NOV 2 8 2018

Michael Martelle
The National Security Archive
Gelman Library, Suite 701
2130 H Street, N.W.
Washington, D.C. 20037

Dear Mr. Martelle,

Thank you for your September 9, 2018 Freedom of Information Act (FOIA) request for the briefing on the Joint Intelligence Operations Center given November 30, 2016.

As the initial denial authority, I am partially denying portions of the document under 5 U.S.C. § 552(b)(1). The denied portions include classified national security information under the criteria of Executive Order 13526 (labeled as (b)(1)).

If you are not satisfied with our action on this request, you may file an administrative appeal within 90 calendar days from the date of this letter by U.S. mail or email. If you submit your appeal in writing, please address it to ODCMO, Director of Oversight and Compliance, 4800 Mark Center Drive, ATTN: DPCLTD, FOIA Appeals, Mailbox #24, Alexandria VA 22350-1700. If you submit your appeal by email please send it to OSD.FOIA-APPEAL@mail.mil. All correspondence should reference U.S. Cyber Command case tracking number 19-R012.

Additionally, you may contact the Office of Government Information Services (OGIS), which provides mediation services to help resolve disputes between FOIA requesters and Federal agencies. Contact information is 8601 Adelphi Road – OGIS, College Park, MD 20740-6001. OGIS may also be reached at ogis@nara.gov, 202-741-5770, and 1-877-684-6448.

Sincerely,
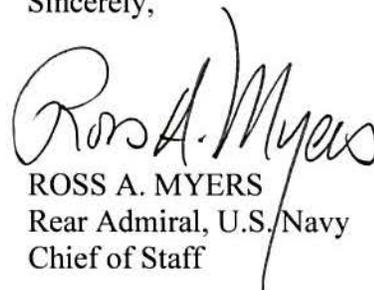
ROSS A. MYERS
Rear Admiral, U.S. Navy
Chief of Staff

USCYBERCOM JIOC

COMBAT TARGETS DIVISION

Improving Targeting Support to Cyber Operations

30 November2016

The overall classification of this briefing is: ~~TOP SECRET//SI//ORCON/NOFORN/FISA~~

Targeting in the Digital (NOT Industrial) Age

Targeting Processes must:

1. *Enable* Cyber Operations against agile, dynamic, fleeting elements in the cyber domain;

2. *Facilitate* an operational level Commander's timely, effective, and relevant decision-making;

3. *Add* value to IC understanding of our targets.

Cyberspace Operations
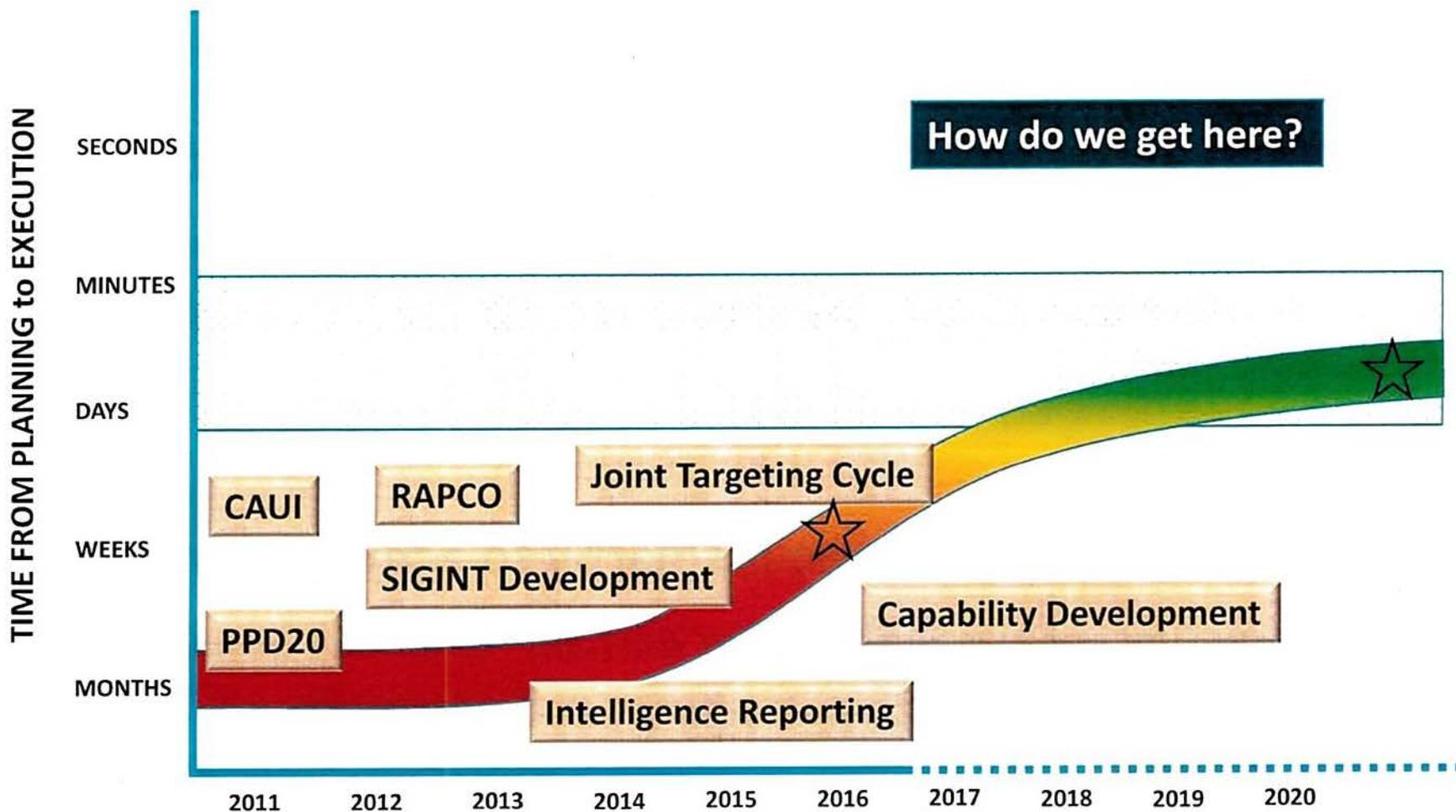
Two Major Considerations

1. When do we need to use the Joint Targeting Cycle?

   - JTC adds necessary structure and rigor, but does not apply to all cyber operations. We should not use the JTC when we do not need it.

2. When we do use it, use it smartly to achieve our goals

   - Targeting entities in the cyber domain requires a better application of targeting structures and processes.

Terminology and Processes

- (U) Target Development
  - Systematic examination of potential target systems to determine the necessary type and duration of action that must be exerted on each target to create an effect that is consistent with the commander's specific objectives
  - JP 3-60

- (TS//SI//REL to USA, FVEY) SIGINT Development
  - (b)(1) Sec. 1.4(a)
  -
  -

- (TS//SI//REL to USA, GBR) Network: Technical or Social/Functional?
  - (b)(1) Sec. 1.4(a)

- (U//FOUO) Battle Damage Assessment
  - The estimate of damage or effect resulting from the application of lethal or nonlethal military force. Battle damage assessment is composed of physical damage assessment, change assessment, functional damage assessment, and target system assessment.
  - CJCSM 3162.01

- (U//FOUO) Cyberspace Temporary Effects Assessment (C-TEAR)
  - USCYBERCOM Joint Target Intel Assessment Guidance for temp degradation or disruption

Similar terminology from different disciplines adds to confusion

Additional Considerations

- (U) JTC is optimized for lethal effects

  - Therefore JTC is *sub-optimized* for non lethal and temporary effects

- (U//~~FOUO~~) Integration of non-lethal fires and information-related capabilities is mostly a planning problem

  - Desire for deconfliction and synchronization does not dictate use of the JTC

- (U) What is the cost/benefit analysis of using the JTC?

Joint Targeting Cycle (JP 3-60)

End State and
CDR's Objectives

Target Development
and Prioritization

Targeting Assessment

Capabilities
Analysis

Mission Planning and
Force Execution

CDR's Decision and
Force Assignment
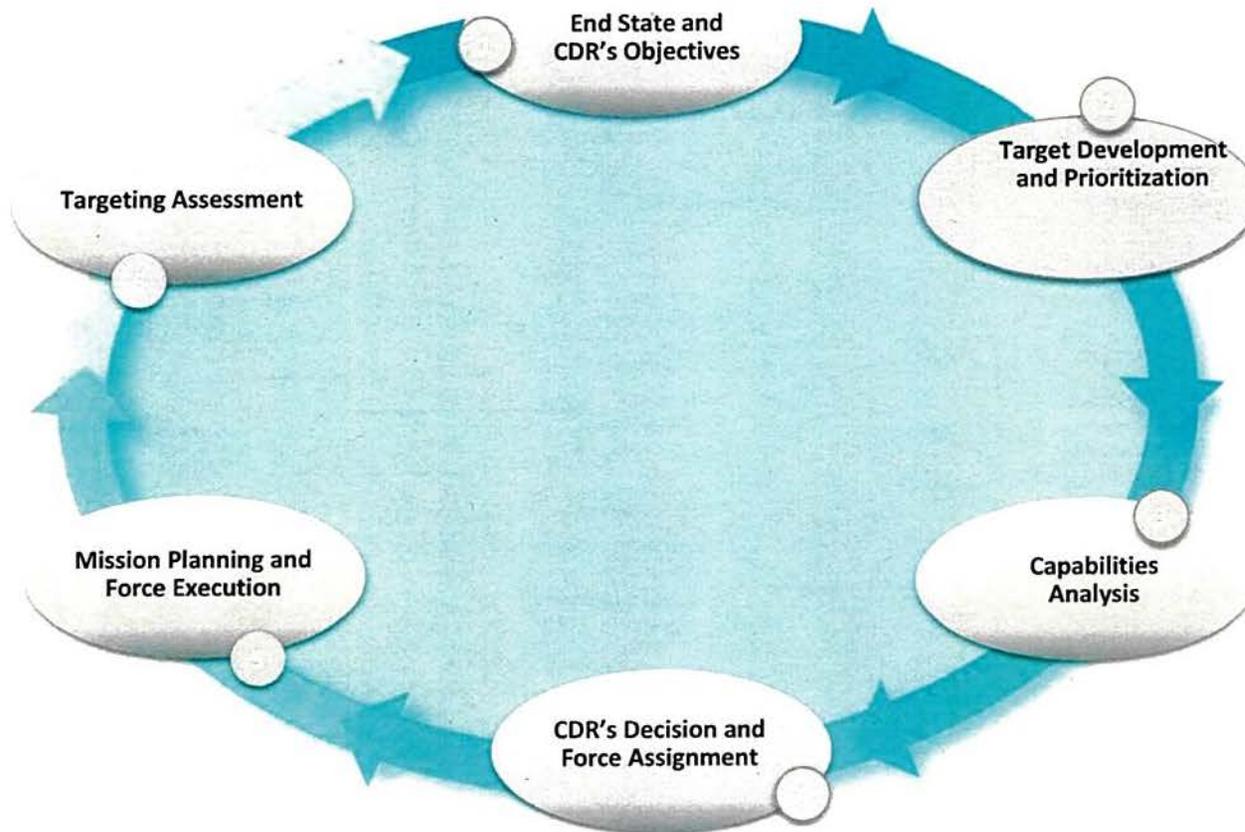
Joint Targeting Cycle (USCYBERCOM)

(b)(1) Sec. 1.4(a)
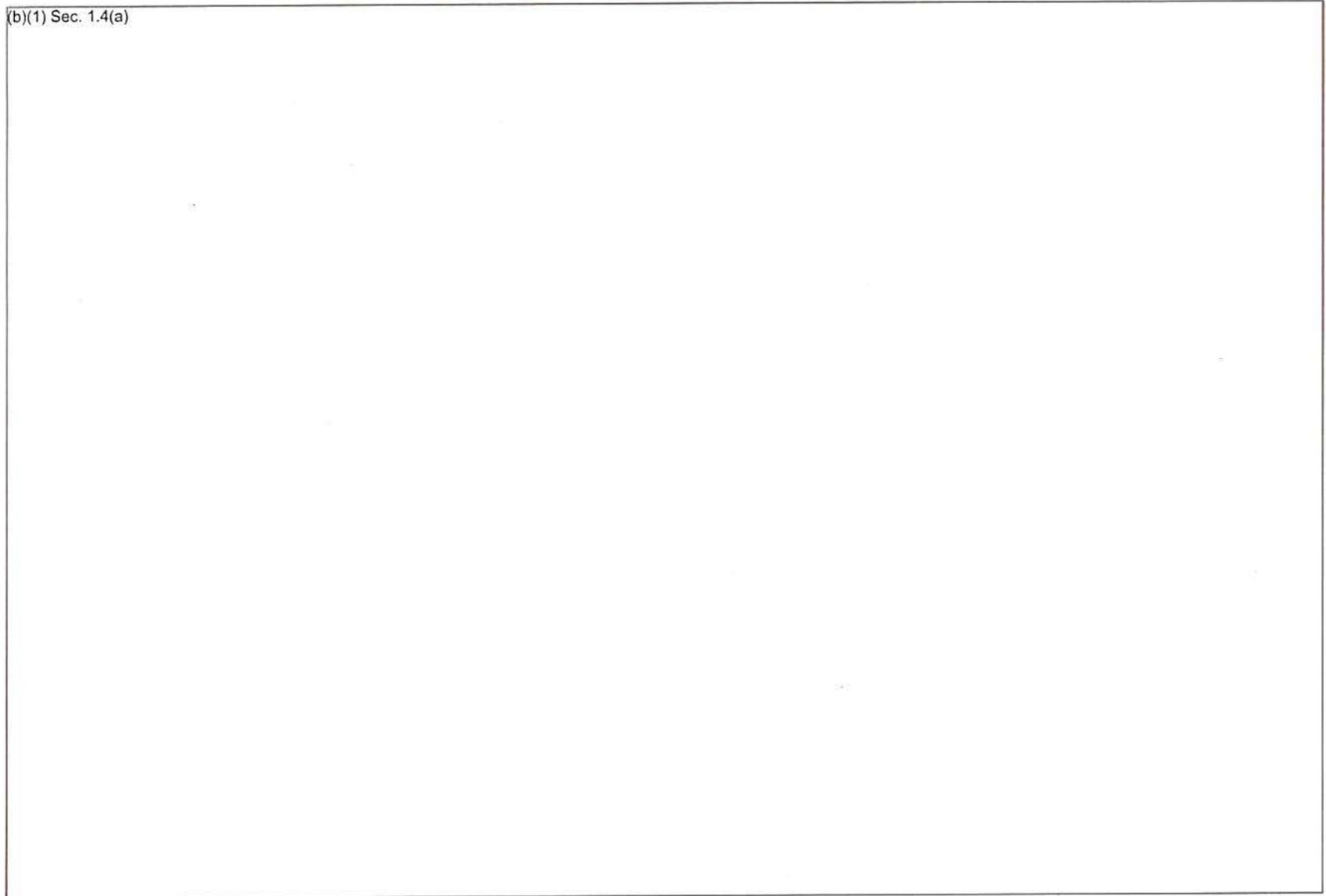
Targeting at USCYBERCOM

(U) **All IAW CJCS Directives. No such thing as a "cyber target"**

(U) **USCYBERCOM Target List examples**

- (S//REL) **F**acility: (b)(1) Sec. 1.4(a)

- (S//REL) **I**ndividual: (b)(1) Sec. 1.4(a)

- (S//REL) **V**irtual: (b)(1) Sec. 1.4(a)

- (S//REL) **E**quipment: (b)(1) Sec. 1.4(a)

- (S//REL) **O**rganization: (b)(1) Sec. 1.4(a)

- (U) For further discussion: Utility of a **N**etwork Target category

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

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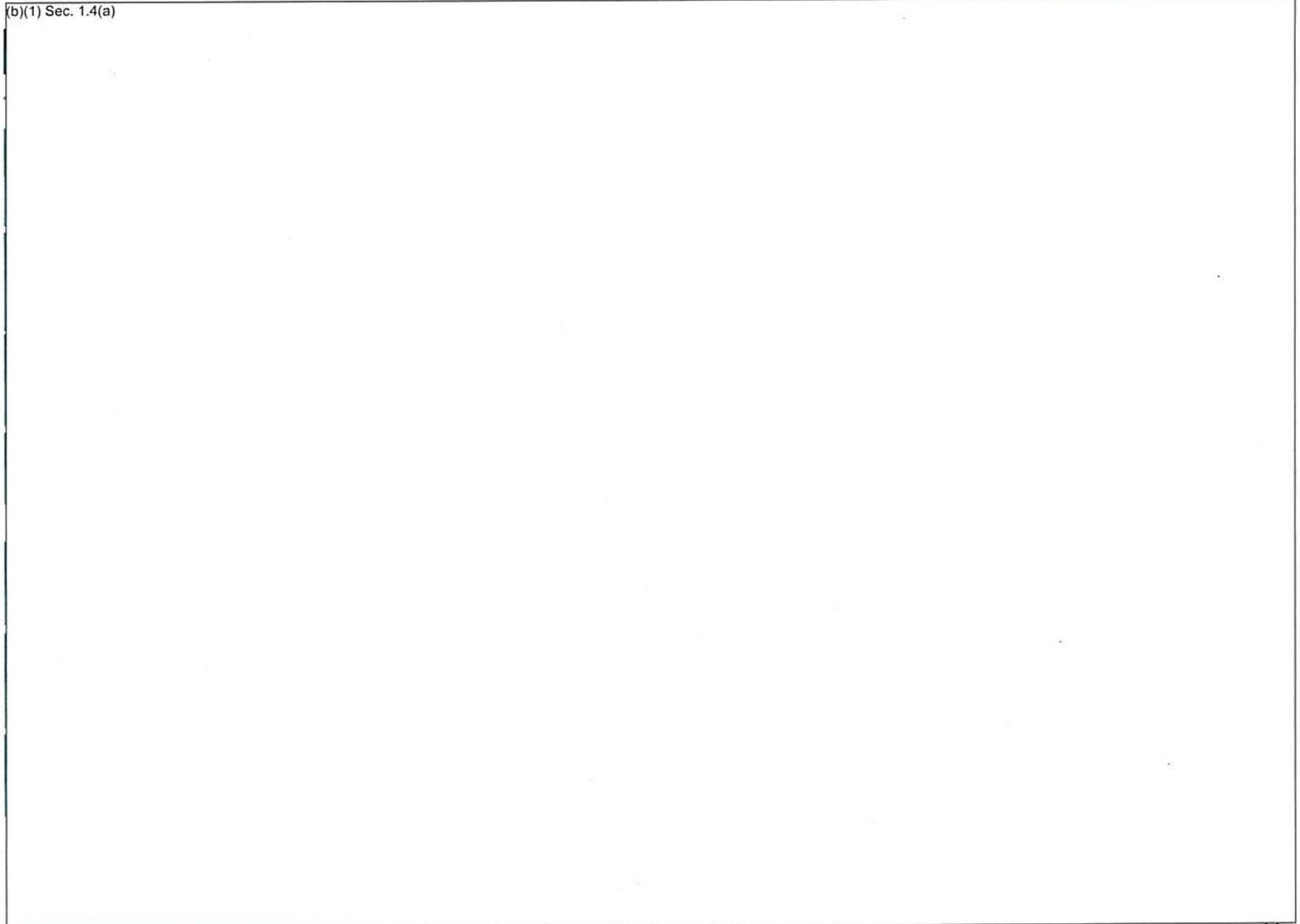
(b)(1) Sec. 1.4(a)

28 Nov 2016 Version 1 J2T

10

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

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

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

28 Nov 2016 Version 1 J2T

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

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

Target Development Relationships

1. End State and Commander's Objective	Taxonomy	Product
	Adversary	**Joint Intelligence Preparation of the Operational Environment**
2. Target Development and Prioritization	**Target System**	**Target Systems Analysis**
	Target System Component	
	Target	
3. Capability Analysis	**Target Element**	**Electronic Target Folder**
	Aim Point	
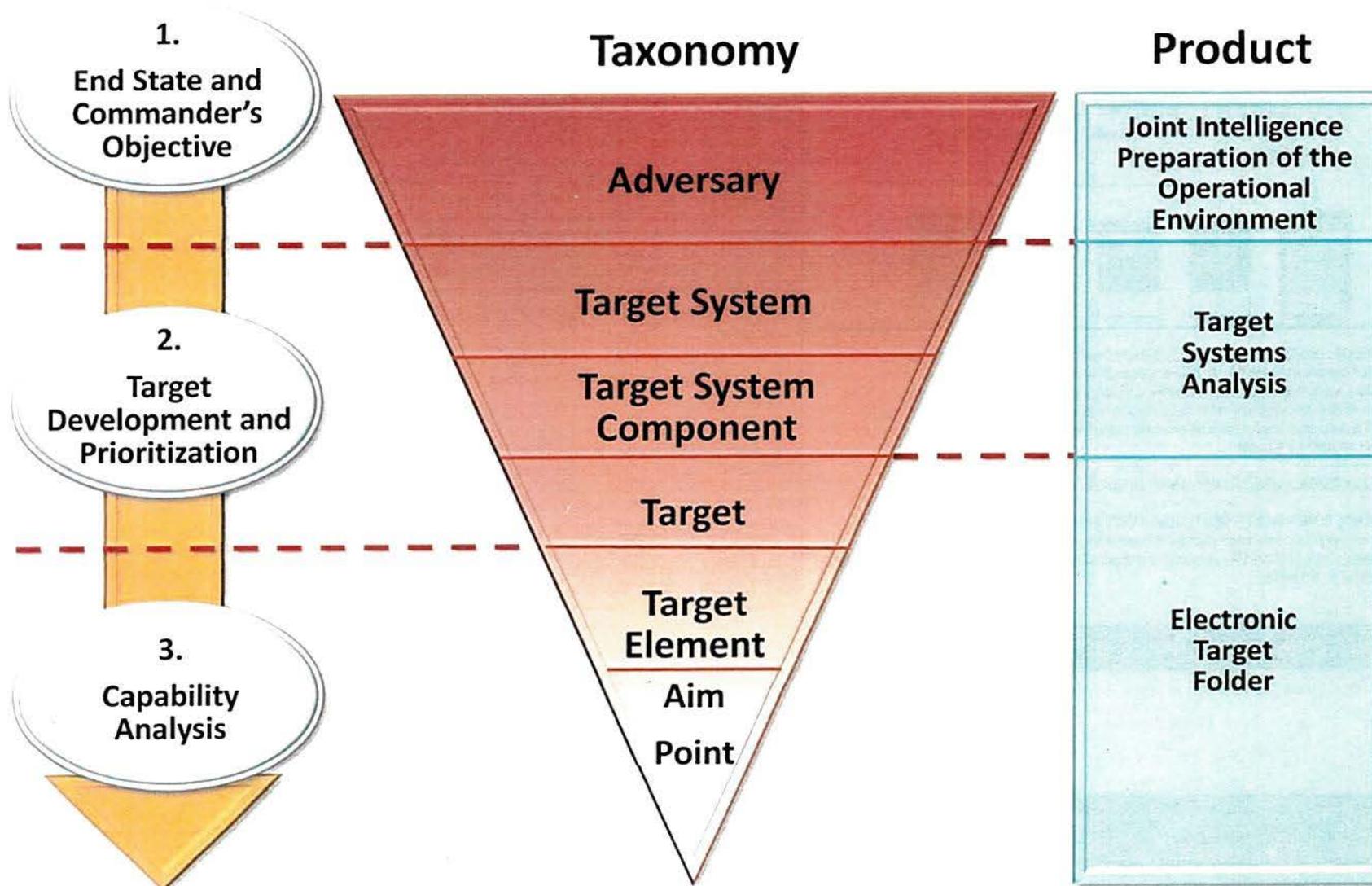
Taxonomy and the 'Art' of Targeting

Taxonomy

Examples

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

1.

End State and Commander's Objective

2.

Target Development and Prioritization

3.

Capability Analysis

Adversary

Target System

Target System Component

Target

Target Element

Aim Point

Success in the "art" of Targeting requires informed application of taxonomy to target elements
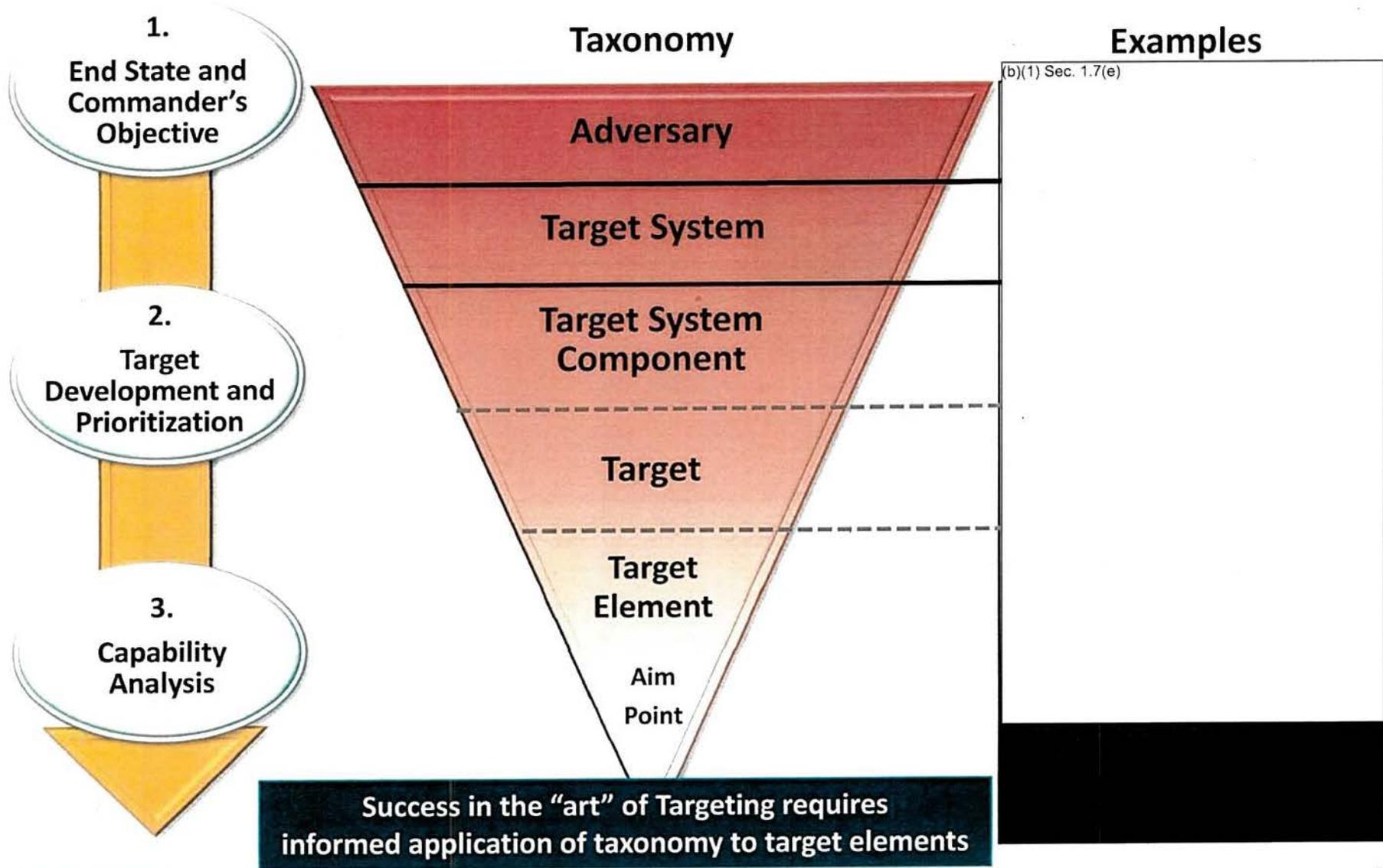
Problem: Adversary VOIP Network

(b)(1) Sec. 1.7(e)
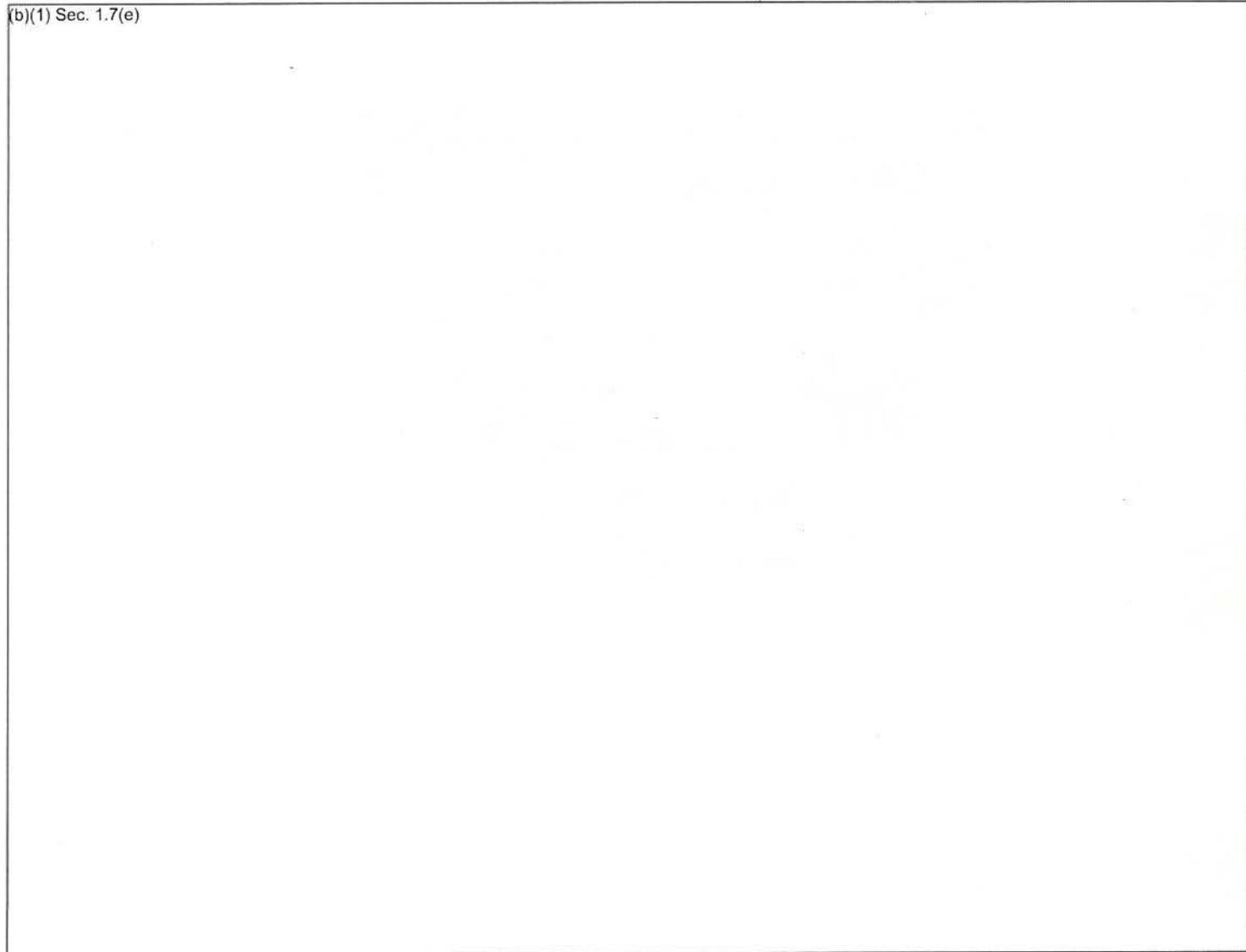
Using Existing Guidance:

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

As a Network Target:

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

Takeaways and Recommendations

- ## Don't use the JTC when you don't need it
  - Examine criteria for what constitutes "fires." When do OCO constitute fires?
  - Take EW problems (SOIs) out of JTC
  - Take MISO problems out of JTC

- ## JTC is useful insofar as it provides a synchronizing function at the operational level of war
  - Targets should be relevant to an operational level commander
    - e.g. (b)(1) Sec. 1.7(e)
  - "Network Target" category would facilitate targeting in the cyber domain
    - Rendering a network as a set of fully developed and associated equipment, facility, virtual, and organization targets will never lead to effective operations.
    - Risk of unbounded network is mitigated by non-lethal nature of OCO
    - Automated system (i.e. MIDB) is not designed for cyber elements. Nor is it necessary.
    - Narrower category than broad, loosely defined "virtual" target category
    - Widely applicable to cyber operations

- ## Joint Targeting Cycle is sound. We must apply it selectively and smartly.

USCC Targeting Way Ahead

- Re-open 'Network' entity discussion with Targeting Enterprise
  - Joint Staff Target Intelligence Working Groups
  - Semi-annual Military Targeting Committee

- Incorporate C-ISIL lessons learned into doctrine
  - Joint Publication 3-60 – Joint Targeting
  - CJCSI 3162 – Battle Damage Assessment

- Coordinate iterative process improvements within USCC
  - Cyberspace Temporary Effects Assessment Report (C-TEAR)
  - Work with J3 to improve Concept of Operation (CONOP) generation

- What we can't change
  - External processes that add overhead to execution (e.g., RAPCO, CAUI)
  - PPD-20 update?