Managers.

(2) (U) (b)(1) Sec 1.7(e)

(a) (U) Provide timely, responsive review and validation of USSTRATCOM (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(b) (U) Provide status to USSTRATCOM/J2 of all Command (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(c) (U) Provide immediate information on and assessments of events that impact collection management tools, communications and dissemination systems, databases, collection sensor and systems, processing, and other support functions.

(d) (U) Provide updates and status concerning changes that affect the execution of collection management functions. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) to facilitate the most responsive tasking of assets in support of the Commander, USSTRATCOM.

(e) (U) (b)(1) Sec 1.7(e) assets in support of USSTRATCOM collection requirements.

(b)(1) Sec 1.4(a)

a. (U) (b)(1) Sec 1.7(e) Refer to Annex B (Intelligence).

b. (U) Friendly

(1) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(2) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

c. (U) Assumptions. Refer to Base Plan.

2. (U) Mission. Refer to Base Plan.

3. (U) Execution. Refer to Annex B (Intelligence).

a. (U) Concept of Operations for (b)(1) Sec 1.7(e) Production

(1) (U) Collection Management. USSTRATCOM/J2 Intelligence Capabilities Branch will provide (b)(1) Sec 1.7(e) support to HQs staff elements only. USSTRATCOM JFCCs, Centers, components, and subordinate commands will assume (b)(1) Sec 1.7(e) for their organizations while keeping HQ informed. JFCC ISR will closely collaborate with USSTRATCOM/J2 to maintain awareness of requirements and ensure synchronization with DOD ISR. Ultimately, reporting agencies will be responsible to both the Command and its subordinate JFCCs.

(2) (~~S//REL~~) (b)(1) Sec 1.4(a) The DOD architecture for (b)(1) Sec 1.4(a) distributed throughout the DOD. (b)(1) Sec 1.4(a) required to support

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AFB NE 68113-6500
28 February 2008

APPENDIX 7 TO ANNEX B TO CDRUSSTRATCOM CONPLAN 8039 (U)
(U) OPR: HQ USSTRATCOM J2
(b)(1) Sec 1.7(e) (U)

(U) References:

a. (U) Joint Pub 2-01, Joint and National Intelligence Support to Military Operations, 7 October 2004 (U)."

b. (U) Chairman of the Joint Chiefs of Staff Instruction (CJCSI), (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) 28 January 2000 (TS).

c. (U) (b)(1) Sec 1.7(e) 18 February 1997 (U).

d. (U) (b)(1) Sec 1.7(e) 10 November 1996 (U)."

e. (U) (b)(1) Sec 1.7(e) 22 March 2007 (U)."

f (U) (b)(1) Sec 1.7(e)

1. (~~S//REL~~) Situation. Given the current intelligence tasks in the CONPLAN, (b)(1) Sec 1.4(a)

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2032~~

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE, NE 68113-6500
26 February 2008

ANNEX J TO COMMANDER USSTRATCOM CONPLAN 8039 (U)
(U) OPR: HQUSSTRATCOM/J53
COMMAND RELATIONSHIPS (U)

References:

a. (U) Unified Command Plan (UCP), 5 May 06 (U//FOUO)

b. (U) (b)(1) Sec 1.7(e) 1 Sep 06 (TS)

c. (U) Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 12 April 2001 (As Amended Through 20 March 2006) (U)

d. (U) Joint Pub 1, Doctrine for the Armed Forces of the United States, 14 May 2007 (U)

e. (U) Delegation of Disclosure Authority Letter, National Disclosure Policy Committee Case No. 6005-00 – Multiple Countries, 7 Jun 00 (S)

f. (U) Memorandum of Arrangement between The Department of Defence of Australia, The Ministry of Defence of The United Kingdom of Great Britain and Northern Ireland, and The Department Of Defense of The United States of America on Information Operations Data Exchange, 6 May 03 (U)

g. (U) 2004 National Response Plan (NRP), Cyber Annex, Dec 04 (U)

h. (U) Trilateral Memorandum of Agreement among the Department of Defense, the Justice Department and the Intelligence Community Regarding (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) 9 May 07 (S//NFS//NF)

1. (U) General

a. (U) Operational Area(s). Refer to Base Plan para 1.b.

b. (U) Scope. This Annex defines the command and cooperative relationships between USSTRATCOM, DOD organizations, non-DOD USG agencies, and civilian entities as they pertain to cyberspace operations.

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2033~~

2. (~~S//REL USA, AUS, GBR~~) Mission. CDRUSSTRATCOM plans and directs integrated DOD cyber operations (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) defend the DOD networks from aggression, and as directed, use cyberspace to advance and defend US interests.

3. (U) Execution. CDRUSSTRATCOM will plan and carry out the strategic, global cyberspace missions for DOD. CDRUSSTRATCOM will be designated as the supported commander by the POTUS or SECDEF, and CJCS for strategic, global Cyberspace Operations (CO) and as a supporting commander for geographic regional CO. As the DOD military lead for CO, CDRUSSTRATCOM serves as a conduit to the C/S/As for operational policy issues and mission operations.

a. (U) CDRUSSTRATCOM Responsibilities

(1) (U) Coordinate through the USSTRATCOM Director, Global Operations/J3 all CO support requested by C/S/As.

(a) (U) Act as C/S/A's primary contact for cyber support through the USSTRATCOM/J3 via the Global Operations Center (GOC). C/S/As can also request cyber support through any STRATCOM component. Such requests will in turn be forwarded to the GOC for internal coordination/action.

(b) (U) Designate the USSTRATCOM Director, Plans and Policy/J5 as the staff element responsible for consolidating, prioritizing, deconflicting and assigning USSTRATCOM Cyberspace resources based on commander's guidance.

(c) (U) Retain Administrative Control (ADCON) authority of the deployed USSTRATCOM CO components (teams consisting of HQ USSTRATCOM, JFCC NW, JTF GNO, and JIOWC personnel, depending on mission requirements) as appropriate.

(2) (U) Exercise Coordinating Authority (CA) with C/S/As, as defined by reference (d) above.

(3) (U) Develop relationships with the C/S/As and external organizations that will maintain and augment existing HQ USSTRATCOM, JTF GNO, JFCC NW, JFCC GSI, JFCC SPACE, and JIOWC relationships.

(4) (U) Coordinate (b)(1) Sec 1.7(e) as appropriate.

(5) (U) Evaluate, select/pursue cyber threats, plan, and prioritize the desired effects necessary to achieve the appropriate combination of the plan's (b)(1) Sec 1.7(e) based on the scenario.

b. (U) USSTRATCOM Components

(1) (U) Lead Component and assignment of forces.

(U)(a) CDRUSSTRATCOM designates JTF GNO as the lead component to operate and defend the DOD GIG. All other USSTRATCOM components are assigned in a supporting role for the operation and defense of the DOD GIG.

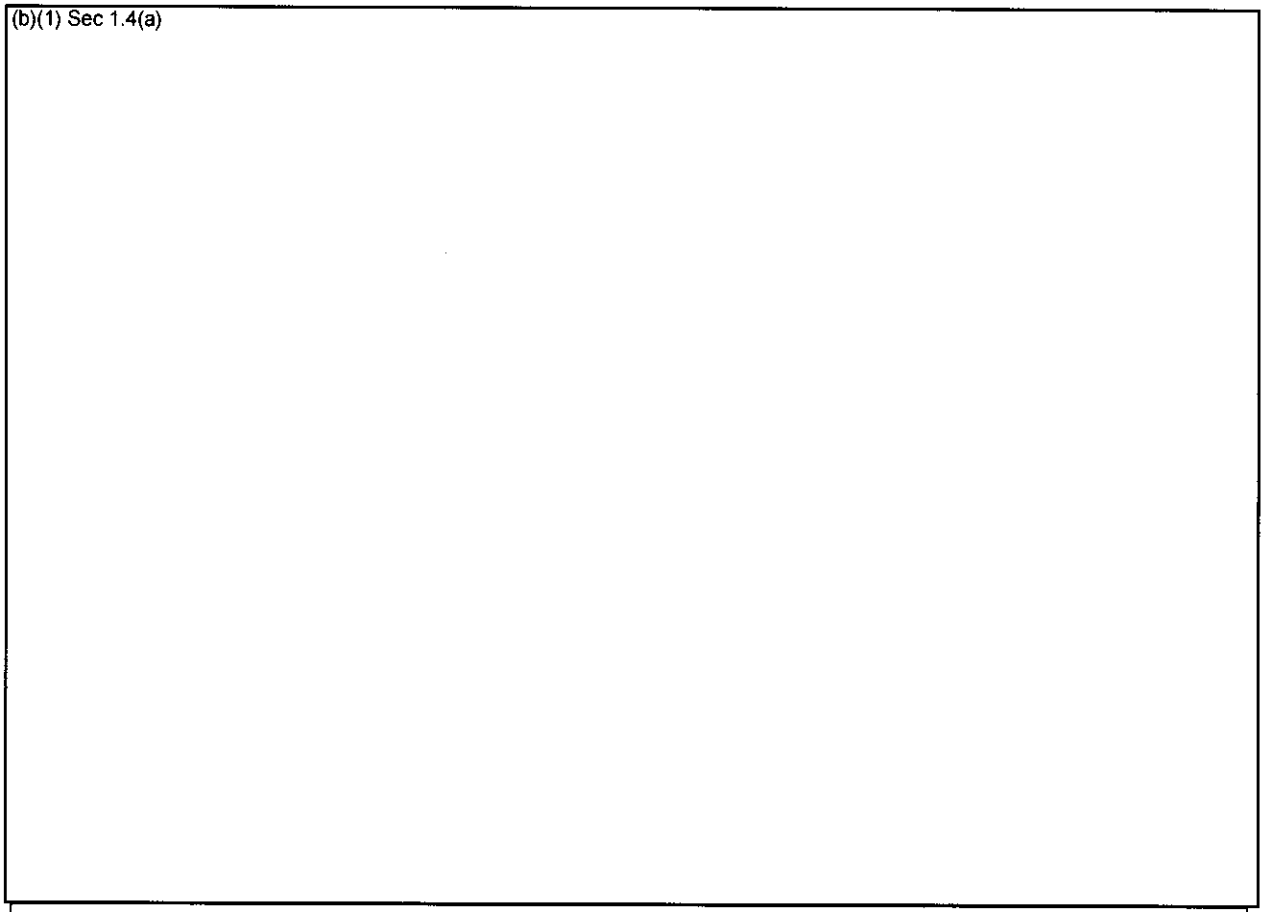
(b) (~~S//REL USA, AUS, GBR~~) CDRUSSTRATCOM will conduct military operations in cyberspace as either the supported or supporting commander. CONPLAN 8039 will provide the methodology for determining (b)(1) Sec 1.4(a) CDRUSSSTRATCOM will designate a lead component and assign forces for execution of specified cyberspace missions based upon the nature of the crisis/contingency. The lead component has the responsibility to integrate offensive and defensive activities (see Figure 1). For timing and tempo of operations, USSTRATCOM assigned cyber forces will (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) The USSTRATCOM designated lead component:

1 (~~S//REL USA, AUS, GBR~~) Will be delegated (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) day-to-day management of assigned cyberspace forces in executing the assigned mission, as appropriate.

(U)2 (~~S//REL USA, AUS, GBR~~) Will support theater operations as directed by CDRUSSTRATCOM.

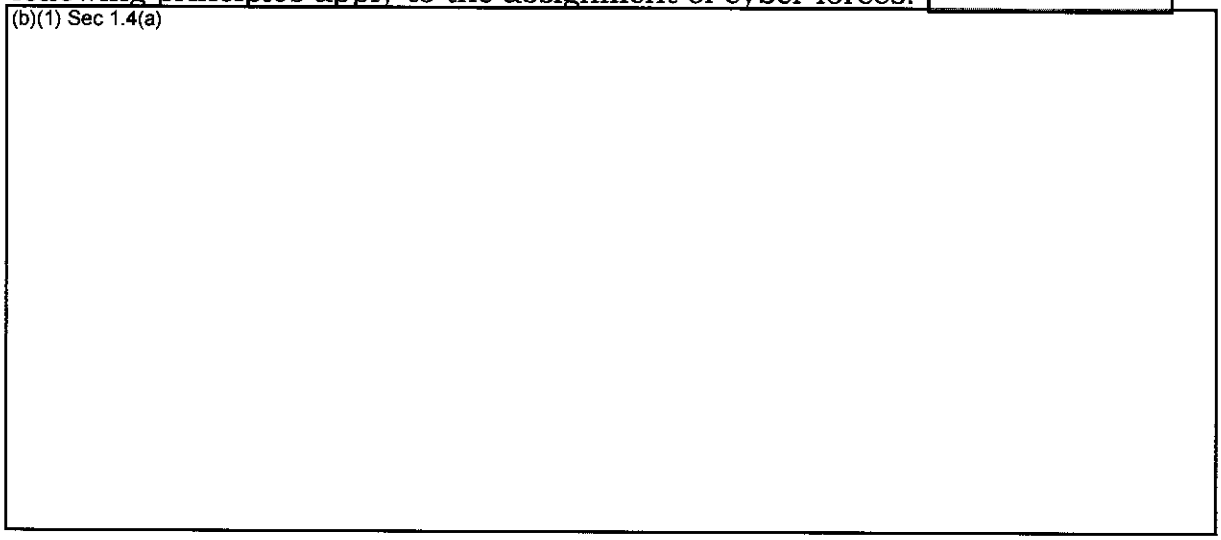
(U)3 (~~S//REL USA, AUS, GBR~~) Will collaborate and coordinate across the USSTRATCOM staff, Service component staffs assigned to USSTRATCOM and their respective operations centers, Combatant Commanders, and other DOD and non-DOD partners to ensure unity of effort in support of military and other national security operations.

4 (~~S//REL USA, AUS, GBR~~) Will request to establish (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) to plan, synchronize, collaborate and deconflict operations.



(U) Figure 1 Command Structure (S//REL USA, AUS, GBR)

(c) (~~S//REL USA, AUS, GBR~~) Assignment of forces. In general, the following principles apply to the assignment of cyber forces: (b)(1) Sec 1.4(a)



(2) (U) USSTRATCOM Components and Service Components

(a) (U) USSTRATCOM Components

1 (U//~~FOUO~~) JTF GNO. As directed by CDRUSSTRATCOM, JTF GNO supports the USSTRATCOM-assigned Unified Command Plan (UCP) mission of global network operations. The UCP 2006 states that USSTRATCOM shall be responsible for planning, integrating, and coordinating DOD global network operations by directing GIG operations and defense and identifying and advocating these desired characteristics and capabilities. CDRUSSTRATCOM, through CDR, JTF GNO, provides the DOD with the direction and oversight to operate and defend the GIG and accommodate interfaces to coalition, allied and non-DOD users and systems. CDR, JTF GNO reports directly to CDRUSSTRATCOM and exercises TACON / OPCON of assigned forces. JTF GNO, upon implementation of CONPLAN 8039 and on behalf of CDRUSSTRATCOM, will assume TACON of assigned defensive CO forces. Commander JTF GNO executes NetOps via assigned forces. As required to fulfill mission requirements, CDR JTF-GNO has authority for direct liaison (DIRLAUTH) with other DOD components to include C/S/As to exchange information germane to cyberspace activities and promote situational awareness relative to hostile acts directed toward DOD networks. The following specific authorities are granted to CDR, JTF GNO:

a (U//~~FOUO~~) CA for the planning and execution of the GIG NetOps mission.

b (U//~~FOUO~~) OPCON or TACON of assigned NetOps and CND forces, as directed.

c (U//~~FOUO~~) Direct Liaison Authorized (DIRLAUTH) between JTF GNO and the following: USSTRATCOM functional components, Service components, subordinate organizations, Combat Commands, and communities of interest; USSTRATCOM will be kept informed. CDR, JTF GNO, is encouraged, consistent with DOD rules and regulations, to develop robust coordinating relationships for information sharing to include: non-DOD US government organizations, intergovernmental organizations, nongovernmental organizations, multinational military commands (alliances and coalitions), state and local governments, commercial and research communities.

2 (U) JFCC NW. On a daily basis, JFCC NW will conduct operational and tactical level planning and day-to-day employment of assigned and attached forces, integration of (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) effects or that directly support national objectives in and through cyberspace. This includes (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) in support of other Combatant Commanders, as directed. At a minimum, the JFCC NW is required to:

a (U) Synchronize all capabilities for operations in and through cyberspace with the JTF GNO, JIOWC, and other JFCCs, as necessary. Assume OPCON or TACON, where applicable, of cyber forces for day-to-day and crisis operations.

b (U) Develop recommendations to alleviate, from a global perspective, operational resource conflicts for operations capabilities of cyber forces.

c (U) Develop Course of Action (COA) recommendations for operations in and through cyberspace in support of USSTRATCOM and national strategic objectives. Support JFCC GSI for the integration of operations in and through cyberspace into USSTRATCOM global strike COAs. Provide an embedded capability in the Global Operations Center (GOC) to support JFCC GSI mission of operational level integration of USSTRATCOM missions and maintaining situational awareness for the commander.

d (U) Coordinate and maintain tactical level intelligence, as necessary, to support components of operations in and through cyberspace. Provide all (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

e (U) Establish a relationship with mission area experts in the applicable regional commander's Standing Joint Force Headquarters (SJFHQ) to provide operational support for NW capabilities. This relationship will include the training and periodic qualification of NW support in SJFHQs, as required.

f (U) Provide support for headquarters USSTRATCOM and other geographic and functional Combatant Commanders exercise, wargames, and experimentation requirements. Integrate and synchronize efforts with USSTRATCOM Training and Exercise Division (J37). Support headquarters development of military utility assessments, research and development efforts, and advocacy of capability needs for the Joint Capabilities Integration Development System (JCIDS) process.

g (U) Report operational readiness assessment of assigned mission areas, as directed by headquarters.

h (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) CDR USSTRATCOM or the requesting CCDR.

(1) (~~S//REL USA, AUS, GBR~~) Authority necessary to
(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(2) (~~S//REL USA, AUS, GBR~~) The following are (b)(1) Sec 1.4(a) operations (see Table 4). Subject (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

Table 1 (b)(1) Sec 1.4(a) (S//REL USA, AUS, GBR)

(a) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(1) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(2) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(3) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) computers, networks, information and information systems is authorized only for the purpose of conducting an approved operation as defined in this plan. (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(4) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(5) (~~S//REL USA, AUS, GBR~~) Supported JFC notification is required for (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) CDRUSSTRATCOM may delegate this authority to the CDR JFCC NW when acting as supported commander. (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(6) (~~S//REL USA, AUS, GBR~~) Supported JFC approval is required for (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) CDRUSSTRATCOM may delegate this authority to the CDR JFCC NW when acting as supported commander, which may be further delegated to a General Officer/Flag Officer within JFCC NW. (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(7) (~~S//REL USA, AUS, GBR~~) All formal requests for approval (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

i (U) The CDR JFCC NW is assigned the following authorities:

(1) (U) CA for the planning and execution of the CO mission.

(2) (U) OPCON or TACON of assigned cyberspace forces, as directed by headquarters.

(3) (U) DIRLAUTH between JFCC NW and other joint and Service components, Combatant Commanders, and DOD agencies, while keeping headquarters informed. JFCC Commanders are encouraged, consistent with DOD rules and regulations, to develop the robust coordinating relationships, to include inter-agency and combined forces where required, to enhance the mission effectiveness of operations in and through cyberspace.

3 (U//~~FOUO~~) JFCC GSI. JFCC GSI will act as the overall lead USSTRATCOM component in direct support of the CDRUSSTRATCOM to develop integrated crisis response COAs, provide integrated analysis of the Command's global mission capabilities, provide execution recommendations for supported and supporting mission tasks, execute global strike missions when directed, and, through a JFCC GSI managed GOC that integrates inputs of all components and Service task forces, provide the headquarters with situational awareness for all operational responsibilities. Provide continuous situational awareness of assigned forces engaged in ongoing global strike operations. Provide coordinated tasking from the headquarters to other joint components and Service task forces, as necessary, for the synchronization of all USSTRATCOM operational and tactical mission planning and execution needs IAW USTRATCOM HC2I CONOPS. At a minimum, the JFCC GSI is required to:

a (U//~~FOUO~~) In accordance with USSTRATCOM's Intelligence Integration CONOPS, coordinate with the (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) global strike intelligence requirements.

b (U//~~FOUO~~) Support USSTRATCOM led efforts to create and maintain strategic-level OPLANs. Support development and coordination of OPLANs and CONPLANs, as directed by headquarters. Support other Combatant Commands with global strike operational planning and execution, as directed by headquarters.

c (U//~~FOUO~~) Assume OPCON or TACON of (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) as directed.

d (U//~~FOUO~~) Support HQ coordination with geographic and functional Combatant Commanders to support ongoing and future operational requirements for USSTRATCOM global strike capabilities.

e (U//~~FOUO~~) Provide support for HQ USSTRATCOM and other geographic and functional Combatant Commanders' exercise, war game and experimentation requirements. Integrate and synchronize efforts with USSTRATCOM Training and Exercise Directorate (J7).

f (U//~~FOUO~~) Support headquarters development of global strike mission research and development and advocacy of capability needs for the Joint Capabilities Integration and Development System (JCIDS) process.

g (U//~~FOUO~~) Be the central manager of the (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) capability.

h (U//~~FOUO~~) Manage the GOC.

i (U//~~FOUO~~) Chair the Information Operations Working Group (IOWG).

j (U//~~FOUO~~) Manage the Joint Integration Working Group (JIWG).

k (U//~~FOUO~~) Manage the Joint Planning Working Group (JPWG).

4 (U) JIOWC. JIOWC is responsible for planning, integrating and coordinating the IO core capabilities of (b)(1) Sec 1.7(e) OPSEC and (b)(1) Sec 1.7(e) and (b)(1) Sec 1.7(e) in support of JFCs. JIOWC is also the USSTRATCOM lead for strengthening IO capabilities across the DOD and is responsible for supporting the SC planning efforts of STRATCOM missions and JFCs when requested. At a minimum, the JIOWC is required to:

a (U) Enable JFCs to plan and execute IO, (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) OPSEC, (b)(1) Sec 1.7(e) and CNO.

b (U) Interface with the Joint Staff, Military Services, DOD and non-DOD agencies to coordinate and integrate IO efforts for joint commanders.

c (U) Participate in (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) support to Combatant Commanders.

d (U) Provide assistance to JFC IO intelligence support efforts.

e (U) Evaluate IO effectiveness in military operations.

f (U) Provide Joint IO wargaming simulations to support joint exercises and experimentation.

g (U) Assist with strategic IO planning and theater engagement.

h (U) The Commander, JIOWC will deploy task organized IO support teams to assist C/S/As as directed by CDRUSSTRATCOM.

i (U) Upon SecDef approval, the Chief, JIOWC Combatant Commander Support Team will fall under OPCON authority of the supported commander.

5 (U) JFCC SPACE. JFCC SPACE will optimize planning, execution, and force management of the assigned missions and to coordinate space operations. JFCC SPACE supports CDRUSSTRATCOM in the conduct of space operations and exercises OPCON of designated space and missile-warning forces on behalf of CDRUSSTRATCOM. CDR JFCC SPACE is designated as the Global Space Coordinating Authority (GSCA) and the lead USSTRATCOM component for execution of Defensive Space Control (DSC) which includes the satellite Telemetry, Tracking & Control (TTC)-portion of cyberspace.

6 (U) JFCC IMD. JFCC IMD serves as the CA on behalf of CDRUSSTRATCOM for planning and execution of the IMD mission. JFCC IMD develops and coordinates IMD concepts of operations and supporting operational plans, to include OPLANs, CONPLANs, FUNCPLANs, and SUPPLANs, as directed by HQ USSTRATCOM. JFCC IMD assumes OPCON or TACON control, as directed, of designated IMD capabilities for day-to-day and crisis operations. JFCC IMD provides day-to-day and crisis operational support to missile defense components. JFCC IMD provides an embedded capability in the GOC to support the JFCC GSI tasks of operational level integration of USSTRATCOM missions and maintaining situational awareness for the commander.

7 (U) JFCC ISR. JFCC ISR conducts planning to employ DOD ISR resources to meet Combatant Commander, national, and departmental requirements. (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
the Joint Staff, U.S. Joint Forces Command (USJFCOM), Combatant Commanders, the military Services, and other mission partners, JFCC ISR ensures the integration of DOD and national ISR efforts to satisfy Combatant Commander and national operational and intelligence requirements. JFCC ISR planning synchronizes the use of national, DOD, and, when feasible, Allied/Coalition ISR capabilities with employment of theater ISR resources.

(b) (U) USSTRATCOM Service Components

1 (~~S//REL USA, AUS, GBR~~) U.S. Army Forces. USSTRATCOM has COCOM of SMDC/ARSTRAT. (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2 (U) U.S. Naval Forces.

a. The Navy (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) Navy forces certified for network defense are embedded in the parent force structure of all Navy component commanders assigned by their respective commanders with assignment of additional forces via Naval Component Task Force-ND (NCTF-ND) as required. JTF GNO has TACON authority of the NCTF-ND (for cyber defense only). The Navy Global Operations and Security Center (NAVGNOSC) is OPCON to JTF GNO. In response to network events or activities, as determined by CDR USSTRATCOM or CDR JTF GNO, the Navy Cyber Defense Operations Command (NCDOC) shall instantaneously be attached to CDR JTF GNO, who will exercise TACON upon contact with the NCDOC until such time that the responses to the events or activities are declared complete by CDR JTF GNO, at which time the Navy will resume control of the NCDOC. (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) When directed

by a Joint Staff deployment order, (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
CDRUSSTRATCOM is designated the supported commander.

b. The Marine Corps (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) Marine forces certified for network defense are embedded in the parent force structure of all Marine component commanders with assignment of additional forces via as required. The Marine Corps Network Operations and Security Center (MCNOSC) is OPCON to JTF GNO for CND. Assignment of other Marine forces will be coordinated through MARFORSTRAT.

3 (~~S//REL USA, AUS, GBR~~) U.S. Air Force Forces.
USSTRATCOM has COCOM of 8 AF (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

c. (U) (b)(1) Sec 1.7(e)

(1) (C//REL) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(2) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
protection (See Base Plan) up to the Top Secret level for the goal of

strengthening information networks; to improve the confidentiality, integrity and availability of information systems; and improve the prediction, detection and response capabilities. USSTRATCOM/J51 is designated as the United States National Lead; JTF GNO is responsible for the operational mission.

d. (U) Alternate Procedures (Succession to Command)

(a) (U) When the position of the combatant commander is vacant, or in the temporary absence or disability of the combatant commander, the deputy commander acts as the combatant commander and performs the duties of the combatant commander until a successor is appointed or the absence or disability ceases. If a deputy commander has not been designated, or is also temporarily absent or disabled, interim command shall pass to the next senior officer present for duty eligible to exercise command, regardless of Service affiliation.

(c) (U) In the event JTF GNO cannot execute command of JTF GNO due to lack of communications or other reasons, succession of command is Deputy JTF GNO, Commander Marine Forces (COMMARFOR), Commander Air Force Forces (COMAFFOR), Commander Global Network Operations and Security Center (CDR GNOSC), Naval Network Warfare Command (NAVNETWARCOM) and Commander Army Forces (COMARFOR).

(b) (U) In the event CDR JFCC NW cannot execute command of JFCC NW due to lack of communications or other reasons, succession of command is Deputy JFCC NW.

(d) (U) In the event CDR JIOWC cannot execute command of JIOWC due to lack of communications or other reasons, succession of command is Deputy JIOWC.

4. (U) Support and Coordination Relationships

(U) a. (~~S//REL USA, AUS, GBR~~) Supporting Military Forces

(1) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) USSTRATCOM or the supported regional commander.

(2) (U) USSTRATCOM Combatant Commander Liaison. USSTRATCOM Liaison Officers (LNOs) will assist COCOM's in coordinating USSTRATCOM cyberspace activities within specific geographic AORs.

(a) (U) All cyber forces supporting a CDR USSTRATCOM mission will immediately establish liaison with the USSTRATCOM LNO when arriving in a commander's theater.

(b) (U) USSTRATCOM regional LNOs will assist coordination of USSTRATCOM CO activities between USSTRATCOM and the GCCs.

b. Coordinating Authorities (Integration)

(1) (U) JFCC GSI

(U) (a) (~~S//REL USA, AUS, GBR~~) Coordinate requirements of the lead Component for non-routine/-daily activities, functions and objectives.

(b) (~~S//REL USA, AUS, GBR~~) In coordination w/ JTF GNO, JFCC NW, JIOWC & JFCC SPACE, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) DOD cyberspace.

(c) (~~S//REL USA, AUS, GBR~~) Assist JIOWC in the development of (b)(1) Sec 1.4(a) operations in and through cyberspace.

(d) (~~S//REL USA, AUS, GBR~~) In coordination with JTF GNO, JFCC NW, JIOWC and JFCC SPACE, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) to facilitate USSTRATCOM cyber execution when in the supporting role.

(U) (e) (~~S//REL USA, AUS, GBR~~) Provide initial assessments of operations, lessons learned, shortfalls and additional requirements or authorities as required.

(U)(2) (~~S//REL USA, AUS, GBR~~) HQUSSTRATCOM/J3. Assist in the coordination and deconfliction with GCCs in support of CONPLAN 8039, Cyberspace Operations.

c. Supporting Agencies

(1) (U) The National Cyber Response Coordination Group (NCRCG). JTF GNO supports and coordinates with the National Cyber Response Coordination Group (NCRCG) on behalf of USSTRATCOM. Per ref g, the NCRCG is an interagency forum where organizations responsible for a range of activities (technical response and recovery, law enforcement, intelligence, and defensive measures) coordinate for the purposes of preparing for and executing an efficient and effective response to a cyber incident of national significance.

(2) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) CDRUSSTRATCOM for DOD

computers and DOD computer networks of the GIG. (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(3) (U) Joint Warfare Analysis Center (JWAC). The JWAC provides
(b)(1) Sec 1.7(e)
this CONPLAN, all JWAC support for operations in and through cyberspace should be coordinated through USSTRATCOM/J3. When this CONPLAN is not in effect, direct liaison (per C/S/A policy) is customary.

(4) (U) National Infrastructure Protection Center (NIPC). The NIPC serves as the focal point for threat assessment, warning, investigation, and response to threats or attacks against national critical information infrastructures. It serves as both a national security and law enforcement organization to detect, deter, assess, warn of, respond to, and investigate computer attacks, intrusion and unlawful acts target against the GIG. USSTRATCOM will normally interface with the NIPC through JTF GNO.

(5) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(6) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(7) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

d. Coordination With Diplomatic Agencies

(1) (U) Department of State (DOS). The SECDEF will coordinate with the Secretary of State on matters concerning diplomatic relations with foreign

governments involved in cyberspace operational matters. Under normal circumstances, CDRUSSTRATCOM will coordinate with the CJCS who in turn will coordinate with the DOS, when considering or recommending (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) as a cyberspace COA.

(2) (U) Department of Commerce (DOC). The SECDEF will coordinate with the Secretary of Commerce on matters concerning interstate and international commerce. There are three main areas of interest related to DOC federal regulatory responsibility concerning computer systems and computer networks: 1) regulating foreign sales of such technology, 2) the National Bureau of Standards that establishes standards and protocols for such technology, and 3) regulating interstate and international commerce related to such technology. Under normal circumstances, CDRUSSTRATCOM will coordinate with the CJCS who will coordinate with the DOC, on matters involving the DOD GIG.

5. Command and Control. (Command Posts).

a. (~~S//REL USA, AUS, GBR~~) Global Operation Center (GOC). The GOC (b)(1) Sec 1.4(a)

b. (U) JTF GNO

(1) (U) The Global NetOps Center (GNC) is the JTF GNO Command Center responsible for executing the daily operation and defense of the GIG. The GNC provides the overall management, control, and technical direction for GIG NetOps and oversees a collaborative coordination process involving all C/S/As, supporting the business, intelligence and warfighting needs of POTUS, SECDEF and the NetOps Community

(2) (U) JTF GNO has a full-time LE/CI Center for coordinating LE/CI activities in support of cyberspace missions. DOD LE/CI organizations have assigned full or part-time LE/CI agents from each of the LE/CI agencies, including Naval Criminal Investigative Service (NCIS), Defense Criminal Investigative Service (DCIS), Air Force Office of Special Investigations (OSI), US Army Criminal Investigations Division (USACID) and Army Intelligence and Security Command (INSCOM). JTF GNO LE/CI Center maintains a coordinating relationship with the IAIP, DHS.

c. (U) JFCC NW. JFCC NW (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

d. (U) JIOWC. The JIOWC is located at Lackland AFB in San Antonio Texas. The organization provides full spectrum IO planning support to C / S / A's worldwide through COCOM support teams.

Kevin P. Chilton
General, USAF
Commander

Official:
Mark H. Owen
Brigadier General, USAF
USSTRATCOM Plans and Policy

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE, NE 68113-6500
26 February 2008

ANNEX K TO USSTRATCOM CONPLAN 8039 (U)
(U) OPR: HQ USSTRATCOM J675

COMMAND, CONTROL, COMMUNICATIONS AND COMPUTER (C4) SYSTEMS (U)

(U) References:

a. (U) USSTRATCOM Strategic Administrative Instruction (SAI) 301-6, Collateral Automated Information System (AIS) Security Policy, Current Edition (U)

b. (U) USSTRATCOM Strategic Administrative Instruction (SAI) 500-1, Information Operations, Current Edition (U)

c. (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

d. (U) Chairman of the Joint Chiefs of Staff Operation Order (CJCS OPORD) 2-FY, Survivable Mobile Command Center Operations (S)

e. (U) CJCSI 6510.01D, Information Assurance and Computer Network Defense, Current Edition (U)

f. (U) CJCSI 3320.01B, "Electromagnetic Spectrum Use in Joint Military Operations", 15 May 06 (U)

g. (U) CJCSI 3320.02B-1, "Joint Spectrum Interference Resolution (JSIR)," 27 Jan 06 (S)

h. (U) CJCSM 3320.02C, "Joint Spectrum Interference Resolution (JSIR)," 27 Jan 06 (U)

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2033~~

1. (U) Situation

a. (U) (b)(1) Sec 1.7(e) (See Annex B, (b)(1) Sec 1.7(e)

b. (U) Friendly. See Appendix J.

(1) (U) Command Centers. See Appendix J.

(2) (U) (b)(7)(E) Provides (b)(7)(E)

(a) (U) Systems Experts: (b)(7)(E)

(b) (U) Network Management and Payload Control: (b)(7)(E)

(c) (U) (b)(7)(E) (b)(7)(E)

(d) (U) Focal Point for implementation of Commander (b)(7)(E) requirements: (b)(7)(E) (b)(7)(E)

(3) (U) (b)(7)(E) (b)(7)(E)

(a) (U) System Expert: (b)(7)(E)

(b) (U) Network Management and Payload Control: (b)(7)(E)

(c) (U) (b)(7)(E)

(d) (U) Focal Point for Unified Commander: SMC for authorized networks; Unified Commander communications planners for requirements.

(4) (U) (b)(7)(E) (b)(7)(E)

(a) (U) System Expert: (b)(7)(E)

(b) (U) Network Monitoring and Payload Control.

(c) (U) (b)(7)(E)

(d) (U) Focal Point for Unified Commander: USSTRATCOM/Command Center, Joint Staff/J38

(5) (U) (b)(7)(E)

(b)(7)(E)

(a) (U) System Expert: (b)(7)(E)

(b)(7)(E)

(b) (U) Network Monitoring and Payload Control: (b)(7)(E)

(b)(7)(E)

(c) (U) Focal Point for Commander Requirements: Individual Unified Commander communications planners or (b)(1) Sec 1.7(e)

(d) (U) (b)(7)(E)

(b)(7)(E)

(6) (U) Other Government and Commercial Satellite Communications.

(b)(7)(E)

2. (U) Mission. Provide command and control connectivity for USSTRATCOM operations on a global basis in support of peacetime, OPLAN, and contingency operations.

3. (U) Execution. Command and Control (C2) of USSTRATCOM assets, by their global nature, is highly dependent upon military and civilian satellite communications systems. USSTRATCOM assists the warfighting Commanders to ensure effective utilization of these systems by coordinating with the Joint Staff and the various System Experts.

a. (U) Concept Operations. Command, Control, and Communication (C3) support (b)(1) Sec 1.7(e) delineated in the execution paragraph of the base plan.

b. (U) Tasks

(1) (U) USSTRATCOM. Execute oversight of assigned SATCOM in support of the POTUS/SECDEF, CJCS, Combatant Commands, and other agencies.

(a) (U) Evaluate health and status of theater SATCOM systems and develop options for spacecraft movements and/or payload configurations.

(b) (U) Recommend spacecraft movements to satisfy warfighting Combatant Commander's SATCOM requirements.

(c) (U) Recommend SATCOM payload reconfiguration when satellite anomalies occur.

(d) (U) Propose SATCOM payload configurations to provide support to POTUS/SECDEF, CJCS, Combatant Commands, and other federal agencies.

(e) (U) Recommend augmenting C3 requirements with commercial and Allied SATCOM resources when Military SATCOM is not sufficient.

(f) (U) Provide SATCOM support for theater operations through (b)(1) Sec 1.7(e)

(g) (U) Develop SATCOM analysis based on developed supporting plans for the Commander and Joint Staff.

(h) (U) Develop alternative solutions for identified shortfalls.

(i) (U) Reassess and evaluate SATCOM environment and adjust plans as needed.

(2) (U) Supported Commands. Identify space-related C3 and SATCOM requirements to USSTRATCOM (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(3) (U) Component Commands. Be prepared to execute the C3 portions of this plan as modified by CDRUSSTRATCOM.

c. (U) Special Measures. All task organizations will use standard Information Security (INFOSEC) procedures and equipment. For joint actions (other than normal operations) with Unified and Specified Commands, the Intertheater COMSEC Package (ICP) will be used.

4. (U) Administration and Logistics

a. (U) Logistics. (N/A)

b. (U) Administration. The USSTRATCOM Knowledge Integration Web (SKIWEB) home page is the primary administration tool and can be accessed directly via SIPRNET.

5. (U) Command and Control

a. (U) Command Relationships. (See 8039 Annex J)

b. (U) Command, Control, Communications Systems. (See Appendices)

Appendices:
1 - Information Assurance (Not Used)
2 - Satellite Communications (Not Included)
3 - Defense Courier Service (Not Used)
4 - Foreign Data Exchange (Not Used)
5 - Electromagnetic (EM) Spectrum Management (Not Used)

Kevin P. Chilton
General, USAF
Commander

OFFICIAL

(b)(6)
CAPTAIN, USN
Director, C2 and Communications Systems

(INTENTIONALLY BLANK)

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE, NE 68113-6500
26 February 2008

ANNEX N TO USSTRATCOM CONPLAN 8039 (U)
(U) OPR: JFCC SPACE
SPACE OPERATIONS (U)

(U) References:

a. (U) National Space Policy, Oct 06 (S//NF)

b. (U) National Security Space (NSS) Protection Strategy, 30 Nov 04 Ver 5 (S//NF)

c. (U) CJCSI 3121.01A, Standing Rules of Engagement /Standing Rules of for US Forces, 13 Jun 05 (U) (SROE/SRUF)

d. (U) DOD Directive 3100.10, Space Policy, 9 Jul 99 (U)

e. (U) DOD Directive S-3600.1, Information Operations, 14 Aug 06 (S)

f. (U) Joint Pub 1-02, Department of Defense (DOD) Dictionary of Military & Associated Terms, 12 Apr 01 (U)

g. (U) DODI 3100.12, Space Support, 14 Sep 00 (U)

h. (U) DODI 3100.14, Space Force Enhancement, 12 Jan 01 (U)

i. (U) DODI 3100.15, Space Control, 19 Jan 01 (U)

j. (U) Joint Pub 3-14, Joint Doctrine for Space Operations, 9 Aug 02 (U)

k. (U) JP 3-13, Joint Doctrine for Information Operations, 13 Feb 06 (U)

l. (U) USSTRATCOM Commander's Strategic Concept, 11 Nov 03 (S/NF)

m. (U) United States Strategic Command (USSTRATCOM) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (S/REL)

n. (U) STRATCOM DIRECTIVE (SD) 505-3, Space Support to the Joint Force

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2033~~

Commander/Designated Space Coordinating Authority, Feb 04 (U)

o. (U) SD 515-2, ITWAA Procedures and System Description, 03 Oct 05 (SECRET)

p. (U) SD 523-2, Theater Event System Architecture and Ops,

q. (U) The Commission to Assess United States National Security Space Management and Organization Final Report, 2001 (U)

r. (U) AFDD 2-2.1, Counterspace Operations, 2 Aug 04 (U)

s. (U) AFDD 2-5, Information Operations, 11 Jan 05 (U)

t. (U) AFTTP 3-1.28, Tactical Employment Space, Mar 05 (S//NF)

u. (U) Space Capstone Threat Assessment, March 2006, NAIC (SECRET//FGI//NOFORN//MR)

v. (U) Horizontal Command and Control (C2) Integration (HC2I) Concept of Operations (CONOPS), 20 Dec 05

1. (U) Situation

a. (U) General

(1) (~~C//REL USA, AUS, GBR~~) US Cyber Operations are a strategic asset of the United States supporting US National Security Objectives. This annex provides an overview of relevant space operations and effects supporting operations executed under CONPLAN 8039. (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

(2) (~~S//REL USA, AUS, GBR~~) Some cyberspace capabilities operate in and through the space environment. (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

b. (U) (b)(1) Sec 1.7(e) Refer to Annex B (Intelligence) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

c. (U) Friendly

(1) (~~S//REL USA, AUS, GBR~~) The architecture (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
may be different in every GCC. Current USSTRATCOM (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
capabilities are briefly described below.

(a) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

1 (b)(1) Sec 1.4(a)

2 (b)(1) Sec 1.4(a)

3 (b)(1) Sec 1.4(a)

(b) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

1 (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

2 (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

3 (b)(1) Sec 1.4(a)

(c) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

1 (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

2 (b)(1) Sec 1.4(a) Analyses

3 Best accuracy (b)(1) Sec 1.4(a)

(2) (~~S//REL USA, AUS, GBR~~) Additional capabilities. Refer to (b)(1) Sec 1.4(a)

d. (U) Assumptions. Refer to Base Plan.

2. (U) Mission. Refer to Base Plan and Annex C (Operations).

3. (U) Execution. Refer to (b)(1) Sec 1.7(e)

4. (U) Administration and Logistics

(U) a. (~~S//REL USA, AUS, CAN, GBR~~) Services are responsible to support forces tasked in this Annex. Requirements that cannot be met by a respective service will be coordinated with USSTRATCOM.

b. (U) Reference Base Plan for additional logistics information.

5. (U) Command and Control

a. (U) USSTRATCOM has delegated JFCC SPACE to provide space mission expertise to plan, support, integrate, assess and synchronize efforts for USSTRATCOM, and other combatant commander's operational level requirements for space control operations.

b. (U) CDRUSSTRATCOM has assigned CDR JFCC SPACE as the GSCA to ensure unity of effort by coordinating, developing and conducting operational-level space campaign planning (including contingency and crisis action/adaptive planning and COA development) and strategy development in

support of USSTRATCOM and other Combatant Commanders. The GSCA is the commander designated by CDRUSSTRATCOM to have "Coordinating Authority" (CA) for the conduct and coordination of global space operations. CA is a specific consultation relationship between military commanders and other agencies, not an authority by which command and control may be exercised. As such, the commander who has been designated as the GSCA can require consultation between the agencies involved, but cannot compel agreement. CDRUSSTRATCOM will specify the common tasks to be coordinated in the establishing directive, without disturbing normal organizational relationships in other matters.

c. (U) The role of the Space Coordinating Authority (SCA) is described and defined in Joint Publication (JP) 3-0 III.2.d.(2) and Strategic Command Directive (SD) 505-3, Space Support To Joint Force Commander Or Designated Space Coordinating Authority. JP 3-0 defines the SCA as being responsible for coordinating and integrating space capabilities in the operational area, and has primary responsibility for joint space operations planning, to include ascertaining space requirements within the joint force. The SCA normally will be supported by assigned or attached embedded space personnel. The processes for articulating requirements for space force enhancement products are established and specifically tailored to the functional area they support, and result in prioritized requirements. The SCA recommends prioritized space force enhancement requirements to support the Joint Force Commander's mission and intent. Utilizing reachback through the JFCC Space at the Joint Space Operations Center, direct support relationships are established to provide optimal support to the Joint Force Commander, integrating and synchronizing space effects within the Joint Force Commander's Joint Operations Area. To ensure prompt and timely support, the supported GCC and CDRUSSTRATCOM may authorize direct liaison between the SCA and applicable component(s) of USSTRATCOM. Joint force Service component commands should communicate their requirements to the SCA, or designated representative, to ensure that all space activities are properly integrated and synchronized.

d. (U) C4 Systems. Refer to Base Plan and Annex K (C4 Systems).

e. (U) Refer to Base Plan and Annex J (Command Relationships) for additional Command and Control information.

Kevin P. Chilton
General, USAF
Commander

OFFICIAL:

WILLIAM L. SHELTON
Lieutenant General, USAF
Commander, JFCC SPACE

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE, NE 68113-6500
28 February 2008

ANNEX S TO USSTRATCOM CONPLAN 8039 (U)

(U) OPR: JFCC NW J59

(b)(1) Sec 1.7(e) (U)

(U) References: Refer to the Base Plan.

1. (U) Situation. This annex discusses (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) capabilities to support CONPLAN 8039.

2. (U) Mission. Refer to the Base Plan.

3. (U) Execution

a. (U) Concept of Operations

(1) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) provides guidance for (b)(1) Sec 1.4(a) planning and execution in CONPLAN 8039. This document identifies to planners that USSTRATCOM has chosen to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) includes Appendices and Tabs that addresses how apportioned and non-apportioned cyberspace (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) capabilities and would be included in (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) The complete annex is available on the HQ USSTRATCOM PDAS Website. (b)(1) Sec 1.4(e) access is required to review the annex.

4. (U) Administration and Logistics. Refer to the Base Plan and Exhibit 4 (Logistics) for each (b)(1) Sec 1.7(e) in the annex.

5. (U) Command and Control. Refer to Base Plan, Annex K (Command Relationships), and Exhibit 5 (Command and Control) for each (b)(1) Sec 1.7(e) in the annex.

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 27 February 2033~~

Kevin P. Chilton
General, USAF
Commander

OFFICIAL:
Mark H. Owen
Brigadier General, USAF
Director, Plans and Policy

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE, NE 68113-6500
26 February 2008

ANNEX V TO COMMANDER USSTRATCOM CONPLAN 8039 (U)
(U) OPR: HQUSSTRATCOM/J53
INTERAGENCY COORDINATION (U)

References:

a. (U) Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 12 April 2001 (As Amended Through 20 March 2006)

b. (U) Joint Publication 3-0, Joint Operations, 17 Sep 06

c. (U) CJCS Manual 6510.1D, Defense in Depth: Information Assurance (IA) and Computer Network Defense (CND) (U//FOUO), 25 Mar 03. Including Ch 1, 10 Aug 2004, current as of 18 Mar 2005.

d. (U) APPENDIX 12 TO ANNEX C (OPERATIONS) TO JTF-GNO OPORD 05-01 (Global Network Operations) INFORMATION OPERATIONS CONDITION (INFOCON) EXECUTION PROCEDURES (C/Rel USA, AUS, CAN, GBR, NZL), 22 May 06

e. (U) Horizontal Command and Control (C2) Integration (HC2I) Concept of Operations (CONOPS) (S/Rel USA, AUS, CAN, GBR), 20 Dec 05

f. (U) Presidential Decision Directive-62 (PDD-62), Protection Against Unconventional Threats to the Homeland and Americans Overseas, 22 May 98

g. (U) Presidential Decision Directive-63 (PDD-63), Critical Infrastructure Program, 22 May 99

h. (U) National Security Policy Directive 1, "Organization of the National Security Council System," 13 Feb 2001

i. (U) National Security Policy Directive 44, "Management of Interagency Efforts Concerning Reconstruction and Stabilization," 7 Dec 2005

j. (U) 2004 National Response Plan (NRP), Cyber Annex, Dec 04

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2033~~

k. (U) Homeland Security Presidential Directive 1: Organization and Operation of the Homeland Security Council. 29 October 2001

l. (U) Homeland Security Presidential Directive 7: Critical Infrastructure Protection. 17 December 2003

m. (U) Homeland Security Presidential Directive 8: National Preparedness. 17 December 2003

n. (U) JP 3-08 Vol I & II Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations, 17 March 2006

o. (U) National Infrastructure Protection Plan, 22-23 Aug 2006

p. (U) Trilateral Memorandum of Agreement among the Department of Defense, the Justice Department and the Intelligence Community Regarding Computer Network Attack and Computer Network Exploitation Activities (DOD-JD-IC MOA) (S//NFS//NF), 9 May 07

q. (U) Memorandum of Arrangement between The Department of Defence of Australia, The Ministry of Defence of The United Kingdom of Great Britain and Northern Ireland, and The Department Of Defense of The United States of America on Information Operations Data Exchange, 6 May 03

r. (U) 2008 National Response Framework (NRF).

s. (U) DODD 3025.1, Military Support to Civil Authorities, January 15, 1993.

t. (U) JP 3-28 Civil Support, September 14, 2007.

1. (U) Situation

a. (U) General

(1) (U) Statement. This Annex provides the basis for interagency coordination for Cyberspace Operations. It defines the roles and interagency relationships among United States (U.S.) Strategic Command (USSTRATCOM), Department of Defense (DOD) organizations, non-DOD U.S. Government agencies and civilian entities as they pertain to supporting CONPLAN 8039's (b)(1) Sec 1.7(e)

(a) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(b) (U) (b)(1) Sec 1.7(e)

(c) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(2) (U) Politico-Military Situation. U.S. reliance on computer systems and networks is vital to commerce and prosperity and is a critical capability of the nation's power. Since adversaries can conduct malicious activities that may jeopardize U.S. interests, including DOD's mission accomplishment and operations, CDRUSSTRATCOM requires proactive and cooperative interagency working arrangements with all agencies involved in cyberspace operations. It is imperative that support be given to the deliberate planning process to ensure interagency coordination is formalized and communicated to all those involved in cyberspace operational missions.

(3) (U) Policy Coordination

(a) (U) National Security Council (NSC)/Policy Coordination Committees (PCCs). Due to its transnational scope, CONPLAN 8039 can affect any of the six regional or 11 functional NSC/PCCs. However, the primary NSC/PCCs affected by CONPLAN 8039 are:

1 (U) Defense Strategy, Force Structure, and Planning (chaired by the Secretary of Defense)

2 (U) Counter-Terrorism and National Preparedness (chaired by the Assistant to the President for National Security Affairs)

3 (U) Proliferation, Counter proliferation, and Homeland Defense (chaired by the Assistant to the President for National Security Affairs)

(b) (U) General Guidance. The following highlights general functions for staff directorate coordination activities:

1 (U) Coordination Authority. JP 1-02 defines coordinating authority as:

> *"A commander or individual assigned responsibility for coordinating specific functions or activities involving forces of two or more Military Departments, two or more joint force components, or two or more forces of the same Service. The commander or individual has the authority to require consultation between the agencies involved, but does not have the authority to compel agreement. In the event that essential agreement cannot be obtained, the matter shall be referred to the appointing authority. Coordinating authority is a consultation relationship, not an authority through which command may be exercised. Coordinating authority is more applicable to planning and similar activities than to operations."*

2 (U) Coordination Relationships. USSTRATCOM will provide the nature of interagency coordination activities and the service categories.

Each agency may participate in operations, operations support and support, as defined below:

a (U) Operations. Actions by agencies to help direct and coordinate the plan's (b)(1) Sec 1.7(e) (see para 1.a. above). Interagency coordination for CONPLAN execution is delineated in the Base Plan by (b)(1) Sec 1.7(e) organization and task. See the Base Plan and (b)(1) Sec 1.7(e)

b (U) Operations Support. Actions by agencies to provide Indications and Warning (I&W), analytical support, tools, and other services.

c (U) Support. Actions by agencies to provide policy, doctrine, guidance, standards, research and development, and other general support for the cyberspace operations mission.

(4) (U) Planning and Execution Coordination. The interconnected and critical nature of the Defense Information Infrastructure (DII) to the National Information Infrastructure (NII), the Global Information Infrastructure (GII) and the GIG fundamentally increases the risk environment for the DOD computers and computer networks of the GIG. In this environment there is a shared risk, beyond DOD's control, that extends globally across networks to include the NII, GII and GIG and geographic boundaries. Cyberspace defense in this complex environment requires an organization to understand the dynamics of information processing, to develop and maintain current situation awareness supported by a Common Operational Picture (COP), and maintain unity of effort and command. To ensure effective cyberspace operations, Commander, USSTRATCOM must coordinate regularly with other DOD, non-DOD agencies and through the Chairman Joint Chiefs of Staff (CJCS) and Joint Staff (JS) to the POTUS, SECDEF and Cabinet Departments to incorporate, where applicable, all guidance, perspectives and available information on cyberspace operations. These include agencies and organizations within DOD, federal government agencies, state and local government, commercial and civilian organizations. Interagency coordination will be critical to the support of current POTUS and SecDef directives such as Presidential Decision Directive (PDD)-62 and PDD-63 and the National Continuity of Operations Plan. Commander, USSTRATCOM will plan, develop and provide recommendations through the CJCS and JS (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

b. (U) Assumptions. Refer to the Base Plan.

c. (U) Legal Considerations. See Base Plan and Appendix 8 (Rules of Engagement) to Annex C (Operations).

(U) 2. (~~S//REL USA, AUS, GBR~~) Mission. Refer to the Base Plan.

3. (U) Execution

a. (U) Concept of Operations. The primary objective of interagency coordination is effective operational execution of the DOD strategic, global cyberspace operations mission. Interagency coordination is absolutely vital to achieving this objective. Commander, USSTRATCOM will use interagency coordination to:

- (U) Assist USSTRATCOM cyberspace mission planning and execution supporting the plan's (b)(1) Sec 1.7(e)
- (U) Leverage the operational value associated with unity of command.
- (U) Improve operational situation awareness and information sharing.
- (~~S//REL USA, AUS, GBR~~) Coordinate, deconflict and integrate mutual initiatives to include the use of the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(1) (U) Commander's Intent. USSTRATCOM Commander's Intent by (b)(1) Sec 1.7(e) can be found in the Base Plan. Within the Base Plan, interagency coordination with respect to planning and authorities is a key event:

(a) (~~S//REL USA, AUS, GBR~~) Planning. USSTRATCOM may also require coordination (b)(1) Sec 1.4(a) USSTRATCOM will also work with the Office of the Secretary of Defense (OSD) and Joint Staff to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b) (~~S//REL USA, AUS, GBR~~) Authorities. Independent of the scale of the cyber engagement criteria, the authority will increase as the cyber engagement criteria grows in sophistication; the cyber engagement criteria may (b)(1) Sec 1.4(a)

(2) (U) (b)(1) Sec 1.7(e) Due to the transregional scope of CONPLAN 8039, interagency support will be tailored to (b)(1) Sec 1.7(e) each (b)(1) Sec 1.7(e) Generally, interagency (b)(1) Sec 1.7(e) is focused on:

(a) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Refer to the Base Plan for (b)(1) Sec 1.4(a) cyberspace by understanding adversary (b)(1) Sec 1.4(a) During this (b)(1) Sec 1.4(a) USSTRATCOM, in conjunction with the agency partners, will:

1 (U) Continue conducting (b)(1) Sec 1.7(e) NetOps mission.

2 (~~S//REL USA, AUS, GBR~~) Continue to develop and refine cyberspace plans (b)(1) Sec 1.4(a) Interagency partners as appropriate.

3 (~~S//REL USA, AUS, GBR~~) Continue to assist in defining the DOD requirements from other agency partners, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

4 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

5 (~~S//REL USA, AUS, GBR~~) Continue to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) with situational awareness of USSTRATCOM's (b)(1) Sec 1.4(a) cyberspace mission.

(b) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) See the Base Plan for military operations associated with this (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) USSTRATCOM, in conjunction with the agency partners, will:

1 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

2 (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) situational awareness to CDRUSSTRATCOM and Staff (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

3 (~~S//REL USA, AUS, GBR~~) Plan (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) and other agency partners.

4 (~~S//REL USA, AUS, GBR~~) Support and facilitate (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) agency partners.

(U)5 (~~S//REL USA, AUS, GBR~~) Provide updated interagency assessment to CDRUSSTRATCOM.

6 (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) to Annex A (Task Organization) (b)(1) Sec 1.4(a) for more information about (b)(1) Sec 1.4(a) operations.

(c) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Refer to the Base Plan for military operations associated with this (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) USSTRATCOM, in conjunction with the agency partners, will:

1 (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) operations.

2 (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) cyberspace situational awareness to CDRUSSTRATCOM and Staff, as well as agency (b)(1) Sec 1.4(a)

3 (~~S//REL USA, AUS, GBR~~) Continue (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) as appropriate, in coordination (b)(1) Sec 1.4(a) other agency partners.

4 (~~S//REL USA, AUS, GBR~~) Support and facilitate processing of (b)(1) Sec 1.4(a) to and from agency partners.

(U) 5 (~~S//REL USA, AUS, GBR~~) Provide updated interagency assessment to the Commander.

6 (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) planning and operations through support to applicable planning and operations groups.

(d) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Refer to the Base Plan for military operations associated with this (b)(1) Sec 1.4(a) The focus of the interagency effort (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) USSTRATCOM, in conjunction with the agency partners, will:

1 (~~S//REL USA, AUS, GBR~~) Continue to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) as appropriate.

2 (~~S//REL USA, AUS, GBR~~) Facilitate the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) operations through effective interagency coordination.

3 (~~S//REL USA, AUS, GBR~~) Support USSTRATCOM (b)(1) Sec 1.4(a) planning and operations.

(U) 4 (~~S//REL USA, AUS, GBR~~) Provide updated assessments to the Commander and agency partners.

5 (~~S//REL USA, AUS, GBR~~) Anticipate (b)(1) Sec 1.4(a) and (b)(1) Sec 1.4(a) operations.

(e) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Refer to the Base Plan for military operations associated with this (b)(1) Sec 1.4(a) interagency coordination focus (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) USSTRATCOM in conjunction with the agency partners, will:

1 (~~S//REL USA, AUS, GBR~~) Continue (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) as appropriate.

(U) 2 (~~S//REL USA, AUS, GBR~~) Facilitate the execution of DOD support to the primary or coordinating agency(s) through interagency coordinating as required.

3 (~~S//REL USA, AUS, GBR~~) Provide updated assessments to the commander and interagency partners regarding (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(U) 4 (~~S//REL USA, AUS, GBR~~) Provide the Commander with situational awareness of cyber-related transition requirements from DOD and agency partners for mutual support.

5 (~~S//REL USA, AUS, GBR~~) Anticipate (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) operations.

6 (~~S//REL USA, AUS, GBR~~) Provide updated cyber assessments to the commander and interagency partners regarding conditions in the (b)(1) Sec 1.4(a)

(f) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Refer to the Base Plan for military operations associated with this (b)(1) Sec 1.4(a) Interagency coordination focus is on providing support, as applicable and upon request, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) USSTRATCOM in conjunction with the agency partners, will:

1 (~~S//REL USA, AUS, GBR~~) Continue (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) as appropriate.

(U) 2 (~~S//REL USA, AUS, GBR~~) Facilitate the execution of DOD support to the primary or coordinating agency(s) through interagency coordinating as required.

3 (~~S//REL USA, AUS, GBR~~) Provide the Commander with situational awareness of cyber-related (b)(1) Sec 1.4(a) DOD and agency partners for mutual support.

4 (~~S//REL USA, AUS, GBR~~) Anticipate (b)(1) Sec 1.4(a) results.

5 (~~S//REL USA, AUS, GBR~~) Provide updated cyber assessments to the commander and interagency partners regarding conditions in the (b)(1) Sec 1.4(a)

b. (U) Tasks and Milestones

(1) (U) USSTRATCOM. The following guidance concerning CDRUSSTRATCOM command responsibilities is provided to assist deliberate planning and CONPLAN execution.

(a) (U) CDRUSSTRATCOM, as the lead Combatant Commander for cyberspace operations and planning, advocates cyberspace requirements for all Combatant Commanders, plans and develops national cyberspace operational requirements, conducts cyberspace operations planning and operations and supports other combatant commander cyberspace operations efforts. CDRUSSTRATCOM will focus on planning, policy, processes, mission coordination, synchronization and integration activities associated with the cyberspace operations mission. Combatant Commands, Services, Agencies

(C/S/As), components, and supporting forces will focus on operational mission execution. CDRUSSTRATCOM will interact with C/S/As to include, but not be limited to, the Joint Staff, SecDef, the Intelligence Community (IC), Law Enforcement (LE) Agencies, National Infrastructure Protection Center (NIPC) and the Department of Homeland Security (DHS) to integrate support and continuously improve the DOD's cyberspace operations processes.

(b) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Concept. USSTRATCOM may designate a lead component to establish a (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) to plan, synchronize, collaborate and deconflict operations for each scenario provided in (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) cyberspace operations in support of the combatant commander's desired objectives.

1 (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) will be offered the opportunity to assist with (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) concurs will be evaluated and adjudicated by CDRUSSTRATCOM. (b)(1) Sec 1.4(a) members are requested to leverage their agency's or organization's abilities to support the commander's objectives. (b)(1) Sec 1.4(a) military control and under SecDef-delegated military authorities.

2 (~~S//REL USA, AUS, GBR~~) Close liaison with all (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) evolve to meet these requirements.

3 (~~S//REL USA, AUS, GBR~~) For (b)(1) Sec 1.4(a) the lead USSTRATCOM component for the operation will provide the opportunity to physically and/or virtually participate in all planning activities and provide a secure and trusted environment that fosters transparency of operational equities. The (b)(1) Sec 1.4(a) will serve the following purposes:

a. (~~S//REL USA, AUS, GBR~~) Assist in the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

b. (~~S//REL USA, AUS, GBR~~) Provide information in support of a (b)(1) Sec 1.4(a) to Combatant Commanders, customers, planners and operators.

c (~~S//REL USA, AUS, GBR~~) Participate in and make recommendations for the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(U) d (~~S//REL USA, AUS, GBR~~) Assist in coordination, collaboration, synchronization, and deconfliction or courses of action in response to combatant commander's requirements, for both deliberate and crisis action planning.

(U) e (~~S//REL USA, AUS, GBR~~) Consider, advise and recommend solutions on all risks posed by planned or on-going operations.

(U) f (~~S//REL USA, AUS, GBR~~) Act as a representative authority or liaison (as determined by each member's organization or agency) on issues related to or surfacing from planned or on-going operations.

(U)g (~~S//REL USA, AUS, GBR~~) Assist in the formal coordination between the lead USSTRATCOM component and interagency senior officials which must [also] be in coordination with the Joint Staff.

h (~~S//REL USA, AUS, GBR~~) An adjunct membership to the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) cyberspace operations, in some cases with differing restrictions or legal requirements. The (b)(1) Sec 1.4(a) cyberspace environment.

i (~~S//REL USA, AUS, GBR~~) The (b)(1) Sec 1.4(a) at least (b)(1) Sec 1.4(a) (and other participants, as invited) to assess and address (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) authority level, or make recommendations for (b)(1) Sec 1.4(a) lead does not have approval authority.

(c) (U) HQ USSTRATCOM/J2 and Components will coordinate with the IC and its appropriate organizations to identify, manage, monitor, and advocate for cyberspace intelligence requirements, standardized reporting, (b)(1) Sec 1.7(e) and general intelligence support. In addition, specified component(s) will also (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) planning activities to focus monitoring, collection and analysis activities. The primary goal is to provide (b)(1) Sec 1.7(e) and value-added analysis for the CDRUSSTRATCOM to conduct global cyberspace missions.

(d) (U) USSTRATCOM will organize, advocate and coordinate cyberspace operational exercises across C/S/As. USSTRATCOM will advocate for standardized training and education requirements and coordinate cyberspace operational modeling and simulation efforts with applicable

agencies. USSTRATCOM will conduct deliberate and crisis action planning and produce a Joint Monthly Readiness Review (JMRR) for the DOD cyberspace operational mission and force structure. This will be based in large measure on inputs from the JFCC NW, the JTF GNO, JIOWC, and also on frequent interaction with C/S/As.

(e) (U) USSTRATCOM will develop, coordinate and advocate for cyberspace operations deliberate planning, concepts, policy, doctrine, (b)(1) Sec 1.7(e) and mission-level requirements. In addition, USSTRATCOM will assist in development and support of command and DOD partnerships with selected industry, academia and allies, including development of the necessary Memoranda of Agreement/Understanding. This will include establishing policies and resolving policy issues.

(f) (U) USSTRATCOM will support development of partnerships and relationships with DOD and non-DOD agencies, private industry and coalition partners. In addition, USSTRATCOM will help develop and advocate for common education, training and awareness standards for users, operators, and administrators. Finally, they will help ensure cyberspace operational requirements are reflected in plans, requirements and Courses of Action (COAs).

(g) (U) The USSTRATCOM/J006, will provide the required legal interpretations, liaison, related services, and inputs to support this plan. J006 will interpret appropriate legal policies and procedures in the development of partnerships and relationships with DOD and non-DOD agencies, private industry and coalition partners and allies. J006 will also work closely with the LE/CI centers in developing potential COAs, which fall under appropriate LE/CI authorities and coordinate with LE/CI legal staffs.

(2) (U) Coordination with Combatant Commanders

(a) (U) JTF GNO.

1 (U) JTF GNO has directive authority with DOD agencies, other than IC agencies, to counter strategic, global network attacks and intrusions and, has coordinating authority for responding to attacks and intrusions directed at DOD intelligence networks. The coordinating authority, with respect to DOD Intelligence networks, shall be exercised consistent with the Defense Criminal Investigative Service's responsibility for the network security for intelligence systems.

2 (U) JTF GNO receives agency incident reports and responses in compliance with (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) and national directives as appropriate. JTF GNO also coordinates with the DOD (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) to maintain status of DOD IC networks and significant incidents or threats to those networks. The IC will

exercise management and security oversight of the DOD IC networks while maintaining routine coordination with and reporting to JTF GNO.

3 (U) JTF GNO also supports and coordinates with the National Response Coordination Group (NCRCG) on behalf of USSTRATCOM. Per ref j, the NCRCG is an interagency forum where organizations responsible for a range of activities (technical response and recovery, law enforcement, intelligence, and defensive measures) coordinate for the purposes of preparing for and executing an efficient and effective response to a cyber incident.

4 (U) (b)(1) Sec 1.7(e) JTF GNO (b)(1) Sec 1.7(e) cyberspace operations. (b)(1) Sec 1.7(e) administrative, logistics, resource management, public affairs, and personnel support. JTF GNO maintains an (b)(1) Sec 1.7(e) may provide operational and technical analytical resources to augment JTF GNO.

5 (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) receives operational direction from JTF GNO.

6 (U) Law Enforcement/Counter-Intelligence (LE/CI). JTF GNO has a full-time LE/CI Center for coordinating LE/CI activities in support of cyberspace operations. DOD LE/CI agencies have assigned full and/or part time LE/CI agents to support the JTF GNO mission from each of the LE/CI agencies, including Naval Criminal Investigative Service, Defense Criminal Investigative Service, Air Force Office of Special Investigations (AFOSI), Army Criminal Investigations Command, and Army Intelligence and Security Command. A SJA provides necessary legal advice to the Commander JFCC NW, Commander JTF GNO and their staffs. The SJA works closely with the LE/CI Center in developing potential COAs which fall under appropriate LE/CI authorities and coordinates with LE/CI legal staffs.

(U) (b) (~~S//REL USA, AUS, GBR~~) JFCC NW. See Annex J, Command Relationships.

c. (U) Coordinating Instructions. This CONPLAN cannot task the Interagency partners. The following are recommendations for the conduct of the CONPLAN 8039 mission.

(1) (U) USSTRATCOM Coordination Activities. Within mission and resource constraints, USSTRATCOM will coordinate with appropriate national agencies, C/S/As and other agencies for cyberspace operations planning and execution. USSTRATCOM will coordinate with the following organizations:

(a) (U) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(b) (U) Intelligence Community (IC). Provide USSTRATCOM with intelligence standards, policy and guidance for intelligence support for cyberspace operations and foreign disclosure.

(c) (U) National Infrastructure Protection Center (NIPC). Provide USSTRATCOM with NII and LEA alerts and warnings, federal agency and private sector coordination and deconfliction, forensic analysis, LE/CI advice and support, NII situational awareness, COP, reporting for cyberspace operations, standardized processes and procedures, GIG coordination/deconfliction, intelligence warning, I&W, and planning and execution support.

(d) (U) Office of the Assistant Secretary of Defense, Networks and Information Integration (OASD/NII). OASD/NII, will provide USSTRATCOM with DOD policy, oversight and guidance, and support C3I, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) resource priorities for cyberspace operations. In addition, OASD/NII will provide Information Assurance (IA) training and certification standards, Information Technology architecture standards, acquisition support, and research and technology. CDRUSSTRATCOM will coordinate with OASD/NII to advocate C/S/A cyberspace operations requirements and priorities, coordination, feedback and policies.

(e) (U) Joint Staff (JS). Provide USSTRATCOM with rules of engagement (ROE), cyberspace operational requirements validation, joint policy and doctrine, joint exercise support, and plans and policy support. USSTRATCOM will coordinate with the JS for cyberspace operational execution, combatant commander cyberspace operational requirements and resource priorities, C4ISR, training, readiness, plans and policy, coordination and situational awareness (SA).

(f) (U) Supporting Combatant Commanders. Provide USSTRATCOM with operational impact assessments, cyberspace operational plans, operations and Information Security (INFOSEC) implementation, cyberspace operations resource requirements and priorities, cyberspace operations reporting, Information Operations Condition (INFOCON) implementation and component cyberspace operations readiness. USSTRATCOM will coordinate with all Combatant Commanders for planning, operations and resource requirements, cyberspace operational integration, coordination and deconfliction, cyberspace operations intelligence warning, I&W, attack assessment, and situational awareness.

(g) (U) Services. Provide USSTRATCOM with operations impact and technical assessments, plans, operations and INFOCON implementation, resource priorities and requirements, cyberspace operations readiness and

reporting and LE/CI intelligence support. USSTRATCOM will coordinate with the Services for intelligence and vulnerability information, red teaming, cyberspace operational integration, intelligence I&W, and attack assessments. The Services will advocate their requirements and priorities, contribute to overall situational awareness, conduct cyberspace operations coordination and ensure systems and operations, integration and deconfliction.

(h) (U) (b)(1) Sec 1.7(e) Provide USSTRATCOM (b)(1) Sec 1.7(e)

(i) (U) (b)(1) Sec 1.7(e) Provide CDRUSSTRATCOM (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) for requirements and priorities, standards, policy and procedures, operational direction, and situational awareness.

(j) (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(k) (U) Law Enforcement/Counter-Intelligence (LE/CI). DOD LE/CI agencies will provide USSTRATCOM with full and/or part time LE/CI agents from each of the LE/CI agencies, including NCIS, DCIS, AFOSI, USACID and INSCOM.

(l) (U) (b)(1) Sec 1.7(e) Provide USSTRATCOM (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(m) (U) Department of State (DOS). Coordinate and provide guidance for COAs requiring diplomatic action or have diplomatic ramifications.

(n) (U) Department of Commerce (DOC). Coordinate and provide guidance for COAs requiring economic action or have economic ramifications.

(o) (U) Department of Justice (DOJ). Per ref n, in exceptional circumstances and with appropriate authorization, military forces may also conduct missions to help the Department of Justice or other Federal law enforcement agencies (LEAs) assist federal, state, or local LEAs. Accordingly USSTRATCOM could be called upon to coordinate and provide guidance for cyber-related COAs requiring legal action or have legal ramifications.

(p) (U) Department of Homeland Security (DHS)

1 (U) Coordinate with USSTRATCOM and provide guidance for COAs related to homeland security and the protection of the United States.

2 (U) Per ref j Department of Homeland Security/Infrastructure Analysis and Infrastructure Protection/National Cyber Security Division (DHS/IAIP/NCSD) will act as the focal point for the security of non-DOD U.S. interests in cyberspace for purposes of analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems.

3 (U) In conjunction with the DOS, DHS will coordinate with USSTRATCOM and the interagency community to work with foreign countries and international organizations to strengthen the protection of U.S. critical information infrastructures and those foreign critical information infrastructures on which the United States relies and may impact DOD networks.

(q) (U) USNORTHCOM. USSTRATCOM will coordinate with USNORTHCOM for domestic cyber related incidents which will likely result in requests for assistance (RFAs) from other federal, state, tribal and local agencies, if their capabilities are exceeded. The Primary Agency in need of cyberspace support submits a Request for Assistance (RFA) to the Office of the Secretary of Defense (OSD) Executive Secretary for planning and assessment, if established the Defense Coordinating Officer (DCO) will validate the requirements on the RFA, the RFA will be forwarded to the Joint Director of Military Support (JDOMs) and the Assistant Secretary of Defense for Homeland Defense (ASD[HD]), a copy is provided to USNORTHCOM J3, JDOMS produces an EXORD for approval and the Secretary of Defense (SECDEF) in coordination with ASD(HD) approves it, and JDOMS issues the SECDEF-approved EXORD . When directed, USJFCOM, in coordination with USSTRATCOM, provides conventional forces to the Commander, US Northern Command, for Defense Support of Civil Authorities in support of other Federal, state, tribal and local government agencies for cyber related domestic incidents.

(2) (U) Additional USSTRATCOM Coordination Activities

(a) (U) Joint Activities. Joint Activities can provide a wealth of information, enabling tools, data and analysis to enhance USSTRATCOM's ability to identify critical nodes, networks, and other points of influence regarding adversaries and U.S. vulnerabilities that can affect U.S. interests in cyberspace. Some of the Joint Activities that USSTRATCOM can leverage when planning for cyberspace operations are the Joint Warfighting Center, Joint Warfare Analysis Center, Joint C4ISR Battle Center, Joint Program Office for Special Technical Countermeasures (JPO-STC), National Defense University (NDU) and Service War Colleges, Defense Advanced Research Projects Agency (DARPA), and Space and Naval Warfare Systems Command (SPAWAR).

(b) (U) Federal Government. As stated in ref n, The Homeland Security Act of 2002 established the DHS whose mission is to lead the unified national effort to secure America by preventing and deterring terrorist attacks and protecting against and responding to threats and hazards to the nation. As such, DHS is the lead federal agency for homeland security. While the most visible support occurs during domestic emergencies or major disasters, the majority of DOD's efforts are directed toward civilian law enforcement or intelligence agencies. This assistance is known as civil support within the defense community because the assistance will always be in support of a lead federal agency. Requests for assistance from another agency may be predicated on mutual agreements between agencies or stem from a Presidential designation of a Federal Disaster Area or a Federal State of Emergency. DOD typically only responds after the resources of other federal agencies, state and local governments to include National Guard and NGOs have been exhausted or when military assets are required. The DOD works closely with other Federal agencies in various domestic arenas. In addition to participating in interagency steering groups and councils, DOD is a partner in several national level incident management and emergency response plans such as the Federal Response Plan (as modified by the Initial National Response Plan, Cyber Annex). It is possible that USSTRATCOM could be called upon to assist in the event of a cyber-related disaster or domestic emergency. Accordingly USSTRATCOM will coordinate possible supporting efforts and plan with the Critical Infrastructure Assurance Office, National Security Telecommunications and Information Systems Security Committee, Office of the Manager of the National Communications System, National Institute of Standards and Technology and Department of Energy National Laboratories. Outside of JTF GNO's responsibility to coordinate with the NCRCG as stated above, all domestic cyber-related incidents which will likely result in RFAs from other federal agencies will be coordinated through USNORTHCOM.

(c) (U) Intelligence Community. Intelligence support provides the JFC with a timely, complete, and accurate understanding of the environment and potential adversaries. The method for collecting intelligence in support of cyberspace operations is generally the same as that for any other military

operation and is conducted in accordance with JP 2-01, Joint and National Intelligence Support to Military Operations. Managing the cyber intelligence collection, analysis, production, and dissemination for a CONPLAN 8039 crisis action may be complicated by non-USG civilians, especially members of IGOs and NGOs, who may be sensitive to the perception that they are being used to gather intelligence. This sensitivity may be based on the viewpoint that intelligence gathering is a provocative act and damages an individual's claim to impartiality. However, general information provided by personnel from IGOs and NGOs may corroborate intelligence gained from other sources. Generally, the best approach to information sharing with the NGOs and international civilian community is to keep the focus on complete transparency in sharing operational information and developing a shared situational awareness and understanding of the objectives to achieve the mission. However, classified information will only be shared with or released to individuals with the appropriate security clearance and need to know. In addition to IGOs and NGOs, USSTRATCOM will coordinate with the National Intelligence Council and the national intelligence agencies to support intelligence needs set forth in this plan.

(d) (U) Coalition Partners. Unity of effort is essential to coordinate cyberspace operations in joint and multinational environments, requiring coordination not only between Services and US agencies, but also among all coalition partners. USSTRATCOM must consider cyber-related priorities between DOD requirements and those of other USG agencies, the country team, coalition or UN forces, NGOs, and any international cyber-related organizations, that may be established. Close communications should be established with all elements to ensure that their cyberspace requirements are fully understood by the USSTRATCOM lead component to enable effective planning and effective cyberspace operations. USSTRATCOM will coordinate with the North Atlantic Treaty Organization (NATO) and other bilateral and multilateral coalitions as required.

(e) (U) Commonwealth Nations. The Commonwealth of Nations, usually known as "the Commonwealth" is a voluntary association of 53 independent sovereign states, all of which are former possessions of the British Empire, except for Mozambique and the United Kingdom itself. The Commonwealth is an international organization through which countries with diverse social, political, and economic backgrounds cooperate within a framework of common values and goals. These include the promotion of democracy, human rights, good governance, the rule of law, individual liberty, egalitarianism, free trade, multilateralism, and world peace. Currently USSTRATCOM has two cyber-related agreements with Commonwealth nations:

1 (~~C//REL USA, AUS, GBR~~) Tri-lateral Memorandum of Agreement (MOA) on IO data exchange. (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) and the Department of Defense of the United States of America, are signatories of a tri-lateral MOA on IO data exchange. The objective of this MOA (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)

2 (U) International Computer Network Defense Coordination Working Group. The International Computer Network Defense Coordination Working Group (ICCWG) is composed of five participating militaries: Australia, Canada, New Zealand, United Kingdom and United States. The ICCWG was established to exchange and conduct multilateral information assurance/computer network defense (IA/CND) up to the Top Secret level for the goal of strengthening information networks; to improve the confidentiality, integrity and availability of information systems; and improve the prediction, detection and response capabilities. USSTRATCOM/J51 is designated as the United States National Lead; JTF GNO is responsible for the operational mission.

(f) (U) Educational Activities. Far reaching changes are concurrently taking place in every major area of human life, perhaps most notably in how we conduct cyberspace warfare. Further, we expect information technology to continue its spectacular climb, greatly impacting cyberspace operations. Therefore, it is imperative that USSTRATCOM engage with educational activities and industry to understand and acquire new cyberspace operational capabilities that may affect DOD cyberspace. Some educational activities USSTRATCOM engages with are: (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) and Security and Service postgraduate schools.

(3) (U) Industry Relationships. For many of the same reasons outlined above, USSTRATCOM engages with educational activities, it will also coordinate with industry through the National Security Telecommunications Advisory Committee (NSTAC), PDD-63 Critical Infrastructure Sector Coordinators and Industry Information Sharing and Analysis Centers. USSTRATCOM may selectively establish relationships with industry that leverage councils and committees with both government and industry members. These top-level relationships will provide USSTRATCOM with a forum for gaining and sharing insights on common and developing telecommunications and security issues, major developments and advanced technologies. Industry participants on NSTAC will gain an understanding of DOD requirements and priorities, as well as insights into possible synergies between the DOD and industry for cyberspace operations.

(4) (U) Government-Industry Forums. The USSTRATCOM staff participates in the established (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
operations. Concurrently, National Science Foundation participants gain an understanding of USSTRATCOM technology needs and priorities for cyberspace operations and information assurance.

(5) (U) US Army. See Annex J (Command Relationships)

(6) (U) Navy Forces (NAVFOR). See Annex J (Command Relationships)

(7) (U) Marine Forces (MARFOR) See Annex J (Command Relationships)

(8) (U) Commander, Air Force Forces (COMAFFOR). See Annex J (Command Relationships)

(9) (U) GNOSC. The GNOSC consists of the Operations Center and DOD CERT and is co-located with JTF GNO. The GNOSC provides both the network operations view to JTF GNO and is the technical "arm" of JTF GNO via the DOD CERT.

(10) (U) JWRAC. The JWRAC is assigned administratively to DISA, and is under TACON of JTF GNO. Comprised of Reserve Component personnel, the JWRAC has the mission to "conduct analysis of content and data resident on publicly accessible DOD web sites across the full range of military operations."

Kevin P. Chilton
General, USAF
Commander

Official:

Mark H. Owen
Brigadier General, USAF
Director of Plans and Policy

(INTENTIONALLY BLANK)

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE, NE 68113-6500
26 February 2008

(U) ANNEX Y TO CDRUSSTRATCOM CONPLAN 8039 (U)
(U) OPR: JIOWC/JSSC
STRATEGIC COMMUNICATION (U)

(U) References: Refer to the Base Plan.

a. (U) National Security Strategy of the United States of America, March 2006 (U)

b. (U) National Defense Strategy of the United States of America, March 2005 (U)

c. (U) National Military Strategy of the United States of America, 2004 (U)

d. (U) US National Strategy for Public Diplomacy and Strategic Communication, 2007 (U)

e. (U) Presidential Decision Directive (PDD) 68, 30 April 1999, International Public Information (U)

f. (U) 2005 Contingency Planning Guidance (U)

g. (U) Strategic Planning Guidance, 22 March 2006 (U)

h. (S) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (S)

i. (S//Rel USA, GBR, AUS) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (S)

j. (U) Quadrennial Defense Review (QDR) Execution Roadmap for Strategic Communication, 25 Sep 2006 (U)

k. (U) National Strategy to Public Diplomacy and Strategic Communications

1. (U) Situation

a. (U) General

(1) (U) The United States faces a growing threat from hostile state, and non-state actors with the intent and capability to threaten US vital interests.

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2033~~

Effective SC by the whole of government is critical to deterring attacks by hostile actors. America must effectively use words, actions, and images to demonstrate the country's will and means to impose costs, while encouraging restraint. According to the 2006 QDR Execution Roadmap, the term strategic communication (SC) is defined as, "Focused U.S. government processes and efforts to understand and engage key audiences in order to create, strengthen or preserve conditions favorable to advancing national interests and policies through the use of coordinated information, themes, plans, programs, and actions with other elements of national power." The POTUS directs the nation's overall SC effort. Based on Presidential guidance, DOS leads America's public diplomacy efforts with foreign state and non-state actors. DOD provides extensive lethal and non-lethal capabilities that should supplement efforts, by DOS and other USG agencies, to engage key audiences to advance US interests and policies. USSTRATCOM planners must consider that words, actions, and images, from the highest to lowest ranking members of the Armed Forces, can profoundly impact the success or failure of USG policies and interests. The CDRUSSTRATCOM must be in continuous contact with the leaders in Washington and other Combatant Commanders as required, to ensure USSTRATCOM efforts are in concert with the overall USG SC effort, pursuant to Presidential guidance.

(2) (U) USG Guidance. USG guidance is fluid in nature, responsive to the global geo-political situation, internal US politics, mood of the American populace, and opinions of key US and world leaders. USG policies and objectives are delineated through speeches, statements, and documents by the POTUS, Secretary of State, Congress, and other influential leaders. USSTRATCOM SC efforts should support the new U.S National Strategy for Public Diplomacy (PD) and Strategic Communication, dated June 2007, which provides three strategic objectives for engaging foreign audiences: (1) America must offer a positive vision of hope and opportunity that is rooted in our most basic values; (2) With our partners, we seek to isolate and marginalize violent extremists who threaten the freedom and peace sought by civilized people of every nation, culture and faith; (3) America must work to nurture common interests and values between Americans and peoples of different countries, culture and faiths across the world. The 2006 NSS establishes eight national security objectives: (1) To champion human dignity; (2) To strengthen alliances against terrorism; (3) To defuse regional conflicts; (4) To prevent threats from weapons of mass destruction; (5) To encourage global economic development (6) To expand the circle of development; (7) To cooperate with the other centers of global power; and (8) To transform America's national security institutions to meet the challenges and opportunities of the Twenty- First Century. Additional clarification on national objectives as they pertain to specific hostile state and non-state actors are available via multiple open source channels.

(3) (~~S//REL USA, AUS, GBR~~) Country/Regional Perspective. Military planners must consider the perceptions, attitudes, and beliefs of each actor, or

target audience. Although communications may be conducted in space or cyberspace, the target audiences reside within Geographic Combatant Command (GCC) areas of responsibility. Every country and region across the globe is unique, with varying opinions and attitudes. (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a) and the respective Geographic Combatant Command's Public Affairs Office, SC Working Group, and Joint Interagency Coordination Group.

b. (U) Adversary. See Annex B (Intelligence) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

c. (U) Friendly

(1) (U) See Base Plan for the general friendly situation.

(2) (U) DOS. The DOS-led SC and PD Policy Coordinating Committee (PCC) supports USG policy and interests as directed by the POTUS. In June 2007, this interagency committee published the US National Strategy for Public Diplomacy and Strategic Communication, under the guidance of Amb. Karen Hughes. This strategy, which supplements the NSS and NMS, provides overarching USG guidance for US diplomatic and communication efforts. A DOD link to the State Department is the DOD Strategic Communication Integration Group (SCIG) Secretariat, which serves as a conduit for the Combatant Commands to surface SC issues for interagency consideration, via an Executive Committee, to the Deputy Secretary of Defense. Other conduits to the State Department include joint inter-agency task forces, joint inter-agency coordination groups, political advisors, and for USSTRATCOM, J5 and JIOWC LNOs at the Pentagon, plus conferences, meetings, seminars, and other means as appropriate.

(4) (U) Geographic Combatant Commands (GCCs). The GCCs use varying processes and organizational structures to plan, execute, and assess SC efforts. Based on Department of State (DOS) and Office of the Secretary of Defense/Public Affairs (OSD/PA) guidance, the GCCs develop themes, messages, and talking points for target audiences in their AORs. USSTRATCOM planners should leverage existing processes and organizations,

such as the GCC SC Working Groups and Strategic Effects Cells/Divisions, as well as the JIOWC's GCC Support Teams to ensure unity of effort.

(5) (U) See base plan and Annex A (Task Organization) for 8039's friendly force capabilities, which are drawn from USSTRATCOM global mission areas for full-spectrum capabilities (b)(1) Sec 1.7(e)

(6) (U) See applicable OPLAN and force deployment lists for the Combatant Commands that will be involved in the operation.

(7) (U) Assumptions. Refer to the Base Plan.

2. (U) Mission. Refer to the Base Plan

3. (U) Execution

a. (U) Concept of Operations

(1) (~~S//REL USA, AUS, GBR~~) The purpose of CONPLAN 8039 is to ensure that the U.S. military can operate in cyberspace (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) providing our own forces the freedom of action in cyberspace. The USG (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a). OSD/PA provides public affairs guidance to the GCC Public Affairs Offices (PAOs), reinforcing USG (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) in coordination with DOS efforts. This annex provides a framework to facilitate the integration and synchronization of DOD SC capabilities as part of an overarching USG cohesive effort to accomplish the mission, focusing on: (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) SC efforts should support US strategic objectives and considerations (b)(1) Sec 1.4(a) as identified in the base plan.

(2) (U) Overall Plan Objectives and End State. Refer to the Base Plan.

(3) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) SC actions (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) operations. Day-to-day operations should emphasize (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) SC planners are tasked to develop a communications strategy that will (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) power to be effective. The planning, execution, and assessment of SC actions (b)(1) Sec 1.4(a) should be closely coordinated with the applicable GCCs, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(4) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) SC planners should revise SC actions based on assessed success or failure to achieve desired (b)(1) Sec 1.4(a)

(5) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(6) (U) (b)(1) Sec 1.7(e) SC efforts will continue to (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) conduct of operations in Cyberspace." SC actions should focus on (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(7) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) The overall SC effort during (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(8) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) SC (b)(1) Sec 1.4(a) USSTRATCOM will (b)(1) Sec 1.4(a) In addition, USSTRATCOM will provide support to the effected GCC, as required, for (b)(1) Sec 1.4(a)

(a) (U) Desired SC Effects which help or support (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

1. (U) Minimize adversary cyberspace activities to conduct aggressive actions against US interest. cyberspace activities by adversaries (b)(1) Sec 1.7(e) supported by the following actions:

2. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) cyberspace.

3. (~~S//REL USA, AUS, GBR~~) Conduct cyberspace (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

4. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) cyberspace.

(U) 5. (~~S//REL USA, AUS, GBR~~) Protect and defend friendly information systems and content.

6. (~~S//REL USA, AUS and GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) cyberspace capabilities.

(9) (~~S//REL USA, AUS, CAN, GBR~~) USSTRATCOM Role. (b)(1) Sec 1.4(a)
(b)(1) Sec 1.4(a)
have been tailored for audiences in their AORs. USSTRATCOM SC planners should also leverage the habitual, working relationships between the JIOWC and the GCCs to ensure unity of effort.

(10) (~~S//REL USA, AUS, GBR~~) End State. The common end-state for all (b)(1) Sec 1.4(a)

(11) (U) Specific Guidance

(a) (U) The SC goal is for DOD to plan, integrate, synchronize, disseminate and (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(b) (U) CDRJIOWC is CDRUSSTRATCOM's SC lead and as such must be kept informed of all USSTRATCOM (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) In times of crisis, the JIOWC Operations Center (OPCENTER) will maintain continuous contact with the USSTRATCOM Headquarters (HQ) GOC, USSTRATCOM senior leadership, POLAD, and PAO. The entire JIOWC will be matrixed as required to support SC planning, execution, assessment and decision making. The JIOWC (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) USSTRATCOM staff and other personnel working SC issues as required.

(c) (U) GCC SC staffs should leverage USSTRATCOM-wide capabilities, such as the USSTRATCOM J2, J3, and J5, PAO, JFCC NW, and JIOWC. The JIOWC's GCC Support Teams and JSSC provide additional sources of SC planning experience across multiple GCC AORs.

(d) (~~S//REL USA, AUS, GBR~~) JFCC/SCC/JTF planners should surface key SC related issues, especially those involving interagency coordination primarily through the GCCs Joint Interagency Coordination Groups (JIACGs), POLADs, and Strategic Communications Working Groups (SCWGs). The CDR JIOWC serves as the USTRATCOM link to the DOD SCIG Secretariat. The Secretariat holds weekly SC Video-Telecommunication Conferences (VTCs), attended by the Combatant Commands, Joint Public Affairs Support Element (JPASE), (b)(1) Sec 1.4(a) and other organizations involved in the DOD SC planning process. This VTC provides a forum for planners to surface key SC issues that may impact deterrence operations, execution, or planning.

(e) (U) SC plans must be tailored for diverse target audiences, such as: (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(12) (U) (b)(1) Sec 1.7(e) SC planners need to determine if the disseminated USG communications (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) USSTRATCOM related actions, such as key speeches by the command leadership. The JIOWC, via the USSTRATCOM J2, can also (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(13) (U) (b)(1) Sec 1.7(e) the impact of USG communication efforts requires baseline data by (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) USSTRATCOM maintains a limited (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

b. (U) Tasks

(1) (U) USSTRATCOM Public Affairs Office. See Annex F (Public Affairs). PAO will provide PA guidance for the command and conduct (b)(1) Sec 1.7(e) for statements or speeches made by USSTRATCOM leadership. The PAO

coordinates the development of PA guidance, to include talking points, with OSD/PA and other Combatant Commands as required.

(2) (U) JIOWC. JIOWC will coordinate SC planning efforts with the GCCs. JIOWC provides SC planning support to USSTRATCOM components and GCCs as required. During crisis situations, JIOWC will maintain continuous contact with the USTRATCOM GOC, SCIG, and GCC staffs as required.

(3) (U) JFCCs and JTF GNO will maintain continuous contact with the USTRATCOM GOC during crisis situations. USSTRATCOM Component Commands should coordinate SC related efforts with the JIOWC, leveraging the JIOWC's GCC Support Team's relationships with the GCC SC and IO staffs.

(4) (U) Other. See Base Plan for tasks within (b)(1) Sec 1.7(e) as appropriate.

c. (U) Coordinating Instructions

(1) (U) This document is effective for planning upon receipt and execution upon approval of the overall base plan as well as the (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(2) (~~S//REL USA, AUS, GBR~~) USSTRATCOM Component Commands will integrate planning efforts to (b)(1) Sec 1.4(a) with the applicable GCCs. Commands should leverage JIOWC GCC Support Teams to conduct (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(3) (~~S//REL USA, AUS, GBR~~) CDRUSSTRATCOM will coordinate with Combatant Commanders in order to develop and provide those commanders (b)(1) Sec 1.4(a) See CDRUSSTRATCOM support plans for specific details.

d. (U) Definitions

(1) (U) Public Diplomacy (PD): Those overt international public information activities of the USG designed to promote US foreign policy (b)(1) Sec 1.7(e) institutions and their counterparts abroad (JP 3-53 and JP 1-02). The DOS has the lead within the USG for PD.

(2) (U) (b)(1) Sec 1.7(e) DOD activities (b)(1) Sec 1.7(e)

communication. (b)(1) Sec 1.7(e)
environment in support of USG information activities through efforts that may include, (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e)

(3) (U) Military Diplomacy (MD): The ability to support those activities and measures U.S. military leaders take to engage military, defense and government officials of another country to communicate USG policies and messages and to build defense and coalition relationships. (Derived from March, 2004 National Military Strategic Plan for the War on Terrorism)

(4) (U) Public Affairs (PA): Those public information, command information, and community relations' activities directed toward both the external and internal publics with interest in the DOD. (JP 3-61). USTRATCOM PAO is lead for the command, and will coordinate with OSD/PA and the applicable GCC PAO.

(5) (U) Military Information Operations (IO): The integrated employment of the core capabilities of (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) in concert with specified supporting capabilities (information assurance, physical security, counter-intelligence, physical attack, and combat communications) and related capabilities (public affairs, civil military operations, and defense support to public diplomacy) (b)(1) Sec 1.7(e)
(b)(1) Sec 1.7(e) (JP 3-13, Feb 07) USSTRATCOM components should leverage the existing working relationships between the JIOWC GCC Support Teams and the GCC IO staffs, to integrate and synchronize SC with IO efforts, to achieve the Combatant Commander's desired effects on local, regional, and global audiences.

4. (U) Administrative and Logistics. See Base Plan.

a. (U) SC personnel and administrative support will be furnished by supporting commands in accordance with Service directives, Command Arrangements Agreements (CAA), Memorandums of Understanding (MOU), Task Force CONOPS, and the logistics concept for support operations outlined in CDRUSSTRATCOM plans and directives.

b. JIOWC will coordinate with USSTRATCOM Strategic Effects Cells and other DOD SCWGs to help synchronize SC across the interagency

5. (U) Command and Control. CDRJIOWC is CDRUSSTRATCOM's SC lead, and as such must be kept informed of all USSTRATCOM (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) In times of crisis, the JIOWC JOC will maintain continuous contact with the USTRATCOM HQ GOC, USSTRACOM senior leadership, POLAD, and PAO. The JIOWC will be matrixed as required to support SC planning, execution, assessment and decision making. The JIOWC GCC Support Teams will maintain continuous contact with the applicable GCC SC planning staffs. The JIOWC's Joint SC Support Cell will maintain close contact with the SCIG at the Pentagon, USSTRATCOM staff and other personnel working SC issues as required. See paragraph 5. "Command and Control" of Base Plan; Annex J (Command Relationships), and Annex K (Command, Control, Communications, and Computers (C4) Systems) to Base Plan as appropriate.

Kevin P. Chilton
General, USAF
Commander

(INTENTIONALLY BLANK)

HEADQUARTERS, US STRATEGIC COMMAND
OFFUTT AIR FORCE BASE, NE 68113-6500
28 February 2008

ANNEX Z TO USSTRATCOM CONPLAN 8039 (U)
(U) OPR: HQUSSTRATCOM/J53
DISTRIBUTION (U)

1. (U) ~~Distribution of this document will be on a strict "need-to-know" basis with limited distribution.~~

2. (U) ~~Consistent with a need-to-know, supporting commands may reproduce and distribute this plan to assigned forces as required to fulfill mission requirements, and as required for the preparation of supporting plans. In addition, the plan is available electronically on the USSTRATCOM SIPRNET/GCCS Homepage.~~

~~Classified by: Multiple Sources~~
~~Reason: 1.4(a), (c), and (g)~~
~~Declassify on: 26 February 2033~~

(U) Table of Distribution (U)

DISTRIBUTION	OFFICE CODE	NO. COPIES
Joint Staff/J7 CWPD	J7	12
OSD		
CHIEF OF STAFF, US ARMY		
CHIEF OF NAVAL OPERATIONS		
CHIEF OF STAFF, USAF		
CMDT, MARINE CORPS		
CMDT, COAST GUARD		
DISA		
DLA		
NGA		
NSA		
DIA		
DTRA		
USCENTCOM	J3	1
	J5	1
USEUCOM	ECJ3	1
	ECJ5	1
USNORTHCOM	J3	1
	J5	1
USPACOM	J3	1
	J5	1
USSOCOM	SOJ3	1
	SOJ5	1
USSOUTHCOM	SCJ3	1
	SCJ5	1
USJFCOM	J2	1
	J3	
	J5	
USTRANSCOM	J5	1
USELEMNORAD (US ONLY)	N/J3	1
	N/J5	1
HQ ACC	A3	1
	A3	1

DISTRIBUTION	OFFICE CODE	NO. COPIES
HQ AMC	A3	1
	A4	1
	XO	1
	TACC	1
HQ AFSPC	XO	1
	A8	1
	14AF	1
	SWC	1
NNSOC	N3	1
NETWARCOM	N3	1
	N9	1
COMMARFORSTRAT		1
HQ SMDC	G5	1
8 AF	A2/INR	1
	TFC 204	1
	8 IWF	1
20 AF	DOME	1
	TFC 214	
HQ USAFE	A8	1
HQ PACAF	A8	1
JWAC	J31	1
HQ AIA	A3	1
	AFWIC	1
	67IW	1
	NASIC	1
DEFENSE SUPPLY CENTER	DSCP-OMP/CC	1
20th IS/TMF	CCOZ	1
Cheyenne Mountain Operations Center	J5	1
480 IG		1
DET 1 608 AOG	SMD	1
Office Naval Intelligence (ONI)		1
COMNAVMETOCCOM		1
AFGW Agency		1
HQ Air Force Reserve Command	AFRC/A3	1
National Guard Bureau	A3	1
Commander, HQ AFOSI	A3	1
Director, NCIS	0022B	1

DISTRIBUTION	OFFICE CODE	NO. COPIES
USSTRATCOM (Internal Distribution)	J1	1
	J2	1
	J3	2
	J4	1
	J5	3
	J6	1
	J7	1
	J8	1
	GISC	1
Joint Functional Component Command Global Strike and Integration (JFCC GSI)	J3	1
	J5	1
Joint Functional Component Command Integrated Missile Defense (JFCC IMD)	J5	1
	J3	1
Joint Functional Component Command Intelligence, Surveillance, Reconnaissance (JFCC ISR)	OPS	1
	PLANS	1
Joint Functional Component Command Network Warfare (JFCC NW)	J3	1
	J5	1
Joint Functional Component Command-Space (JFCC SPACE)		1
Joint Information Operations Warfare Command (JIOWC)		1
STRATCOM Center for Combating Weapons of Mass Destruction (SCC WMD)		1
Joint Task Force Global Network Operations (JTF GNO)	J3	1
	J5	1
NSA Rep to USSTRATCOM		1
CIA Rep to USSTRATCOM		1
DIA Rep to USSTRATCOM		1
NGA Rep to USSTRATCOM		1
NRO Rep to USSTRATCOM		1
NASA Rep to USSTRATCOM		1
DISA Rep to USSTRATCOM		1
USSTRATCOM NAOC	Plans	2

Kevin P. Chilton
General, USAF
Commander

OFFICIAL:

Mark H. Owen
Brigadier General, USAF
Director, Plans and Policy

(INTENTIONALLY BLANK)