

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Commander's Handbook for Counter Threat Finance



Version 1.0

**Joint Staff, J-7
Joint and Coalition Warfighting
Suffolk, Virginia**

13 September 2011

UNCLASSIFIED//FOR OFFICIAL USE ONLY



DEPUTY DIRECTOR, J-7 JOINT STAFF
JOINT AND COALITION WARFIGHTING
116 LAKE VIEW PARKWAY
SUFFOLK, VA 23435-2697

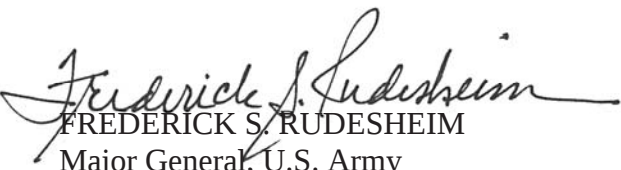
MESSAGE TO JOINT WARFIGHTERS

As Joint Staff J-7 continues to interact with the combatant commands and Services, we recognize that there is very little doctrinal guidance on counter threat finance (CTF). Consequently, we have developed this pre-doctrinal handbook to help joint force commanders and their staffs understand the scope and importance of CTF and provide information and guidance on its process; best practices; planning, execution, and assessment considerations; and resources.

Department of Defense (DOD) CTF activities and capabilities apart from those included under DOD CTF intelligence deny, disrupt, destroy, or defeat finance systems and networks that negatively affect US interests in compliance with all existing authorities and procedures. This includes those activities and capabilities undertaken with other government agencies and/or partner nations. DOD CTF counters financing used to engage in terrorist activities and illicit networks that traffic narcotics, weapons of mass destruction, improvised explosive devices, other weapons, persons, precursor chemicals, and related activities that support an adversary's ability to negatively affect US interests.

The combatant commanders are responsible for planning, executing, and synchronizing DOD CTF day-to-day activities within their respective areas of responsibility or functional areas. Effectively executed CTF greatly enhances joint military operations. However, lessons learned from the field indicate that CTF needs to be improved. CTF missions and processes being used by the joint force today do not effectively keep pace with operational need and are not adequately documented. The current CTF process is ad-hoc, cumbersome, and unresponsive. Data is available in abundance, but the joint warfighter is starving for actionable information required to support operations to the tactical edge. The current process does not support the timely and accurate assessment of collected data, limiting the joint force's ability to conduct meaningful operations.

We hope this handbook stimulates the joint community's thinking about how to address CTF challenges. We encourage you to use the information in this handbook and provide feedback to help us capture value-added ideas for incorporation in emerging joint doctrine, training, and professional military education.


FREDERICK S. RUDESHEIM
Major General, U.S. Army
Deputy Director, J-7, Joint Staff,
Joint and Coalition Warfighting

PREFACE

1. (U) Scope

This handbook provides an understanding of the processes and procedures being employed by joint force commanders (JFCs) and their staffs to plan, execute, and assess counter threat finance (CTF) activities and integrate them into their joint operation/campaign plans. It provides fundamental principles, techniques, and considerations related to CTF that are being employed in the field and are evolving toward incorporation in joint doctrine.

2. (U) Purpose

This handbook provides users with a pre-doctrinal reference describing how to employ CTF principles to achieve operational objectives. Its primary purpose is to improve the US military's use of CTF through educating the user on joint CTF basics, best practices, and processes.

3. (U) Background

a. (U) One of the major lessons learned from military operations in the past decade is that we now face adaptive networked threats that rapidly adjust their operations to offset friendly force advantages in numbers and technology and that these adaptive networks are a world-wide phenomena that posed a wide array of challenges across the range of military operations. To address this threat, it became necessary to provide the joint force with a common understanding of how adaptive networks operated, their strengths and vulnerabilities, and what actions the JFC could undertake to defeat them. Based on a foundation of established doctrinal processes such as joint intelligence preparation of the operational environment and the joint operation planning process, and by leveraging lessons learned, best practices and updated analysis of the near to mid-term threats confronting US forces, the community developed a methodology to directly address the challenges posed by adaptive threats. Known as “attack the network” (AtN), it is a focused approach to understanding and operating against a well-defined type of enemy activity—such as terrorism, insurgency, organized and criminal actions—that threatens stability in the operational area and is enabled by a network of identifiable nodes and links.

b. (U) AtN is lethal and nonlethal actions against networks conducted continuously and simultaneously at multiple levels (tactical, operational, and strategic) that capitalize on or create key vulnerabilities and disrupt activities to eliminate the enemy's ability to function in order to enable success of the operation and campaign. The AtN methodology is designed to enable a joint force staff to enhance its understanding of how an enemy network operates and apply the resources needed to disrupt its ability to efficiently and effectively conduct its activities.

Preface

c. (U) Every network has key activities that enable it to exist, conduct operations, and adapt to environmental changes. This handbook focuses on disrupting one of the key functions – finance. By denying the network easy access to funds, we make it more difficult for the network to resource its operations and its freedom of action and movement in the area of operations. The JFC, in cooperation with interagency, host nation and multinational partners, can engage in a wide range of strategic to tactical activities to disrupt the enemy network’s ability to reliably fund and resource their operations and deny them the operational flexibility they need to adapt and continue to exist.

d. (U) The Department of Defense shall work with other US Government departments and agencies and with partner nations to deny, disrupt, or defeat and degrade adversaries’ ability to use global licit and illicit financial networks to negatively affect US interests.

4. (U) Content

a. (U) Although not without historical precedent, the idea of CTF has emerged from the experiences gained during US military operations in Iraq and Afghanistan. As a result, the research and the examples used throughout this handbook draws primarily from experiences in Iraq and Afghanistan, but proposes potentially valuable solutions to the JFC in any operational area.

b. (U) Specifically, this handbook provides:

(1) (U) Fundamental background information on CTF, its objectives, and required capabilities;

(2) (U) Considerations for developing visibility of planned and ongoing related activities and coordination with potentially numerous, non-military stakeholders;

(3) (U) A discussion of specific training requirements for effective planning, execution, and assessment of CTF; and

(4) (U) A compilation of current best practices that also may serve as a bridge between current practices in the field and their migration into doctrine.

5. (U) Development

CTF, as a means to attain operational objectives, is not currently addressed in joint doctrine. This handbook was developed to codify, at the operational level, practices emerging to fill this existing shortfall. Extensive research into organizations, processes, policies, and regulations that govern the execution of CTF is the foundation of this handbook. More importantly, development included close coordination with, and significant input from, both civilian and military experts. The content was regularly vetted with these experts to assure relevance and accuracy of both theory and practice.

As a result, this handbook represents the current state of best practices and offers recommended solutions to improve the JFC's ability to conduct CTF.

6. (U) Application

This handbook is designed to provide the joint community with essential information on the rationale for CTF use, principles for using CTF, and lessons learned from how this concept has been employed in past and ongoing operations. Although this handbook contains extracts from some doctrinal and pre-doctrinal publications, it is not approved joint doctrine. Rather, it is a non-authoritative supplement to the current, extremely limited, documentation on the establishment of mechanisms to deny, disrupt, destroy, or defeat funding and value transfer items to adversaries to achieve operational objectives. It offers some useful techniques, processes, and procedures that can be used in the combatant commands by JFCs and their staffs. More importantly, it acknowledges the role, resources, and implications for achieving operational objectives in the presence of the multiple agencies and organizations involved in financial operations that are beyond the formal command and control of military commanders.

7. (U) Contact Information

Comments and suggestions on this important topic are welcome. The Deputy Director, J-7 Joint Staff, Joint and Coalition Warfighting, Joint Doctrine Support Division points of contact are Mr. Marc Halyard, at 757-203-5508 and E-mail marc.halyard@hr.js.mil; and Mr. Chuck Shaver at 757-203-6062 and E-mail: charles.shaver.ctr@hr.js.mil.

Intentionally Blank

TABLE OF CONTENTS

	PAGE
EXECUTIVE SUMMARY (U).....	ix
CHAPTER I	
OVERVIEW (U)	
• Introduction (U)	I-1
• Financial Capability of Adversary Groups (U)	I-4
• Joint Force Commander's Benefit from Counter Threat Finance (U).....	I-5
• Purpose: Why this Handbook is Necessary (U)	I-6
• Counter Threat Finance Defined (U).....	I-6
• International/Trans-National/Regional Threat Finance Collection Priorities (U)	I-7
CHAPTER II	
ROLES AND RESPONSIBILITIES (U//FOUO)	
• Introduction (U).....	II-1
• Department of Defense Roles and Responsibilities (U//FOUO)	II-1
• Department of Defense Organizations (U//FOUO)	II-3
• United States Government Agencies (U)	II-6
• Intergovernmental Organizations (U)	II-17
CHAPTER III	
PLANNING CONSIDERATIONS (U)	
• Introduction (U)	III-1
• Military Planning and Mission Partners (U)	III-2
• Counter Threat Finance Limitations and Considerations during the Joint Operational Planning Process (U)	III-3
• Staff Estimates (U)	III-6
• Environments (U)	III-6
• Planning Considerations for the Joint Force Commander (U)	III-8
• The Counter Threat Finance Organization (U)	III-12
CHAPTER IV	
OPERATIONS (U)	
• Introduction (U)	IV-1
• Unified Action (U)	IV-1
• Differences between Military and Interagency Participants (U)	IV-2
• Command and Control (U)	IV-4
• Threat Finance Cell (U)	IV-5
• Operational Area (U)	IV-9
• Types of Activities and Operations (U)	IV-10

Table of Contents

• Military Support Tasks to Counter Threat Finance (U)	IV-11	
• Operations Reporting (U)	IV-13	
• Operations Considerations for the Joint Force Commander.....(U)		IV-14
 CHAPTER V		
INTELLIGENCE AND FINANCIAL INFORMATION (U//FOUO)		
• What the Joint Force Commander Needs to Know (U//FOUO)	V-1	
• Planning (U//FOUO)	V-4	
• Collection (U//FOUO)	V-6	
• Processing and Exploitation (U//FOUO)	V-8	
• Analysis and Production (U//FOUO)	V-9	
• Dissemination and Integration (U//FOUO)	V-10	
 CHAPTER VI		
ASSESSMENT (U)		
• Background (U)	VI-1	
• Metrics (U)	VI-2	
• The Focus of Assessment (U)	VI-4	
• Strategic Metrics Preparation (U)	VI-5	
• Assessment Considerations for the Joint Force Commander (U)	VI-7	
• Assessment Framework (U)	VI-8	
 CHAPTER VII		
OPERATIONAL IMPLICATIONS (U)		
• General (U)	VII-1	
• Doctrine (U)	VII-1	
• Organization (U)	VII-3	
• Training (U)	VII-4	
• Materiel (U)	VII-5	
• Leadership and Education (U)	VII-5	
• Personnel (U)	VII-6	
• Facilities (U)	VII-6	
 APPENDIX		
A Collection Guidelines (U)	A-1	
B Financial Institutions and Transfer Systems (U)	B-1	
C Analytical Techniques (U//FOUO)	C-1	
D Illustrative Measures of Effectiveness (U)	D-1	
E Training and Education (U)	E-1	
F References (U)	F-1	
G Endnotes (U)	G-1	

GLOSSARY

Part I	Abbreviations and Acronyms (U)	GL-1
Part II	Terms and Definitions (U)	GL-5

FIGURE

I-1	(U) Example Activities that Source Adversaries	I-3
I-2	(U) Financial Capability of Adversary Organizations	I-4
C-1	(U) Notional Criminal/Terrorist Enterprise Business Model	C-1

Intentionally Blank

EXECUTIVE SUMMARY (U) COMMANDER'S OVERVIEW

- (U) Complements and supplements (rather than supplants) extant joint doctrine for planning, execution, and assessment of counter threat finance (CTF) operations at the operational level
- (U) Describes the elements of CTF including the capabilities required for implementation
- (U) Introduces planning considerations for incorporation of CTF into joint operation/campaign planning
- (U) Identifies key stakeholders and potential partners in implementing CTF recognizing the need for an inclusive, holistic approach
- (U) Addresses assessment and the joint implications of conducting CTF
- (U) Identifies the training requirements for implementation of CTF
- (U) Provides recommendations and identifies best practices as a baseline for further development and refinement of CTF
- (U) Discusses the operational implications of CTF

(U) Scope and Purpose

(U) This handbook provides an understanding of the processes and procedures being employed by joint force commanders (JFCs) and their staffs to plan, execute, and assess counter threat finance (CTF) activities and integrate them into their joint operation/campaign plans. It provides fundamental principles, techniques, and considerations related to CTF that are being employed in the field and are evolving toward incorporation in joint doctrine.

(U) This handbook provides users with a pre-doctrinal reference describing how to employ CTF principles to achieve operational objectives. Its primary purpose is to improve the US military's use of CTF through educating the user on joint CTF basics, best practices, and processes.

(U) Overview

(U) **Counter threat finance** (CTF) refers to the activities and actions taken by the Department of Defense (DOD) and other United States Government (USG) organizations to deny, disrupt, destroy, or defeat threat finance systems and networks that negatively affect US interests in compliance with all existing authorities and procedures. This

Executive Summary

includes persons and entities that provide financial and material support to illicit networks such as terrorists, insurgents, drug traffickers, weapon traffickers, human traffickers, or corrupt government officials that are attempting to undermine their own governments or efforts of the host nation (HN), coalition, or US forces.

(U) DOD, interagency, and international partners worldwide have concluded that by countering threat finance activities, they can disrupt the finance process used by adversary groups and thereby weaken or even destroy their viability. Effective CTF operations depend on developing an understanding of the functional organization of the adversary, the adversary's financial capabilities, operating methods, identifying the adversary's operating areas and detecting and identifying the sources of funding.

(U) The ability of an adversary to raise funds is based upon their requirement to perform the actions and activities necessary to generate and obtain funding which may leave vulnerabilities which are exploitable

(U) JFCs have long understood the necessity and value of attacking an adversary's military supply lines. CTF provides an analogous means of attacking modern, irregular adversaries.

(U) Finances are the lifeblood of adversary networks. Denying the adversary its finances makes it harder, maybe impossible, for the adversary to pay, train, arm, feed, clothe, gather information and produce the propaganda which supports the fighters. Countering an adversary's finances can have a significant impact on the organization's morale. CTF can increase costs and risk for the adversary.

(U) Roles and Responsibilities

(U) The use of financial intelligence as a methodology to identify and disrupt terrorist organization has had significantly increased across the Intelligence Community (IC). CTF responsibilities are vested and addressed at the highest levels of the USG. The **National Security Council** is charged with developing policy and identifying, assessing, and coordinating interagency actions, to counter threat finance that might potentially or directly impact the US. .

(U) The **Department of Defense (DOD)** has a multiple supporting roles in the CTF arena. The senior DOD leadership has recognized the significance, both strategically and tactically, of a capable and robust CTF posture. United States Special Operations Command is the primary synchronizing organization for CTF operations and activities. The **Under Secretary of Defense, Intelligence** maintains responsibility for all DOD intelligence matters related to CTF.

(U) DOD Directive (**DODD**) **5205.14**, “**DOD Counter Threat Finance Policy**,” dated August 19, 2010, establishes CTF as a DOD mission and assigns CTF responsibilities within DOD.

(U) The **Defense Intelligence Agency**, under the authority, direction, and control of the USD(I), is responsible for providing the DOD CTFI contribution to foreign intelligence and counterintelligence as part of the DIA mission

(U) **United States Special Operations Command** has been charged with synchronizing the CT plans of the six geographic combatant commands.

(U) **Combatant Commands** have been charged with planning, executing, and synchronizing day-to-day CTF activities within their respective AORs or functional areas.

(U) All members of the **Intelligence Community (IC)** have a role in CTF, but that role varies from member to member. Several IC members are tasked with both the collection of intelligence and enforcing federal law.

(U) The **Treasury Department** also enhances national security by implementing economic sanctions against foreign threats to the US, identifying and targeting the financial support networks of national security threats, and improving the safeguards of US financial systems.

(U) The **Department of State** has several bureaus and offices that manage various programs and activities that help combat terrorist financing.

(U) The **Department of Justice** has the lead responsibility for investigating and prosecuting terrorist acts, including all forms of material support to terrorist organizations.

(U) **Department of Homeland Security** has a supporting role in tracking terrorist financing and conducting related investigations within the US and select overseas activities.

(U) Threat financing networks are global, so the US has entered into several agreements to improve and facilitate international organizations' CTF efforts. The **United Nations** is one of the key international entities in the fight against terrorist organizations and networks. The **Financial Action Task Force** is an intergovernmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing. **The Egmont Group of Financial Intelligence Units**, cooperate, especially in the areas of information exchange, training, and the sharing of expertise to improve cooperation in the fight against money laundering and the financing of terrorism. The **International Criminal Police Organization** facilitates cross-border police co-operation, and supports and assists all organizations, authorities and services whose mission it is to prevent or combat international crime.

(U) Planning Considerations

(U) CTF requires the integration of the efforts of disparate organizations in a whole-of-government approach in a complex environment.

(U) Joint operation/campaign plans and operation orders (OPORDs) should be crafted to recognize the core competencies of various agencies and military activities be coordinated and resources integrated, when and where appropriate, with those of others to achieve the operational objectives. The JFC and staff need to consider the non-military options being developed, especially as they relate to CTF. Because the JFC will issue coordination instructions as part of initial guidance, identification of mission partners is a critically important part of initiation. The JFC and staff need to identify the end states and objectives of various mission partners (including their execution timelines and planning horizons). Course of action development should consider the unique capabilities and authorities of mission partners as well as any gaps they may have, as identified in mission analysis. The JFC should ensure the red cell understands and appreciates the impact CTF can have on an adversary. The JFC should consider if the course of action places mission partners in the best posture for future operations/activities. The **concept of operations** needs to provide sufficient detail to outline coordination mechanisms with other mission partners.

(U) A CTF staff estimate should identify and examine factors that may influence CTF operations, which support and are integrated with tentative COAs.

(U) The JFC and staff need to understand the high-level impact the operational environment will have on CTF activities. This understanding can lead to the creation of a more comprehensive, feasible, and achievable plan

(U) The JFC tasked to support or lead CTF should ensure coordinating authorities, channels, and terms of reference are carefully established and documented,

(U) CTF planning will identify the organizations and entities that will be required to conduct CTF action and activities. CTF organizations may include various combinations of three basic structures: Organic CTF element established within a military staff at the CCMD or JTF level; CTF element comprised of DOD and interagency personnel operating at a foreign deployed location within a military area of operation; CTF element comprised of DOD and interagency personnel operating outside a military operational area, probably at a CCMD HQ.

(U) Operations

(U) CTF tactics, techniques, and procedures can provide enhanced information on the activities, organization, placement, vulnerabilities, and capabilities of an adversary. CTF personnel should ensure that they are aware of all ongoing and planned operations to provide commanders with information that could lead to the engagement of threat financial operators, assets or facilities.

(U) Some targets are better engaged by DOD elements and some CTF targets must be engaged through interagency, multinational or HN organizations. All of the challenges to unified action will clearly hold for CTF.

(U) Differences between military and interagency participants include planning timelines; event/action focused versus system/process focused, tactic, techniques, and procedures/doctrine versus rules of evidence; and rules of engagement versus rules for escalation of force.

(U) When a joint DOD/USG interagency organization is stood up, the chain of command, lines of communication, and tasking authority must be clearly delineated and agreed to prior to the joint CTF organization being deployed

(U) As described in the Counter Threat Finance Roadmap Threat Finance Cell (TFCs) can be established at any level based on available personnel resources. Expertise on adversary financial activities can be provided through the creation of TFCs at brigade HQ and higher. The TFC would include a mix of analysts and subject matter experts on law enforcement, regulatory matters, and financial institutions that would be drawn from DOD and other USG agency resources. The TFC's responsibilities vary by echelon.

(U) Adversary finance organizations can have global reach and are generally not geographically constrained. The JFC might find that much of the threat finance network, including potentially key nodes, will extend beyond the operational area.

(U) Military support to CTF is not a distinct type of military operation. Rather, it represents a military activity against a specific capability of an adversary. Additionally, CTF can support several types of military operations.

(U) Military support tasks to CTF can fall into four broad categories: support civil agency and host nation activities (including law enforcement); direct military actions; intelligence collection; and operations to generate intelligence.

(U) The JFC needs to ensure that routine/conventional reporting from operations is available to intelligence personnel and that the reporting reflects PIRs and other intelligence requirements

(U) Intelligence and Financial Information

(U) Information and intelligence on threat financial networks has the potential to provide JFCs with a better understanding of one of the most important support functions for threat networks. Therefore, the JFC and staff planning efforts should consider threat finance information to enhance the understanding of the operational environment. A review of the baseline intelligence and the JIPOE should be conducted to determine the existing intelligence gaps regarding the adversary's financial networks, operations and

Executive Summary

personalities. If necessary, the J-2 should prepare and submit new or revised PIRs related to threat finance for the JFC's approval when gaps are identified.

(U) Collection operations acquire information about the adversary and other relevant aspects of the operational environment and provide that information to intelligence processing and exploitation elements. Collection disciplines complement each other, and the collection manager should resist favoring or becoming too reliant on a particular sensor, source, system, or technique.

(U) Significant aspects of CTF can be highly specific and technical. Additional processing and exploitation may be required to assist analysts.

(U) Military CTF analysts, especially at the lower levels of command, are focused on using financial information to support targeting.

(U) There is nothing regarding CTF intelligence requiring significant changes to dissemination and integration processes and procedures, but an effort should be taken to ensure the executing unit is included in the dissemination of any resultant intelligence and ensure intelligence is being shared with all appropriate stakeholders.

(U) Assessment

(U) JFCs should know the importance and use of CTF capabilities within the context of measurable results for countering adversaries and should embed this knowledge within their staff. By assessing common elements found in adversaries' financial operations, such as composition, disposition, strength, personnel, tactics, and logistics, JFCs can gain an understanding of what they might encounter while executing an operation and identify vulnerabilities of the adversary.

(U) Metrics on threat finance may appear to be of little value because it is very difficult to obtain fast results or intelligence that can be immediately actionable. Actions against financial networks may take months to prepare, organize, and implement, due to the difficulty of collecting relevant detailed information and the time lags associated with processing, analysis, and reporting findings on threat financial networks.

(U) The JFC's staff should assess the adversary's behaviors based on the JFC's desired end state and determine whether the adversary's behavior is moving closer to that end state.

(U) Preparing a consolidated, whole-of-government set of strategic metrics for threat finance will be extremely challenging.

(U) The JFC and staff should consult with participating agencies and nations to establish a set of metrics which are appropriate to the mission or lines of operations assigned to the CTF organization.

(U) There has been a longstanding need for measures of effectiveness focused on diplomatic, informational military and economic efforts in places prone to conflict. Outcomes, or "effects" indicate the success or failure of project or mission efforts, and seek to measure the attainment (progress toward/away) of conditions that engender stability and self-sustaining peace.

(U) Operational Implications

(U) Full and effective implementation of CTF requires development and adoption of doctrine, organization, training, materiel, leadership, personnel, and facilities (DOTMLPF) solutions. Specifically, more work needs to be done to codify CTF within DOD, analyze existing doctrinal processes and publications to determine needed modification, provide organizational recommendations to support process change, and develop CTF training modules for JFCs, staffs, and subordinate echelons. Changes within the DOTMLPF framework can enhance the effectiveness of CTF operations.

Intentionally Blank

CHAPTER I OVERVIEW (U)

"Money is the oxygen of terrorism."

Colin Powell
7 November 2001

1. (U) Introduction

a. (U) **Counter threat finance** (CTF) refers to the activities and actions taken by the Department of Defense (DOD) and other United States Government (USG) organizations to deny, disrupt, destroy, or defeat threat finance systems and networks that negatively affect US interests in compliance with all existing authorities and procedures. This includes persons and entities that provide financial and material support to illicit networks such as terrorists, insurgents, drug traffickers, weapon traffickers, human traffickers, or corrupt government officials that are attempting to undermine their own governments or efforts of the host nation (HN), coalition, or US forces. In order to fully understand CTF, it is important to understand what threat finance is and how the acquisition, distribution, and management of wealth supports adversaries and their operations. This chapter describes how threat finance works and how to conduct CTF operations. Subsequent chapters provide more depth and detail on various CTF topics.

b. (U) **Threat finance** is the manner in which adversarial groups move and use funds to support their illegal activities or profit from them. It includes the generation, movement, storage, management, control, accountability, distribution, and disbursement of funds and/or valuable commodities that can be traded or converted to money by adversaries.

c. (U) **Finance** refers to the provision of venture or financial capital to another individual, company, or organization, with the expectation that the initial invested principal will be returned with interest, or a specified percentage rate of return; or the provision of funding to another individual, company, or organization; or the provision of loans, trade credit, or similar financial instruments to individuals, companies, or organizations; or the provision of any financial service that promotes, facilitates, or enhances fund-raising, financing, payment, or investment plans, actions, and activities by individuals, companies, or organizations.

d. (U) **Financial instruments refer** to items of value and all forms of currency which are exchangeable for currency, equipment, materiel, weapons, shelter, transportation, communications, services, favors, and other forms of support. Items of value include, but are not limited to: stolen credit cards or credit card numbers, black market consumer items (e.g., appliances, computers, foodstuffs), counterfeit currency, counterfeit documents, stocks, bonds, vehicles, real estate, facilities, cash value cards, e-currencies, jewelry and precious metals (especially gold), fuel and repair parts, building materials, livestock, weapons, drugs, which can be transferred and converted to cash at the time and place of the adversary's choosing. Sources can be both licit and illicit.

e. (U) **Financier** is an individual, company, or organization that provides venture or financial capital to another individual, company, or organization, with the expectation that the initial invested principal will be returned with interest, or a specified percentage rate of return; provides funding to another individual, company, or organization; or that extends loans, trade credit, or underwrites similar financial instruments to other individuals, companies, or organizations; or that provides any financial services that promote, facilitate, or enhance fund-raising, financing, payment, or investment plans, actions, and activities by individuals, companies, or organizations; or a broker, accountant, or money-service provider that handles money, particularly in large quantities.

f. (U) There is a direct correlation between a adversary's level of activity and its ability to pay for that activity. It is critical for the US and its multinational partners around the world to counter the possible sources, methods, and effects of threat finance activities.

g. (U) Examples of activities that provide sources of funds to adversary organizations include but are not limited to those listed in Figure I-1.

h. (U) DOD, interagency, and international partners worldwide have concluded that by countering threat finance activities, they can disrupt the finance process used by adversary groups and thereby weaken or even destroy their viability. Effective CTF operations depend on developing an understanding of the functional organization of the adversary, the adversary's financial capabilities, operating methods, identifying the adversary's operating areas and detecting and identifying the sources of funding. For example, in Afghanistan, adversary organizations are receiving funds and financing from a wide variety of sources including drugs, smuggling, foreign governments, local population, foreign private donors, nongovernmental organizations (NGOs), companies such as cell phone carriers, and even multinational and USG contractors operating in the environment. The proliferation of sources means their finances are less susceptible to CTF activities (but not impervious), because action against one source can be offset by increased revenues from others.

i. (U) CTF actions use elements of the economic instrument of national power as additional tools as well as law enforcement, regulatory and political methods to create desired effects and, ultimately, achieve military and national strategic end state.

Example Activities that Source Adversaries	
• Illegal taxation	• Black market operations
• Illegal roadblocks	• Credit card fraud and identity theft
• Counterfeiting currencies, pharmaceuticals, alcohol and tobacco products, and other goods and materials	• Smuggling (e.g., drugs, weapons contraband, foreign fighters, human smuggling, highly taxed goods including alcohol and tobacco, restricted goods, precursor chemicals)
• Take over and sale of homes	• Prostitution
• Sale of digital video disks	• Extortion and protection rackets
• Embezzlement or diversion of government funds by adversary personnel in positions of authority, or by compromised government officials	• Embezzlement or diversion of foreign aid materials and funds by adversary personnel in positions of authority, or by compromised government officials
• Kidnapping	• Theft and sale of fuel
• Loan fraud	• Robbery
• Contract fraud and bid rigging	• General theft
• Loans to farmers involved in illegal drugs	• Convoy hijacking
• Government sponsors	• Exploitation of government grants
• In-person and internet solicitation	• Applications for micro loans
• Local donors	• Investment in financial markets
• Foreign donors	• Investments in local businesses
• Diaspora community donations	• Front company operations
• Exploitation of charities, nongovernmental organizations, and religious organizations	• Ownership and management of legitimate businesses used for money laundering purposes
• Vehicle theft and resale	• Bank and payroll theft
• International solicitation	• Zakat abuse (Welfare contributions to poor and deprived Muslims)

(U) Figure I-1. Example Activities that Source Adversaries

2. (U) Financial Capability of Adversary Groups

a. (U) The ability of an adversary to raise funds is based upon their requirement to perform the actions and activities necessary to generate and obtain funding which may leave vulnerabilities which are exploitable (see Figure I-2). Critical requirements to support the capability to raise funds can be correlated to the following:

Financial Capability of Adversary Organizations	
• Successfully raise/solicit funds; control and manage, account for, store, transfer, distribute, and disburse funds	• Disburse funds and make payments on time with a minimal threat of interdiction and a degree of accountability
• Meet expected and unforeseen financial obligations	• Transfer funds quickly and with minimal threat of interdiction
• Maintenance of a reliable and steady flow of income, preferably from multiple income streams	• Grow and expand a profitable, self-sustaining threat organization over time and space
• Withstand temporary financial setback by maintaining a cash/asset reserve	

(U) Figure I-2. Financial Capability of Adversary Organizations

(1) (U) Having sufficient numbers of proficient and reliable personnel with the skills, training, education or experience to perform the actions that can successfully develop the organization, methods and infrastructure necessary to raise or solicit funds; transfer, control and manage funds; account for funds; provide security for, store, transfer, distribute, and disburse funds.

(2) (U) The development of financial operating methods capable of circumventing and exploiting laws, regulations, sanctions, and designation by law enforcement and regulatory agencies. This includes developing and maintaining a secure means of communication and developing a viable operational security (OPSEC) process for the adversary.

(3) (U) Having or creating a secure financial operating environment to include obtaining access to intelligence on government operations.

(4) (U) Infiltration or corruption of government agencies or compromise of government officials responsible for law enforcement or regulatory actions against an adversary.

(5) (U) Infiltration or control of government agencies or compromise of government officials responsible for the control of government assets and financial resources that can be exploited by adversaries.

(6) (U) Identifying and obtaining access to financial resources that can provide a reliable and steady flow of income, preferably from multiple income streams, which can provide sufficient funds to pay for overhead and fixed expenses, operational expenses, and special expenses that are incurred by the adversary.

(7) (U) The ability to maintain a cash or asset reserve that will allow the group to operate if there is a disturbance in the flow of funds to the group.

(8) (U) Obtaining access to and using financial entities that can transfer funds quickly and with minimal threat of interdiction.

(9) (U) The capacity to grow, and expand, a profitable, self-sustaining threat organization over time and space.

3. (U) Joint Force Commander's Benefit from Counter Threat Finance

a. (U) Joint force commanders (JFCs) have long understood the necessity and value of attacking an adversary's military supply lines. CTF provides an analogous means of attacking modern, irregular adversaries.

b. (U) Finances are the lifeblood of adversary networks. Denying the adversary its finances makes it harder, maybe impossible, for the adversary to pay, train, arm, feed, clothe, gather information and produce the propaganda which supports the fighters. Successfully denying the adversary's finances decreases their ability to conduct operations which oppose and threaten US forces and which challenge US objectives and interests up to and including protecting the Homeland.

c. (U) Countering an adversary's finances can have a significant impact on the organization's morale. Money is one of the strongest recruiting and retention tools that any organization possesses. Money and the means to provide for their families are often the motivation for joining a threat group. The loss of income and the threat group's loss of financial credibility can be devastating to maintaining group membership and recruiting new personnel.

d. (U) CTF can increase costs and risk for the adversary. The adversary needs financing to operate. As CTF operations deny methods, routes, and sources of revenue, the adversary is forced to adjust. In so doing, CTF forces the adversary to make choices that involve greater cost, risk, or that are less aligned with the group's core ideology. As a result of CTF, the adversary is forced to economize by possibly conducting fewer operations, by choosing targets more judiciously, or by adapting to tactics, techniques, and procedures (TTPs) that can be more readily detected and interdicted. CTF may also force the adversary to rely more heavily on the local population to fund its operations. This can serve to divide the adversary from the local population, especially when coupled with effective military information support operations (MISO).

e. (U) CTF, by itself, will almost certainly be insufficient to destroy an adversary's will or capability. It may however, make it harder for the adversary to conduct

Chapter I

operations. It also shows the adversary and its leaders, the JFC will challenge and attack all aspects of the organization's operations.

4. (U) Purpose: Why this Handbook is Necessary

a. (U) Money and other financial resources are usually of critical importance for adversary networks. Without it, adversaries can be incapable of organizing, recruiting, and maintaining the broad infrastructure necessary to run an effective organization. As such, finding the means to quickly and securely raise, launder, transfer, store, and gain access to funds remains a top priority for all terrorist groups.¹

b. (U) Experience has shown the effective employment of CTF requires careful and close synchronization and coordination between DOD, other USG agencies, the HN government, and interorganizational partners. This collaborative working environment should be based on mutual interest, purpose, trust, and commitment to continued and persistent cooperation to successfully achieve unity of effort.

c. (U) The need for a more integrated effort in Afghanistan, for example, was recognized after several years of ad hoc activities and was prompted by the US Civilian-Military Campaign Plan. Thus, this handbook acknowledges the roles, resources, implications, and authorities of the multiple agencies and organizations involved in CTF, as described in Chapter II, "Roles and Responsibilities."

d. (U) Recognizing the need for meaningful and reliable information and support in developing CTF strategies and methodologies, this handbook provides a needed joint context at the operational level and extrapolates CTF lessons learned in one or more operational areas for application on a global basis.

e. (U) For a complementary resource that describes the broader but related topic of integrated financial operations please refer to the *Integrated Financial Operations Commander's Handbook, A Joint Force Guide to Financial Operations*. It provides an understanding of the processes and procedures being employed by JFCs and their staffs in planning, executing, and assessing efforts to integrate USG financial operations into campaign plans. It provides fundamental principles, techniques, and considerations related to those being employed in the field.

5. (U) Counter Threat Finance Defined

a. (U) Department of Defense Directive (DODD) 5205.14, *DOD Counter Threat Finance (CTF) Policy* defines DOD CTF activities and capabilities as:

"DOD activities and capabilities, apart from those included under DOD Counter Threat Finance Intelligence (CTFI), to deny, disrupt, destroy, or defeat finance systems and networks that negatively affect US interests in compliance with all existing authorities and procedures. This includes those activities and capabilities undertaken with other Government agencies and/or partner nations. DOD CTF counters financing used to engage in terrorist activities and

illicit networks that traffic narcotics, weapons of mass destruction (WMDs), improvised explosive devices, other weapons, persons, precursor chemicals, and related activities that support an adversary's ability to negatively affect US interests."

DOD CTFI is defined as DOD intelligence actions, including those undertaken with other USG agencies and/or multinational partners that involve the collection, processing, integration, evaluation, analysis, interpretation, production, and dissemination of intelligence products in support of DOD CTF activities and capabilities.

b. (U) As developed by the CTF community of interest, this handbook's working definition of CTF is:

"the means to detect, identify, deny, destroy, defeat, contain, disrupt, exploit, deter, or dismantle the collection, storage, transmission, distribution, and usage of currency, assets or resources, which support state and non-state threats to US national security."

c. (U) CTF activities include, but are not limited to, countering narcotics trafficking, proliferation activities WMD and WMD networks, trafficking in persons, weapons trafficking, precursor chemical smuggling, terrorist revenue and logistics, and other such activities that generate revenue through illicit networks. In addition, CTF activities are used to counter funds generated by licit means but used to fund adversary operations.

"...members of violent extremist organizations (VEOs) from the Middle East remain active in Latin America and the Caribbean and constitute a potential threat. Hezbollah supporters continue to raise funds within the region to finance their worldwide activities."

General Douglas M. Fraser
Commander, United States Southern Command
5 April 2011

6. (U) International/Trans-National/Regional Threat Finance Collection Priorities

a. (U) Traditional TTPs for conducting US military combat operations do not necessarily apply to the irregular threats posed by non-state actors in the threat finance arena. Strategies for detecting and defeating a conventional adversary's combat power do not necessarily apply to finding a clandestine network, illicit financier, or even recognizing the trappings of threat finance indicators. Critical to both TTP development and execution is an understanding of what is needed in terms of information and the establishment of key collection priorities. Listed below are some of the basic collection priorities. A more detailed breakdown of these collection priorities is included in Appendix A, "Collection Guidelines."

(1) (U) Who are the financiers and donors that provide financial resources, services, and other items of value to adversaries and what are their motivations?

(2) (U) What methods do adversaries use to raise, launder, transfer, store, secure, manage, account for, gain access to, distribute, or disburse funds?

(3) (U) Which of these fundraising methods are local?

(4) (U) Which of these fundraising methods is most critical to the financial operations of the threat group?

(5) (U) Who are the money service providers and facilitators in the group?

(6) (U) Who are the financial managers, financial planners, investment managers, financial security operators, fund raisers, fund and tax collectors, bookkeepers, auditors, couriers, and financial facilitators, in the group?

(7) (U) How are adversaries managing and controlling their money?

(8) (U) How are adversary personnel moving their money between operational areas and safe havens or across areas of responsibility (AORs)?

(9) (U) Where and how are the adversary personnel spending their money?

b. (U) Focusing on the identification of threat finance actions, recognizing the indicators of active adversary finance networks and individuals, and emphasizing the importance of disrupting and dismantling threat finance activities at the lowest possible operational level will provide a positive impact on JFC's operational environment. It will also feed and support the regional and transnational efforts in CTF operations overall.

Terrorist Financing. The Arabian Peninsula remains the most important source of financial support for al-Qa'ida and its affiliates and adherents around the world. This is despite the fact that important progress has been made by some of our Gulf partners, especially Saudi Arabia and the United Arab Emirates (UAE), in disrupting terrorist financial support networks. Other countries in the region have not made the same political commitment to prioritize action against al-Qa'ida terrorist financing activity and, as a consequence, remain relatively permissive operating environments for al-Qa'ida financiers and facilitators. The United States will continue to emphasize disrupting the access of terrorists—especially al-Qa'ida, its affiliates, and its adherents—to sources of financial support. We will continue to push for enhanced unilateral action by these governments and closer cooperation with the United States while retaining our ability to take unilateral action as well.

**National Strategy for Counterterrorism
June 2011**

CHAPTER II

ROLES AND RESPONSIBILITIES (U)

“The Commanders of the Combatant Commands are responsible for planning, executing, and synchronizing DOD CTF day-to-day activities within their respective areas of responsibility or functional areas.”

**Department of Defense Directive 5205.14
DOD Counter Threat Finance (CTF) Policy
19 August 2010**

1. (U) Introduction

Since the 9/11 terrorist attacks in the US, the use of financial intelligence as a methodology to identify and disrupt terrorist organizations has had significantly increased across the Intelligence Community (IC). CTF spans a wide range of actions and activities all having significant implications for the safety, security, and sovereignty of the US. CTF responsibilities are vested and addressed at the highest levels of the USG. The National Security Council (NSC) is charged with developing policy and identifying, assessing, and coordinating interagency actions, to counter threat finance that might potentially or directly impact the US. .

2. (U//FOUO) Department of Defense Roles and Responsibilities

a. (U) The DOD has a multiple supporting roles in the CTF arena. The senior DOD leadership has recognized the significance, both strategically and tactically, of a capable and robust CTF posture. Within its supporting role, the DOD also has a variety of capable organizations with CTF missions. United States Special Operations Command (USSOCOM) is the primary synchronizing organization for CTF operations and activities. The Under Secretary of Defense, Intelligence [USD (I)] maintains responsibility for all DOD intelligence matters related to CTF.

b. (U) CTF has been an essential component against the insurgencies in both Iraq and Afghanistan. Building upon lessons learned from both conflicts, the DOD issued DOD Directive (DODD) 5205.14, “*DOD Counter Threat Finance Policy*,” dated August 19, 2010, which establishes CTF as a DOD mission and assigns CTF responsibilities within DOD.

c. (U) DODD 5205.14 drives the institutionalization and operationalization of CTF within DOD. Since current and future adversaries rely on a number of funding sources to operate, and identifying and thwarting financial supply lines are a proven means of disrupting threats to US national security, CTF is an important capability in DOD and the services. Ultimately, success in CTF will depend on DOD’s ability to integrate with, support, and complement other USG, multinational, and HN activities.

d. (U) The key policy objectives of DODD 5205.14 are:

Chapter II

(1) (U) DOD shall work with other USG departments and agencies and with partner nations to deny, disrupt, or defeat and degrade adversaries' ability to use global licit and illicit financial networks to negatively affect US interests.

(2) (U) DOD shall:

(a) (U) Conduct strategic planning through the Joint Staff and combatant commands (CCMDs), including lines of operations to exploit and counter adversaries' finance networks in coordination with the Under Secretary of Defense for Policy [USD(P)] via the Chairman of the Joint Chiefs of Staff.

(b) (U) Develop and include integrated capabilities in force planning constructs to exploit and counter financial networks that negatively affect US interests.

(c) (U) Support other USG agencies' CTF activities in accordance with applicable laws, regulations, policy, and memorandums of agreement and understanding.

(d) (U) Establish early integration of CTF interagency representatives into the DOD planning process, when appropriate.

(e) (U) Coordinate, through USD(I), on intelligence issues related to DOD CTF and enhance and extend Defense Intelligence Enterprise capabilities to support DOD CTF activities and CCMD operations, policy, and acquisition.

(f) (U) Establish appropriate management oversight of DOD CTF activities.

(g) (U) Conduct all DOD CTFI activities in accordance with DODD 5240.01.

e. (U//FOUO) The *DOD Counter Threat Finance Roadmap* explains the strategic intent and identifies the five key objectives behind DODD 5205.14. Those objectives are:

(1) (U//FOUO) **Support a Whole-of-Government, Full-Spectrum Approach to CTF.** In full coordination with the National Security Staff's (NSS) TF Sub-Counterterrorism Security Group (CSG), DOD will support interagency CTF efforts, serving as a provider of resources including funding, personnel, and technology to support interagency efforts aimed at counterterrorism (CT), counternarcotics, and countering transnational organized criminal activities.

(2) (U//FOUO) **Enhance CTF Support for Law Enforcement against Top-Priority Transnational Threats.** DOD will support the efforts of US law enforcement partners tasked to find, follow, freeze, and seize illicit funds; prosecute financiers; and target complex criminal revenue-generating and laundering activities. Such support will

aid the broader national security interest of disrupting and dismantling illicit financing, global drug trafficking, and transnational organized crime networks.

(3) (U//FOUO) **Organize, Train, and Support Threat Finance Cells (TFCs).** In accordance with the guidance contained in DODD 5205.14, each CCMD will be responsible for creating a dedicated CTF capability. In the event of a major combat operation, TFC personnel will be in a position to deploy and augment in-country combat support elements. In peacetime environments, DOD will provide financial and analytical support to interagency CTF efforts. Additionally, US Special Operations Command (USSOCOM) will coordinate activities to improve DOD CTF doctrine, organization, training, and equipment.

(4) (U//FOUO) **Develop Core DOD CTF Capabilities.** DOD will develop or enhance the following CTF capabilities in full coordination with the NSS's TF Sub- CSG and in partnership with the interagency CTF community:

(a) (U//FOUO) **CTF Operational Capabilities:** Support USG agencies' capabilities, both with DOD authorities and with the support and guidance of law enforcement, intelligence, diplomatic, and policy partners.

(b) (U//FOUO) **Financial Order of Battle:** Create a comprehensive and standardized framework for targeting an adversary's financial infrastructures for major vulnerabilities.

(c) (U//FOUO) **CTF Intelligence (CTFI):** Work with partners in the IC to expand the collection, analysis, dissemination, and exploitation of CTF intelligence.

(5) (U//FOUO) **Define and Incorporate CTF into DOD Doctrine, Strategy, and Operational Planning.** The importance and use of CTF capabilities within the context of measureable efforts for countering our adversaries must become embedded knowledge within DOD. CTF concepts and doctrine will be applied throughout the full range of relevant DOD intelligence, planning, and operational activities, where appropriate.

3. (U//FOUO) Department of Defense Organizations

a. (U) While the DOD is the lead agency for military operations against terrorist organizations and states that sponsor them, it has a supporting role in countering threat finance. According to DODD 5205.14, the DOD is responsible for supporting USG entities and partner nations in their efforts to "deny, disrupt, or defeat and degrade adversaries' ability to use global licit and illicit financial networks to negatively affect US interests."

b. (U) **Defense Intelligence Agency (DIA).** DIA, under the authority, direction, and control of the USD(I), is responsible for providing the DOD CTFI contribution to foreign intelligence and counterintelligence as part of the DIA mission. DIA, shall:

Chapter II

(1) (U) Satisfy the DOD CTFI requirements of the Secretary and Deputy Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the Director of National Intelligence (DNI).

(2) (U) Provide the DOD CTFI contribution to national foreign intelligence and counterintelligence.

(3) (U) Plan, manage, and execute DOD CTFI operations during peacetime, crisis, and war.

(4) (U) Serve as the intelligence conduit for the CCMDs within the interagency and as the DOD lead for coordinating DOD CTFI support to meet CCMD requirements; lead efforts to align analysis, collection, and intelligence, surveillance, and reconnaissance activities with all operations; and link and synchronize defense and national intelligence capabilities.

(5) (U) Periodically review capabilities of CTFI activities and recommend improvements to the USD(I).

(6) (U) Consolidate selected DOD CTF elements under a new Joint Intelligence Task Force for CTF (JITF-CTF) under DIA.

c. (U//FOUO) **United States Special Operations Command.** USSOCOM has been charged with synchronizing the CT plans of the six geographic combatant commands (GCCs) as components of a global campaign and submitting the combined information to the Joint Chiefs of Staff. The USSOCOM Threat Finance Exploitation Branch was established to “coordinate and integrate military operations...that lead to the detection, identification, targeting, disruption, or destruction of terrorist financial support systems.” In 2004, it hosted the first Terrorism Finance Joint Planning Group, which began to outline ways CCMDs can disrupt terrorist financing. Due to the connection between narcotics trafficking and threat finance, the USSOCOM Counter Narcoterrorism Program “provides US Special Operations Forces to GCCs, ambassadors, and other USG agencies to address the nexus of this crime and the terrorism it funds. Recent Counter Narcoterrorism Program efforts include SOF-led training and security assistance to partners in Colombia and Panama.”

d. (U//FOUO) **Combatant Commands.** The CCMDs have been charged with planning, executing, and synchronizing day-to-day CTF activities within their respective AORs or functional areas. Each CCMD was directed to establish a threat finance unit that analyzes and exploits financial intelligence. Because threat financing varies significantly in different operational areas, each CCMD threat finance unit will likely have a somewhat different organization and focus.

(1) (U//FOUO) **CCMD Threat Finance Capability.** Each CCMD has a CTF entity that analyzes and exploits financial intelligence that is relevant to its geographic

region or functional area. For example, USSOUTHCOM focuses on narcotics trafficking, while USCENTCOM's strategy centers on terrorist and insurgent activity. However, each CCMD may have a different title for its CTF entity. For instance, USSOCOM calls its entity a TF Exploitation Branch. Each of the TF Exploitation entities are resourced, manned, and used to varying degrees based on the emphasis that is placed on their importance by the GCC, and not all TF Exploitation entities operate at the same level of proficiency.

(2) (U) **The Iraq Threat Finance Cell (ITFC).** The ITFC was established in 2005 with the mission "to improve US efforts to gather, analyze, and disseminate intelligence relating to the financial networks of insurgents, terrorists, and militias in Iraq."² This includes adversary groups like Al-Qaeda and the Mahdi Army of anti-American cleric Moqtada al-Sadr, among others. Although originally co-chaired by the Department of Treasury and USCENTCOM, it is now headed by the DOD. ITFC is made up of personnel from a number of USG agencies, including the Federal Bureau of Investigation (FBI), the Internal Revenue Service (IRS) and the Joint Interagency Coordination Group (JIACG), among others. The ITFC is based in Baghdad. Though specific methods and sources are unavailable at the unclassified level, anecdotal evidence suggests that the ITFC's CTF efforts have been successful. In January 2008, Robert M. Kimmitt, Deputy Secretary of Treasury, cited an example of the ITFC assisting Multinational forces in exploiting financial data obtained from raids in Iraq as evidence that JFCs in Iraq have "come to rely" on the ITFC financial analysis "to help combat the Iraqi insurgency and disrupt terrorist, insurgent, and militia financial networks." The success of the ITFC has been the basis for the creation of a similar TFC in Afghanistan.

The ATFC has at its disposal the full spectrum of US tools and authorities, including diplomacy, law-enforcement actions, military operations, and targeted financial measures, to go after threat finance in Afghanistan.

**David Cohen,
Assistant Secretary for Terrorist Financing
Department of the Treasury**

(3) (U) **Afghan Threat Finance Cell (ATFC).** Following the success of the ITFC, the NSC established the ATFC in November 2009 with the Drug Enforcement Administration (DEA) designated as lead, Treasury and DOD as co-deputies, and other USG agencies and partner nations participating as required. The ATFC has the "dual mission of disrupting the trafficking networks supporting the insurgents and collecting information on senior Afghan Government officials suspected of corruption.

(a) (U) The ATFC's mission is inextricably linked to countering drug trafficking and the culture of corruption on which threat finance depends. Accordingly, the ATFC focuses on identifying financiers operating throughout Afghanistan "with connections to insurgent activities, drug trafficking and public corruption. The ATFC produces target packages for many of these financiers which are passed to the military and law enforcement officials" for use in prosecuting or designating individuals.

Chapter II

(b) (U) In an effort to build Afghan capability, the ATFC conducts “a vast majority” of its investigations and operations with Afghan counterparts, such as the Sensitive Interdiction Unit, the Public Prosecutors Office, and vetted judges. Many of the target packages that ATFC develops are passed to Afghan counterparts for their assistance and action, as well as to other USG agencies.

4. (U) United States Government Agencies

a. (U) The NSC is responsible for the overall coordination of the interagency framework for combating terrorism, to include disrupting terrorist financing. Under the NSC, a series of committees and working groups develop policy, share information, and coordinate the response to terrorist threats against US interests. The NSC’s TF Sub-CSG has the primary responsibility of ensuring proper coordination on CT financing activities and information sharing among interagency partners, intelligence organizations, and law enforcement communities. It also addresses departmental primacy and jurisdiction in the threat finance arena

(1) (U) One of the primary missions of the NSC TF Sub CSG is the coordination of domestic and international designations of terrorist and their affiliated groups. Each member of the IC can nominate individuals or groups for domestic and international designation. The designation process is time and resource intensive, but can be one of the most effective tools for CTF. A domestic designation leads to the freezing of assets of the individual or group by the Department of Treasury, Office of Foreign Asset Control (OFAC). An international designation, via DOS using a United Nations Security Council Resolution (UNSCR), effectively freezes any terrorist or their associated organizations from using the international banking system. A UNSCR 1267 designation is specific to Al Qaeda and a 1373 designation for all other terrorist organizations. Once a person or group is designated, identifiable assets are to be frozen and banks are not allowed to enter into any financial arrangements with the designated entities.

(2) (U) The NSC TF Sub CSG ensures the equities of each IC member as it relates to both positive and negative impacts of foreign and domestic designations.

b. (U) **The Intelligence Community (IC).** The IC is a coalition of 17 agencies and organizations within the executive branch that work both independently and collaboratively to gather the intelligence necessary to conduct foreign relations and national security activities. As such, all members of the IC have a role in CTF, but that role varies from member to member. Several IC members are tasked with both the collection of intelligence and enforcing federal law. Using task forces, local and state law enforcement work effectively with their federal counterparts. Using all of the federal, state, and local laws in a coordinated effort to target threat finance activities is one of the most effective tools in CTF. Financial gain is the primary motivation behind most crime. Adversaries use illicit profits to fund terrorist activities. Law enforcement understands how to target illegal activity and the IC is using law enforcement information to turn it into actionable intelligence.

(1) (U) **Office of the Director of National Intelligence (ODNI).** The DNI serves as the head of the IC, overseeing and directing the implementation of the National Intelligence Program and acting as the principal advisor to the President, the NSC, and the Homeland Security Council for intelligence matters related to national security.

(2) (U) ODNI operates the **National Counterterrorism Center (NCTC)**, which serves as the USG's "central and shared knowledge bank on known and suspected terrorists and international terror groups" and "provides the authoritative database" for the USG terrorist watchlist. The NCTC conducts strategic operational planning for USG CT activities and integrates all instruments of national power, including diplomatic, financial, military, intelligence, homeland security, and law enforcement to ensure unity of effort.

c. (U) **Department of the Treasury.** The Treasury Department is the executive agency responsible for promoting economic prosperity and ensuring the financial security of the United States. The Treasury Department also enhances national security by implementing economic sanctions against foreign threats to the US, identifying and targeting the financial support networks of national security threats, and improving the safeguards of US financial systems.

(1) (U) Since June 1995, the Secretary of the Treasury has been responsible for identifying and blocking terrorist funds within the US and its jurisdiction. In addition, a number of Treasury Department offices work with other USG agencies to implement Executive Order 13224 *Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism* along with key statutory provisions of the Currency and Foreign Transactions Reporting Act, commonly referred to as the Bank Secrecy Act of 1970 (BSA) and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (better known as the USA PATRIOT Act), and to enhance information sharing among intelligence, law enforcement, and financial institutions.

(2) (U) For DOD, the Treasury Department's primary role in CTF is the production of domestic and international terrorism designation packages. Members of the IC provide intelligence to Treasury for compilation into a final designation package. Each member of the IC must approve the designation prior to the OFAC order being served and/or DOS request for 1267/1373 designation.

(3) (U) It should be noted that the Department of Treasury does not have any law enforcement capabilities. Their power lies within the use of administrative sanctions leading to the blocking/freezing of assets. Once an asset is frozen, other law enforcement agencies (FBI, DEA, Bureau of Immigration and Customs Enforcement (ICE), IRS-CID) can provide court orders asking for the assets to be seized by the USG. Once the assets are legally seized, the proceeds from the liquidation of the asset can be used to fund further CTF programs.

(2) (U//FOUO) The Department of Treasury is responsible for identifying, monitoring and blocking the assets of threats to the United States within its jurisdiction. The primary office within the department that is involved in the effort to disrupt threat financing is the Office of Terrorism and Financial Intelligence (TFI). Within the TFI, the following organizations deal with CTF-related issues:

(a) (U//FOUO) **Financial Crimes Enforcement Network (FinCEN).** FinCEN is responsible for “receiving, analyzing, and disseminating disclosures from financial institutions concerning suspected proceeds of crime and potential financing of terrorism.” Through the Egmont Group, an international network of Financial Intelligence Units (FIUs), FinCEN disseminates financial intelligence globally as it relates to ongoing law enforcement efforts. Additionally, FinCEN is responsible for administering the BSA, by maintaining a record-keeping system used by banks and other financial institutions (e.g., money services businesses, broker/dealers, casinos, currency exchangers) to file suspicious financial activity reports. The BSA is one of the United States’ main tools for countering abuses (i.e., threat financing, money laundering) of the US financial system, as it provides information that can be used to track a specific adversary’s financial transactions. It increases transparency within the financial system in order to prevent criminal access to financial services and products, whether to fund terrorist operations or to hide the profits of other crimes, such as drug trafficking. FinCEN is not a law enforcement agency, nor a member of the IC. They do not have the ability to do comparative analysis of BSA data against other IC agency data.

(b) (U//FOUO) **Office of Terrorist Financing and Financial Crimes (TFFC).** The main focus of the TFFC is policy and strategy development, interfacing between various entities, both foreign and domestic, and private organizations that focus on countering threat financing. In addition, the TFFC works with members of the IC and the DOD to incorporate its financial intelligence techniques regarding terrorist financing into the more general problem of threat finance. TFFC also leads the US delegation to the Financial Action Task Force (FATF), which has created global standards for countering money laundering and terrorist financing. FATF also plays a role in countering threats like proliferation, terrorism and the deceptive financial practices of countries like Iran.

(c) (U//FOUO) **Office of Intelligence and Analysis (OIA).** OIA is responsible for analyzing financial information in order to generate intelligence to disrupt the funds of individuals or organizations that may pose a threat to national security. One of the OIA’s main goals is to provide “expert analysis and intelligence production on financial and other support networks for terrorist groups, proliferators, and other key national security threats.”

(d) (U//FOUO) **Office of Foreign Asset Control.** Within the TFI, OFAC is responsible for “administering and enforcing targeted financial sanctions against specific countries, regimes, terrorists, drug traffickers, and selected other threats to the national security, foreign policy, or economy of the United States.” Taking its authority

from legislation as well as from the Presidential emergency powers, OFAC can freeze assets and impose controls on financial transactions within US jurisdiction.

(5) (U//FOUO) **Internal Revenue Service - Criminal Investigation (IRS-CI).**

The IRS-CI division investigates an array of financial crimes that pertain to CTF. IRS-CI assists in the financial aspects of terrorism investigations, particularly the abuse of non-profit organizations to finance terrorist organizations and activities. IRS-CI also focuses on legal-source (tax refund fraud) and illegal-source financial crime (e.g., telemarketing scams, money laundering), both of which tighten the overall financial sector in support of CTF. To counter the use of money laundering, IRS-CI works within existing law enforcement strategies to investigate international and domestic drug traffickers and their money laundering regimes and to trace illegal proceeds back to the criminal. IRS-CI also collaborates on interagency task forces in High Risk Money Laundering and Related Financial Crimes Areas. These domestic regions (e.g., Chicago) are designated as high-risk for money laundering and other financial crimes, as a result of drug trafficking as well as other criminal activities, and necessitate interagency “collaborative investigative techniques.”

(a) (U) Within IRS-CI, the CI Counterterrorism Lead Development Center (CT-LDC) is a single facility that provides support to all ongoing IRS terrorism investigations by using “advanced analytical technology and [leveraging] valuable income tax data...to proactively identify potential patterns and perpetrators with a particular focus on the use of tax exempt organizations to fund terrorist activities.” The CT-LDC liaison agents facilitate the flow of information to the FBI’s Joint Terrorism Task Force (JTTF). Another group within IRS-CI, CI Computer Investigative Specialists supports all terrorism investigations which “[involve] the acquisition of digital evidence “ by “extracting financial records stored in computer hard drives, computer networks, and even the Internet.”

(b) (U) IRS-CI works with Treasury’s TFFC and OFAC, the FBI, in the fight against threat finance. IRS-CI also partners with the FBI, specifically the FBI’s Terrorism Financing Operations Section (TFOS), and the JTTF, by “focusing on financial leads, conducting witness interviews, participating in ‘jump teams’ sent to the Middle East, Europe, and the Caribbean to conduct financial investigations, and analyzing financial data.” Because the IRS possesses expertise in investigating tax evasion, money laundering, and fraud, it frequently supports FBI investigations into individuals and groups who fund their activities using these same illegal techniques. At the international level, IRS-CI participates in the FATF on behalf of the United States.

d. (U//FOUO) **Department of State (DOS).** The DOS serves as the USG’s lead agency for all efforts to combat terrorism overseas. DOS has a variety of programs in combat zones designed to achieve diplomatic goals. While many of these programs go beyond DOD operational capabilities, DOS spends significant amounts of money on infrastructure assessments and subsequent training. Incorporating DOD operations into DOS programs has been beneficial in accomplishing DOD missions

Chapter II

(1) (U) To safeguard the international financial system against terrorist financing and money laundering, the DOS:

(a) (U) Coordinates efforts to build international support for efforts against terrorist finance;

(b) (U) Works through US missions around the world to encourage countries to take actions to freeze terrorist assets when found:

(c) (U) Works with US missions to develop new initiatives to strengthen international cooperation against terrorist finance; and;

(d) (U) Supports efforts to provide technical assistance to foreign governments working against terrorist finance.

(2) (U) Within the DOS, the Office of the Coordinator for Counterterrorism (S/CT) and the Bureau of International Narcotics and Law Enforcement Affairs (INL) have the primary responsibility for coordinating capacity building abroad to disrupt terrorist financing, while the Bureau of Economic, Energy, and Business Affairs (EEB) has primary responsibility for international coalition building. In addition, DOS has several other bureaus and offices that manage various programs and activities that help combat terrorist financing.

(3) (U//FOUO) As the USG department responsible for international diplomacy and enacting the foreign policy of the United States, the DOS is uniquely positioned to conduct CTF. DOS has access to nearly all foreign governments through US embassies. Within each embassy are Country Teams, comprised of representatives from USG organizations, which coordinate information sharing and policy efforts in a HN. Terrorism Finance Coordinating Officers from the DOS Office of Terrorism Finance and Economic Sanctions Policy are attached to selected embassies worldwide to coordinate CTF policy implementation. The DOS works with the Departments of Justice and the Treasury to designate adversaries that have committed, or pose a significant risk of committing, acts of terrorism that threaten the security of US nationals or the national security, foreign policy, or economy of the US; and provides support and training assistance to countries in order to meet international CTF standards. Additionally, the Secretary of State has the ability to designate terrorists and terrorist organizations, which imposes certain legal obligations on US citizens and businesses. Within the DOS, the following organizations have prominent roles in CTF:

(a) (U//FOUO) **Office of the Coordinator for Counter Terrorism.** The Office of the Coordinator for Counter Terrorism synchronizes USG efforts to identify and halt terrorist financing abroad and coordinates US policy on terrorist financing with foreign governments, non-state actors, and multilateral organizations. Within the S/CT, the Counterterrorism Finance Unit assesses and provides technical training and assistance to foreign governments that are trying to improve “their ability to investigate, identify, and interdict the flow of funds to terrorists.” The Counterterrorism Finance Unit also

provides interagency training for improving legal frameworks, financial regulatory systems, FIUs, law enforcement, and judicial/prosecutorial development. Also within the S/CT, the Terrorist Designation Unit prepares possible terrorist designations for review by the Secretary of State and reviews and implements terrorist designations made by the US Department of Treasury.

(b) (U//FOUO) **Bureau of International Narcotics and Law Enforcement Affairs.** The INL advises the President, the Secretary of State and other USG departments and agencies on the progress of policies against international narcotics and crime regimes, including money laundering and other financial crimes. Every year, the INL produces a report to Congress detailing its strategy to combat international crime and provides funding to anti-money laundering (AML) organizations worldwide, including several FATF entities (e.g., MONEYVAL [The Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism], the Caribbean Financial Action Task Force, the Intergovernmental Action Group against Money-Laundering in West Africa and the Organization of American States Experts Group to Control Money Laundering, among others). Together with the S/CT, the INL co-chairs the interagency Terrorist Finance Working Group, which provides technical assistance to countries whose financial sectors are vulnerable to, or have already fallen victim to, financial crimes and terrorist financing.

(c) (U//FOUO) **Bureau of Economic Energy and Business Affairs.** The EEB's responsibilities lie at the "critical nexus of economic prosperity and national security." Within the EEB, three offices conduct CTF-related operations. The Energy Sanctions and Commodities Office developed and negotiated the Kimberley Process certification scheme, which closely monitors rough diamonds so that they cannot be used to fund violence and political and social unrest in Africa. The Office of Terrorism Finance and Economic Sanctions Policy works to build international support for CTF, encourages other nations to freeze terrorist assets and provides technical assistance to foreign governments that need assistance implementing CTF policies. The Office of Terrorism Finance and Economic Sanctions Policy also develops and coordinates strategies for imposing sanctions on other nations, according to US foreign policy (e.g., Iran).

(d) (U//FOUO) **United States Mission.** A mission is led by a Chief of Mission (COM), usually the ambassador, but at times the chargé des affaires, ad interim (the chargé), can lead the mission when no US ambassador is accredited to the country or the ambassador is absent. While an embassy may have some regional and multilateral responsibilities, it is primarily concerned with a broad bilateral relationship across many fields, some of which touch on aspects of CTF. The Mission provides an "on the ground" perspective with regard to the political and economic impacts of CTF. It also provides entrée to HN CTF counterparts and entities in banking, financial, economic, tax, customs, law enforcement, intelligence, and security fields. The Embassy often has influence and bilateral programs with the HN that can build long term capabilities and result in changes in HN policy, laws, regulations or enforcement actions that can be used effectively

Chapter II

against adversary financial operatives and networks. Establishing an interagency TFC in a region or individual country requires the concurrence of key personnel including, the relevant COM and the National Security Staff's CSG. If operating in a foreign country during peacetime, the TFC and all staff fall under the authority of the relevant COM.

(e) (U//FOUO) **Chief of Mission.** The COM is responsible for recommending and implementing national policy, to include CTF, regarding the foreign country(ies) or intergovernmental organization (IGO) to which he or she is accredited. The COM interacts with DOS and other strategic-level planners and decision makers to provide recommendations and considerations for crisis action planning directly to the combatant commander (CCDR) and JFC of a joint task force (JTF). The COM may confer with the JFCs regularly to coordinate US military activities with the foreign policy direction being taken by the USG toward the host country.

(f) (U//FOUO) **Country Team.** The country team, headed by the COM, is the senior in-country interagency coordinating body and theoretically mirrors/reflects the CTF process in Washington. It is composed of the COM, Deputy Chief of Mission (DCM), the senior member of each US department or agency in country, and other USG personnel as determined by the COM. Each country team member presents the position of his or her parent organization to fellow members and conveys country team considerations back to the parent organization. Although some agencies have a limited regional presence (e.g., FBI Legal Attaché, Treasury, IRS), it is unlikely that all interagency members of the CTF effort will be present in country. A CTF working group may be established but, without substantial augmentation, its capability is likely to be limited. Legal Attaché Offices conduct law enforcement and intelligence liaison and are a forward presence for the FBI in the International Terrorism Financing Working Group and the Joint Terrorist Financing Task Force. The DOS's representatives have links to regional and functional bureaus and also to the Ambassador-at-large for Counterterrorism and S/CT, who co-chairs the Terrorist Finance Working Group, develops coordinated strategies to defeat terrorists abroad and secure the cooperation of international partners, and "coordinates the delivery of technical assistance and training to foreign governments to help them improve their ability to investigate, identify and interdict the flow of funds to terrorists."

(g) (U//FOUO) **Chief of Station.** The Chief of Station is the senior intelligence officer and the DNI representative in embassies overseas. As such, the station chief has a dominant role in intelligence and related operations and provides, in part, a forward deployed presence of the IC and CTF intelligence.

(h) (U//FOUO) **Senior Defense Official (SDO)/US Defense Attaché (DATT).** The DATT is the direct representative of the Secretary of Defense, the DATT's service Chief and the Geographic CCDR, and serves as the COM's principal military advisor on defense and national security issues. The SDO is the senior diplomatically accredited DOD military officer assigned to a US diplomatic mission, and the single point of contact for all DOD matters involving the embassy or DOD organizations assigned to or working from the embassy. The DATT is usually but not always the SDO.

The attachés serve as liaisons with their HN counterparts and are valuable sources of information for the COM and CCDR on the military affairs of the HN. The attachés may assist in the foreign internal defense (FID) program by exchanging information with the CCDR's staff on HN military, political, humanitarian, religious, social, and economic conditions and interagency coordination.

(i) (U//FOUO) **Security Assistance Officer (SAO).** The SAO, if assigned, is the most important FID-related military activity under the supervision of the COM, oversees the provision of US military assistance to the HN within the context of Security Force Assistance and USG security sector reform initiatives. The SAO operates under the direction of the COM but reports administratively to the CCDR and is funded by the Defense Security Cooperation Agency. The SAO assists HN security forces by planning and administering military aspects of the security assistance program and helps the country team communicate HN assistance needs to policy and budget officials within the USG. For FID related CTF operations, the SAO, to the extent authorized by law, may support and coordinate with other USG agencies to develop the capability and capacity of HN non-defense security forces and their supporting institutions in order to counter threats from subversion, lawlessness, and insurgency. For instance, this might include supporting the training of HN civil police in individual and collective tasks in contested environments when other USG-agencies' trainers and advisors are unable to do so or the transition of responsibilities for such training and advisory duties to other USG agencies as the security environment allows.

e. (U) **Department of Justice (DOJ).** The DOJ has the lead responsibility for investigating and prosecuting terrorist acts, including all forms of material support to terrorist organizations. DOJ enforcement agencies investigate criminal activity at the direction of DOJ prosecutors with the goal obtaining criminal convictions. DOJ provides legal assistance to partner nations by assisting in drafting laws which meet international standards set by the UN and other international bodies. DOJ provides training to foreign prosecutors and judges and works with HN law enforcement agencies to improve investigative and evidentiary gathering techniques. Within the DOJ, the FBI has the lead role in law enforcement and criminal matters related to terrorism. The major entities with the DOJ that are involved in disrupting threat financing are the Organized Crime Drug Enforcement Task Forces (OCDETF), the DEA, and TFOS, which falls under the FBI.

(1) (U) **OCDETF.** The DOJ's OCDETF Program was established in 1982 to combat money laundering organizations and criminal enterprises. A number of USG agencies participate in the OCDETF Program, including DEA, Bureau of Alcohol, Tobacco Firearms, and Explosives (ATF), FBI, IRS, ICE, the US Coast Guard (USCG), the US Marshals Service, the Criminal and Tax Divisions of the US DOJ and numerous state and local agencies. OCDETF produces an annual Consolidated Priority Organization Target List, a list of "command and control elements of the most prolific international drug trafficking and money laundering organizations." Targeting these elements allows federal drug resources to focus on "identifying and targeting the major trafficking organizations, [and] eliminating the financial infrastructure of drug organizations by emphasizing financial investigations and asset forfeiture."

(2) (U//FOUO) **Drug Enforcement Administration.** The DEA is a law enforcement agency within the DOJ. Its mission is to “enforce the controlled substances laws and regulations of the United States and bring to the criminal and civil justice system of the United States, or any other competent jurisdiction, those organizations and principal members of organizations, involved in the growing, manufacture, or distribution of controlled substances appearing in or destined for illicit traffic in the United States.” The DEA is responsible for investigating organizations involving illegal drugs, some of which may be tied to CTF activities. At the request of the NSC TF Sub CSG, the DEA has the lead role in the ATFC. This is based on the belief that the Taliban is heavy reliant on drug profits to fund its illicit activities

(3) (U//FOUO) **Federal Bureau of Investigation.** The FBI is an investigative and intelligence agency within the DOJ. It has the mission of protecting US national security and countering criminal activities. Because of its dual missions in law enforcement and national security, the FBI has the responsibility and jurisdiction to counter both criminal money laundering and threat financing.

(a) (U//FOUO) The FBI has been designated as the primary law enforcement agency in all terrorism investigations with connections to the US, and is the lead investigative agency for CTF. Investigations of criminal activity and intelligence gathering are very similar. The FBI conducts investigations in order to develop evidence of a crime to be used in future prosecutions. DOD can request information from FBI investigation and is statutorily required to share intelligence with other IC members. The FBI has had an active program with FinCEN conducting CTF data analysis with great success. The FBI accomplishes this through its investigative programs and through its Legal Attaché (Legat) program within US Embassies throughout the world.

(b) (U) Money laundering falls under the direction of its Criminal Investigative Division. The Division’s Financial Crimes Section and Money Laundering Unit specialize in tracing illegal proceeds. The Financial Crimes Section maintains an Asset Forfeiture Program which launches “a parallel financial investigation...to locate the proceeds and prove their connection” to a case. The money is then returned to victims of the crime or retained by law enforcement agencies. While it is common knowledge that this practice occurs with narcotics crimes, it is also used in international and domestic terrorism cases. By “[depriving] wrongdoers of the proceeds of their crimes,” the Asset Forfeiture Program “disrupts, and dismantles criminal and terrorist organizations,” and “[destroys] the financial infrastructure of criminal enterprises.”

(c) (U) Formed immediately after 9/11, the Terrorist Financing Operations Section of the FBI's Counterterrorism Division “builds on the FBI’s expertise in conducting complex criminal financial investigations and long-established relationships with the financial services sector” to “[coordinate] efforts to track and shut down terrorist financing.” TFOS tasks include “conducting full financial analysis of terrorist suspects and their financial support structures,” and “developing predictive models and conducting data analysis to facilitate the identification of previously unknown terrorist suspects.”

TFOS works jointly with prosecutors; law enforcement, both national and international; the intelligence community; and regulatory bodies to exploit financial information in CTF cases. In particular, TFOS targets nonprofit organizations, which may be funneling money to adversaries. FBI offices have ongoing investigations into such cases and “the TFOS has acted as a clearinghouse for these cases and has summarized the collected data.” The Section also “[engages] in an aggressive international outreach program to share information regarding terrorist financing methods” so that international CTF partners can benefit from the CTF data that TFOS has already gathered.

(d) (U) The FBI also heads the JTTF program, which brings federal, state, and local law enforcement agencies throughout the country, along with representatives from the IRS, ICE, DOD, TREAS, and DOS, together to coordinate information sharing on CT investigations. More than 100 JTTFs throughout the US are managed by the National JTTF, which is located at FBI headquarters.

(e) (U) **Legal Attachés.** The FBI has a Legats in over 100 countries and covers every country in the world. The Legat is a senior FBI agent (GS-15) whose job is to coordinate the gathering of evidence of crimes wherein violations of US law has occurred. Additionally the Legat coordinates the exchange of intelligence between law enforcement entities within the HN to the benefit of both countries. The FBI has Designated Intelligence Disclosure Officials Authority, the equivalent of a Foreign Disclosure Officer within DOD, to pass intelligence generated by the FBI to its counterparts in the HN. HNs can request FBI assistance in investigating criminal activity to include forensic analysis not available to local law enforcement

f. (U) **Department of Homeland Security (DHS)** has a supporting role in tracking terrorist financing and conducting related investigations within the US and select overseas activities.

(1) (U) **United States Coast Guard.** The USCG and the DHS have limited but unique resources and capabilities to detect, monitor, assess, contain, analyze, disrupt, and deter threat finance activities. Both USCG and DHS have law enforcement authority that allow for the collection, retention, and dissemination of information. Additionally, USCG and DHS are both members of the IC, giving them the ability to collect and disseminate national intelligence information. Both the Coast Guard’s uniformed service and the US Coast Guard Investigative Service (CGIS) liaise with law enforcement community partners including task forces such as OCDETF and JTTF, providing the USCG with unlimited access to law enforcement information. Additionally, CGIS with DHS coordination has access to the FinCEN records to review bank records, credit card data, business records, check casher records, money remitter records, and trade records. Internally, the USCG and CGIS have access to the Marine Information for Safety and Law Enforcement (MISLE), a database that holds historical records on maritime boardings and inspections.

(a) (U) The USCG Intelligence Organization is comprised of the National Intelligence Element, Counter Intelligence, and Foreign Intelligence. The USCG has the

Chapter II

analytical capability to review and assess ship knowledge, commercial vessel information, shipping information, and international maritime organization information.

(b) (U) The USCG Intelligence Coordination Center (ICC) is the fusion center for all maritime information for the USCG and is the vital link between maritime civilian law enforcement and the DOD CTF efforts in the maritime domain. The USCG is linked with El Paso Intelligence Center (EPIC) created by the DOJ and staffed by the DEA, Counter-Terrorism Intelligence Center (CTIC), and works closely with the Office of Naval Intelligence to support CCMDs. Lastly, the USCG coordinates and liaises with representatives from the fifteen other intelligence agencies.

(2) (U) **Bureau of Immigration and Customs Enforcement.** ICE is the investigative arm of DHS as it relates to violations of laws when DHS is the lead investigative agency. ICE has a mission to target current terrorist funding sources and identify possible future sources. ICE provides law and border enforcement training and technical assistance to foreign governments in conjunction with other US law enforcement agencies and the international law enforcement agencies. ICE uses Currency Transaction Report data as a valuable analytic tool for detecting illegal activity, developing leads, and furthering investigations. Customs and Border Protection (CBP) monitors violation of immigration law and import/export violations. Once CBP identifies violations, ICE is tasked with developing the case for further criminal prosecution.

(a) (U) ICE also takes the lead in countering bulk cash smuggling. Located in Williston, VT, ICE's Bulk Cash Smuggling Center (BCSC) "provides one-stop shopping, 24 hours a day" to federal, state, local and international law enforcement agencies that are working to investigate identify and disrupt bulk cash smuggling activities. BCSC "provides real-time tactical intelligence, investigative support and expertise in the transportation and smuggling of bulk cash... [and] financial investigative expertise that will help them to better follow the money trail." In 2005, ICE partnered with US Customs and CBP to launch Operation Firewall, which targets criminals smuggling bulk cash via commercial and private passenger vehicles, commercial airline shipments and passengers and pedestrians crossing US borders between Mexico and Canada. ICE and CBP also partner to combat bulk cash smuggling at US ports-of-entry.

(b) (U) ICE's Trade Transparency Unit was established in 2004 to combat trade-based money laundering (TBML) by building partnerships with US trading partners. Under this program, the US will exchange trade data with partner countries in order to "identify instances and patterns of trade-based money laundering" by analyzing "trade data for anomalies that would only be apparent by examining both sides of a trade transaction." A special computer system called Data Analysis & Research for Trade Transparency System was developed to assist investigators by allowing them to see both sides of a transaction, making crimes such as TBML, smuggling, tax evasion, and customs fraud easier to detect.

(c) (U) ICE also participates in the FATF and the DOJ's OCDETF.

g. (U//FOUO) The **Central Intelligence Agency (CIA)**. The CIA serves as a source of analysis on topics of concern and also works closely with the other organizations in the IC in support of the intelligence consumer. The CIA specializes in analyzing human intelligence (HUMINT), or intelligence gleaned from human sources, and disseminates that intelligence to appropriate organizations of the USG.

5. (U) Intergovernmental Organizations

a. (U) Threat financing networks are global, so efforts to identify and disrupt adversary access to funds should also be global. Moreover, because the overwhelming majority of threat finance activity is outside US jurisdiction, the US has entered into several agreements to improve and facilitate international organizations' CTF efforts.

b. (U) **United Nations (UN)**. The UN is one of the key international entities in the fight against terrorist organizations and networks. The most significant role that the UN has with regard to terrorist financing is the imposition and enforcement of international financial sanctions through the designation lists maintained under numerous United Nations Security Council Resolutions (UNSCR), including 1267, 1373, and 1617. Although the UN consists of numerous departments and specialized agencies, the Counterterrorism Implementation Task Force and the Counterterrorism Committee have the largest roles in disrupting terrorist finances.

(1) (U) **UN Security Council 1267 Committee**. UNSCR 1267, passed in October 1999, set up the "1267 Committee," to monitor the sanctions imposed on then-Taliban-controlled Afghanistan for its support of Osama Bin Laden and Al Qaeda. These sanctions require UN member states to, among other things, freeze assets of persons and entities listed by the 1267 committee. The Council has revised and strengthened these sanctions since 1999. On January 30, 2004, the Council, in Resolution 1526 (2004), further strengthened and expanded the Committee's mandate by requiring that states freeze economic resources derived from properties owned or controlled by Al Qaeda and the Taliban and also that states cut the flow of funds derived from non-profit organizations and alternative/informal remittance systems to terrorist groups.

(2) (U) **Financial Action Task Force. FATF** (<http://www.fatf-gafi.org>) is an intergovernmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing. FATF is a policy-making body, which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

(a) (U) FATF monitors members' progress in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures globally. In performing these activities, FATF collaborates with other international bodies involved in combating money laundering and the financing of terrorism.

Chapter II

(b) (U) FATF does not have a tightly defined constitution or an unlimited life span. FATF reviews its mission every five years. FATF has been in existence since 1989. In 2004, Ministry representatives from the 35 FATF members agreed to extend the mandate until 2012.

(c) (U) FATF standards are comprised of the *Forty Recommendations on Money Laundering* and the *Nine Special Recommendations on Terrorist Financing* (<http://www.fatf-gafi.org/recommendations>)

“FATF will continue to set anti-money laundering and counter-terrorist financing standards in the context of an increasingly sophisticated financial system, and work to ensure global compliance with those standards. FATF will enhance its focus on informal and non-traditional methods of financing terrorism and money laundering, including through cash couriers, alternative remittance systems, and the abuse of non-profit organizations.”

**Terrorist Financing: US Agency Efforts
and Inter-Agency Coordination,
Congressional Research Service, 2005**

c. (U) **Egmont Group of Financial Intelligence Units**

(1) (U) Over the past years, specialized governmental agencies have been created as jurisdictions develop systems to deal with the problem of money laundering and other financial crimes. These entities are commonly referred to as FIUs. They offer law enforcement agencies around the world an important avenue for information exchange. An FIU is a central office that obtains financial report information, analyzes it, and then discloses it to an appropriate government authority to support money laundering, criminal proceeds, or terrorism financing investigations. FIUs have attracted increasing attention with their role in AML programs. They are able to provide a rapid exchange of information (between financial institutions and law enforcement / prosecutorial authorities, as well as between jurisdictions), while protecting the interests of the innocent individuals contained in their data.

(2) (U) Recognizing the benefits inherent in the development of a FIU network, a group of FIUs met in Brussels in 1995 and decided to establish an informal group for the stimulation of international co-operation. Now known as the Egmont Group of Financial Intelligence Units, (<http://www.egmontgroup.org>) these FIUs meet regularly to find ways to cooperate, especially in the areas of information exchange, training, and the sharing of expertise.³ The goal of the Egmont Group is to provide a forum for FIUs around the world to improve cooperation in the fight against money laundering and the financing of terrorism and to foster the implementation of domestic programs in this field. Under the Egmont principles, each member will share financial intelligence within the Egmont Group. The IC can ask FinCEN to contact an Egmont FIU on a specific target. Some FIUs are more responsive than others, and requests should be judiciously used in certain countries to avoid compromising ongoing operations

"INTERPOL fully supports the Egmont Group's statement that the key issue in anti-money laundering efforts is to ensure that critical pieces of information reach the investigators and prosecutors charged with arresting criminals and recovering illegal funds. INTERPOL's Anti-Money Laundering Unit is dedicated to increasing the flow of money laundering information among financial investigators by forging alliances with financial intelligence units and financial crime units around the world."

**INTERPOL
Anti-Money Laundering Unit**

d. (U) **International Criminal Police Organization (INTERPOL).** INTERPOL is the world's largest international police organization, with 188 member countries. Created in 1923, it facilitates cross-border police co-operation, and supports and assists all organizations, authorities and services whose mission it is to prevent or combat international crime. As part of its international and impartial character, INTERPOL also aims to facilitate international police co-operation even where diplomatic relations do not exist between particular countries.

(1) (U) With regard to countering financial crimes, INTERPOL's primary focus is on payment cards, money laundering, intellectual property crime, currency counterfeiting, and new technologies, all of which can be used by terrorist organizations to fund their operations.

(2) Within INTERPOL, the Fusion Task Force (FTF) has the lead for conducting antiterrorism efforts. The FTF's primary objectives include identifying active terrorist groups and their members; soliciting, collecting, and sharing information and intelligence; providing analytical support; and enhancing the capacity of member countries to address the threats of terrorism and organized crime.

(3) INTERPOL's Anti-Money Laundering Unit was established to promote the flow of relevant money laundering information between investigators and to maintain relations with national, regional, and international FIUs and financial crime units. In conjunction with Europol's Financial Crime Unit, INTERPOL also identifies points of contact around the world for the Camden Assets Recovery Inter-Agency Network, "an informal international network for tracing, freezing, seizing and confiscating the proceeds from criminal activities."⁴

Intentionally Blank

CHAPTER III

PLANNING CONSIDERATIONS (U)

"TCOs [Transnational Criminal Organizations] and the illicit trafficking they conduct continue to be the primary threat to regional security.... In countering this international threat, working with our partners, we must attack TCOs in a broad, coordinated manner, to include demand reduction; eradication and regulation of source materials; suppression of money laundering; interdiction of the illicit shipments as they transit to the United States and other end-user countries; and ultimately the disruption and dismantling of TCOs operating in the region. However, TCOs are increasingly sophisticated and have proven resilient and adaptive to attempts to disrupt their operations."

General Douglas M. Fraser
Commander, United States Southern Command
April 5, 2011

1. (U) Introduction

a. (U) Joint Publication (JP) 5-0, *Joint Operation Planning*, asserts joint planning integrates military actions with other instruments of national power and multinational partners in time, space, and purpose to achieve a specified end state. CTF requires the integration of the efforts of disparate organizations in a whole-of-government approach in a complex environment. The JFC generally plays a supporting role in the planning and execution of CTF operations. However, in an operational area where armed conflict is being conducted, the JFC will typically be the supported JFC, while other mission partners operating in the operational area will often be the lead for planning and executing CTF operations. Nevertheless, because mission partners have different and distinct missions as well as expertise and capabilities not inherent in DOD, the JFC should have situational awareness of their activities and the ability to coordinate and synchronize with these organizations in order to support these agencies in achieving their objectives. Similarly, mission partners should have situational awareness of military activities and the ability to coordinate and synchronize with the JFC in order to help achieve DOD objectives.

b. (U) CTF activities which eliminate or disrupt insurgent funding and identify host government corruption can help remove adversary fighter and operatives from the environment, decrease adversary morale, reduce the adversary's operational effectiveness, and help to stabilize an area and promote its political and economic development. CTF activities constitute a set of additional tools available to generate desired effects and, to achieve the JFC's objectives. As such, the JFC and staff need to fully integrate CTF activities into joint plans.

c. (U) In order to integrate CTF activities into joint plans, the JFC and staff will continue to use the joint operations planning process (JOPP) as delineated in JP 5-0 and supporting doctrinal publications. Integrating CTF does not change the JOPP. As such, this chapter will focus on the limitations and considerations specific to CTF rather than a general review of JP 5-0.

d. (U) Military operations support the near and long term plans of policy makers but they will not have the same lasting impact that cultural, political, law enforcement and regulatory change and actions will have. CTF elements, as subject matter experts, have the responsibility to inform the JFC, and his staff, on the possible enablers available through interagency partners, multinational organizations, and the HN.

DISRUPTING ILLICIT FINANCIAL FLOWS TO EXTREMISTS

Al-Qaeda, the Taliban, and other extremist groups receive significant income from both the regional narcotics trade and outside funding sources. To weaken the extremist threat, we are redoubling efforts to reduce illicit financial flows and disrupt support networks by pursuing a whole-of-government, three-pronged counter threat finance strategy:

1. Engaging countries that are sources of external funding for terrorist and insurgent groups;
2. Using targeted sanctions against terrorist financiers and facilitators; and
3. Providing technical assistance to strengthen Pakistan and Afghanistan's counter-terrorist financing, legal, regulatory, and enforcement capacity.

This strategy emphasizes the role of international partners in disrupting illicit financial flows, as well as stronger partnership with the Afghan and Pakistani authorities.

**Afghanistan and Pakistan Regional Stabilization Strategy
January 2010**

2. (U) Military Planning and Mission Partners

a. (U) Because the solution to a problem when conducting military operations, seldom, if ever, resides within the capability of just one organization, joint operation/campaign plans and operation orders (OPORDs) should be crafted to recognize the core competencies of various agencies and military activities be coordinated and resources integrated, when and where appropriate, with those of others to achieve the operational objectives. Operations in both Iraq and Afghanistan have clearly shown there will not be a single authority over civilian USG agencies, let alone HN and international mission partners, with clearly defined roles and responsibilities (i.e., unity of command). At best, “unity of effort” may be achieved. Coordinating and integrating efforts between the joint force and USG agencies, multinational partners, IGOs, NGOs, and the private sector cannot and should not be equated to the command and control (C2) of a military operation. Non-military stakeholders do not have similarly sized resources nor the same mission and reporting requirements. More critically, their perspectives on a situation, planning timelines and horizons, and possible solutions are different and the different professional and social cultures can sometimes create friction.

b. (U) Plans and OPORDS should be crafted to recognize the core competencies and unique authorities of various mission partners and should coordinate military activities with those of mission partners to achieve the desired end state. Mission partners often possess far greater expertise, and in some cases, more capabilities than the military to execute political, diplomatic, and economic missions. JP 3-08 states, “The degree to which military and civilian components can be integrated and harmonized will bear directly on efficiency and success.” Hence, it is imperative partners in the operational area are included, whenever possible, in the planning process.

3. (U) Counter Threat Finance Limitations and Considerations during the Joint Operational Planning Process

a. (U) **Initiation.** As stated in JP 5-0, “Military options normally are developed in combination with other nonmilitary options so that the President can respond with all the appropriate instruments of national power.” To the extent possible, the JFC and staff need to consider the non-military options being developed, especially as they relate to CTF. Because the JFC will issue coordination instructions as part of initial guidance, identification of mission partners is a critically important part of initiation. Additionally, the JFC should review intelligence products and staff estimates to determine sufficiency and relevancy as they relate to CTF.

b. (U) **Mission Analysis.** During mission analysis, the goal is to understand the purpose of the operation and issue appropriate guidance to drive the rest of the planning process. Because, more often than not, the military will be supporting other mission partners, examination of the environment and guidance should include the mission partners and not focus solely on the military’s mission and objectives. Based on the identification of mission partners undertaken as part of initiation, the JFC and staff need to identify the end states and objectives of various mission partners (including their execution timelines and planning horizons). Additionally, the JFC and staff should identify where objectives and end states of mission partners reinforce and conflict with military end states. The consideration of the military and the mission partners’ end states and objectives should inform the JFCs’ mission success criteria. Further, the JFC and staff should identify where execution timelines and planning horizons for CTF mission partners are most closely aligned with the military and where they are the most different. In addition to identifying the constraints and restraints on the military during mission analysis, the JFC and staff should identify unique authorities and capabilities mission partners can provide as well as gaps and deficiencies mission partners might have. The JFC in conjunction with mission partners and higher headquarters will decide how the military will participate in CTF activities. Should the military support HN law enforcement or perhaps US law enforcement as the lead for CTF activities eventually leading to legal prosecution? Should the US military lead CTF activities supported by HN and US law enforcement agencies with a primary focus on threat finance interdiction and capture/kill of key adversary personnel? The JFC’s initial intent and planning guidance should reflect these findings and decisions. Additionally, the JFC should identify critical information requirements (CCIRs), including priority intelligence

requirements (PIRs) that adequately and appropriately address the need for information and intelligence relating to the adversary's use of and need for finance.

c. (U) **Course of Action (COA) Development.** COA development should consider the unique capabilities and authorities of mission partners as well as any gaps they may have, as identified in mission analysis. The JFC and staff should endeavor to identify where the military can benefit from action led by mission partners and where mission partners can benefit from actions led by the military. CTF elements must assist in the development of courses of action that will include activities or support that will be requested from interagency partners, multinational organizations, or HN. This includes identification and recommendations for engagement options against adversary combatant and noncombatant personnel and entities within and outside the operational area. Additionally, where the military desires to have actions led by other mission partners, COA development should include those mission partners (vice just consultation) wherever possible to fully understand the constraints and restraints implied by the mission partner being in the lead. For example, the military believing the HN police should lead an effort does not mean the police have the capabilities or authorities to do so or their priorities would permit it. Actions taken by both the military and mission partners should be integrated into the different COAs as appropriate. Additionally, the relative weight of effort by the military and mission partners may serve to distinguish between COAs as they are developed. Where CTF is a significant aspect of the assigned mission, JFCs and their staffs may consider CTF as a separate line of effort. Where CTF is less significant, it should be integrated with other lines of effort.

d. (U) **COA Analysis and Wargaming.** During COA analysis and wargaming where CTF is a feature of the mission and environment, the JFC should ensure the red cell understands and appreciates the impact CTF can have on an adversary. Doing this will provide the most accurate assessment and analysis of the impact CTF COAs will have on the achievement of overall objectives and end states, but does not guarantee an accurate prediction of the impact of different COAs. Without this expertise, however, the true impact, both positive and negative, of CTF activities cannot be developed by the JFC. In the same way the "... wargame and synchronization matrix efforts will be particularly useful in identifying cross-component support resource requirements," they can also be useful in identifying support resource requirements across mission partners, where a mission partner is reliant upon action or effort by the military or vice versa.

e. (U) **COA comparison.** When comparing COAs, one criterion the JFC should consider is: Does the COA place mission partners in the best posture for future operations/activities? This is particularly important where execution timelines and planning horizons of mission partners extend far beyond those of the military. The JFC needs to consider, as one of many factors, how the military's execution of CTF activities will impact the subsequent CTF activities of other mission partners in the months, and years, after the military has completed its mission and re-deployed.

f. (U) **Plan or Order Development**

(1) (U) **Concept of Operations (CONOPS) Development.** When the JFC and staff are developing the CONOPS, it needs to provide sufficient detail to outline coordination mechanisms with other mission partners. Where multiple mission partners are leading CTF activities, the CONOPS needs to lay out the means and mechanisms by which different military units, which may be supporting or supported by the mission partner activities, can coordinate planning, execution and support.

(2) (U) **Plan or Order Development Activities.** While not all development activities are appropriate for CTF missions, the following activities highlight CTF-specific planning considerations:

(a) (U) **Force Planning.** In support of overall plan development, planners should consider whether sufficient and appropriate CTF forces and capabilities are available to conduct CTF missions and support CTF mission partners. If not, are more or different forces available? If more or different forces are not available, what impact will this have on the plan?

(b) (U) **Support Planning.** In support of overall plan development, planners should consider not just any unique support requirements for forces conducting CTF activities (e.g., physical storage for evidence) but should also consider any necessary support for mission partners which the military has agreed to provide.

(c) (U) **Deployment Planning.** In support of overall plan development, planners should consider not just any unique deployment requirements for forces conducting CTF activities but should also consider any necessary deployment support for mission partners, which the military has agreed to provide (e.g., airlift for law enforcement personnel).

(d) (U) **Shortfall Identification.** When conducting shortfall identification, planners may need to independently consider mission partners' ability to generate adequate capabilities and their ability to do so on the military's timetable. Where planners assess generation capabilities may not match plan requirements, a shortfall should be noted and addressed with the JFC and higher authorities.

(e) (U) **Feasibility Analysis.** Feasibility analysis, particularly as it relates to CTF, can be very challenging. Assessing and analyzing whether the assigned mission can be accomplished using available resources within the time contemplated by the plan requires deep understanding of mission partner capabilities, gaps, cultures, authorities, and timelines. Conversely, the mission partners require a deep understanding of the military's capabilities, gaps, cultures, authorities, and timelines. Participation (not simply consultation) by mission partners should be the goal whenever possible. Adequate training, including internships and personnel exchanges if possible, can help ameliorate, but not completely solve this challenge by helping to develop a deeper level of understanding of different mission partners.

(f) (U) CTF activities and actions should be integrated in the overall plan and not limited to an individual annex. Interagency planning is typically included in a separate annex within the military plan. CTF activities and actions for interagency organizations may be delineated there.

4. (U) Staff Estimates

Because they are key outputs for COA development, COA analysis and wargaming, and COA comparison, staff estimates are discussed separately, but the information and processes involved in each of those step of the JOPP are vitally important to inform the staff estimates. Given the specialized knowledge, unique requirements, and varied participation in CTF, the JFC may benefit greatly from a CTF staff estimate. A CTF Staff Estimate should identify and examine factors that may influence CTF operations, which support and are integrated with tentative COAs. Collaboration among relevant military, interagency, and multinational staff organizations during the staff estimate process facilitates the iterative refinement of COA. As such, the staff estimate can serve as a means to generate this collaboration amongst the mission partners and the military. It is important to remember, however, the manpower and resource constraints many mission partners are under, especially when compared to the military. Therefore, expectations for participation in the staff estimate process should be discussed early and the staff estimate process should respect the input of mission partners and should give them voice to the JFC and the planning process in order for it to be worth the effort and resources for mission partners.

"In some respects, the global effort to combat terrorist financing is only as effective as its weakest links. Terrorist groups take advantage of vulnerabilities and gaps in the system, and gravitate toward countries and regions whose efforts are lacking."

**The Money Trail
Finding, Following, and Freezing Terrorist Finances
Matthew Levitt and Michael Jacobson**

5. (U) Environments

a. (U) Equally important to understanding the role and functions of mission partners, the JFC and staff need to understand the high-level impact the operational environment will have on CTF activities. This understanding can lead to the creation of a more comprehensive, feasible, and achievable plan.

b. (U) Perhaps the most pervasive and significant attribute of the operational environment in which the military conducts CTF is its dynamic nature. While finance is the lifeblood of adversary organizations, especially irregular adversaries, security is the lifeblood of the finance arm of those organizations. Adversary finance organizations exist and flourish by operating without detection. When detected they will change locations, tactics, and sources of income to avoid monitoring, exploitation, and

interdiction. This means adversary finance organizations are constantly changing and evolving in move/counter-move fashion with CTF efforts.

c. (U) JFCs and staffs should appreciate the authorities under which they operate. The forces they are apportioned and allocated and the rules which govern their operations will be defined by the mission they are assigned and the environment in which they operate.

d. (U) **Missions.** The JFC's assigned missions, which CTF activities will support, will largely dictate the authorities and the force with which the JFC will operate. If the mission is Homeland Defense at sea inside the 12 mile territorial sea limits of the US, the authorities under which the JFC operates will be governed by different US laws than if the JFC is operating in a foreign country. Additionally, the political considerations and ramifications of a JFC assigned enforcement of sanctions will mean the forces apportioned and the rules of engagement (ROE) under which CTF activities may be conducted will be quite different than if assigned a mission to participate in stability operations.

e. (U) **Location.** Where the JFC is assigned to operate will impact greatly on the authorities under which the military operates, the forces apportioned, and the rules which govern the operations. When operating domestically the authorities under which the military operates and the forces it may be apportioned will be quite different than when overseas. Further, the authorities, forces, and rules will be different if operations are taking place in a foreign country, which has invited the US in and is working with US military and interagency CTF, than a country where US forces may not have overt or direct access and where deniability is a concern.

f. (U) **Impact.** Understanding the impact of the mission assigned should occur very early in the JOPP (initiation and mission analysis), but will inform all aspects of the planning process. Continuous reappraisal of the impact of the mission and the environment is required throughout planning and execution. Because the adversary and the environment are so highly dynamic, so too will be the impact those have on CTF activities. As missions change, the authorities and rules under which the military executes those missions change. Failure to take account of those changes can create gaps and seams where the adversary can flourish and can result in lost opportunities for the US. Additionally, given the global nature of adversary finance organizations, the JFC and staff should account and plan for operating against the adversary finance organization in a wide variety of environments under different authorities and rules. The JFC and staff should also plan how to coordinate with other JFCs when adversary finance organizations and activities cross AOR boundaries.

6. (U) Planning Considerations for the Joint Force Commander

a. (U) The following non-exhaustive list highlights some general planning considerations for the JFC:

(1) (U) The JFC tasked to support or lead CTF should ensure coordinating authorities, channels, and terms of reference are carefully established and documented, with the aim of facilitating their missions and flexibility while not promoting duplication of effort and confusion. Such authorities constitute the rules of the road for multilateral, multinational, interagency organization, such as those engaging in CTF, and they should contribute to unity of effort and common situational awareness.

(2) (U) The JFC should respect existing authorities and adapt process models, as appropriate to the mission, of other organizations, units, and commands engaged in CTF. A useful rule of thumb would be to look first at those organizations, units, and commands in the operational area engaged in CTF and expand outward from there.

(3) (U) Reporting procedures and doctrinal nomenclature should be developed and evolved to support the mission, in full recognition that national policy requirements serve as the basis for CTF procedures and formats.

(4) (U) The JFC should establish operating procedures that ensure coordination is authorized, empowered, and sought out at all levels of the organization and direct that certain, specified coordination processes run through the organization. The JFC and staff should specify how internal processes will be structured to make them effective and adaptable to accommodate the participation of a wide variety of agencies and nations. CTF elements must also be informed about the actions and activities of interagency partners, multinational organizations, and HN that may be impacted or conflict with the planned military operations.

(5) (U) The JFC and higher authorities should consider the types of CTF missions and lines of operation that the unit will be assigned and ensure staff analysis and decision-making processes are either in place which can leverage the full expertise of all mission partners while providing them a mechanism to voice concerns or problems while still ensuring the success of the organization.

b. (U) The following non-exhaustive list highlights some strategic planning considerations for the JFC:

(1) (U) Strategic plans are required to create the policies for applying CTF; making requests to and coordinating with the interagency partners to obtain personnel, capabilities, and resources; determining the amount of time that the CTF capability will be required; establish training, staffing and provide funding for CTF organizations and initiatives that will be used to apply and enforce national CTF policy.

(2) (U) Strategic planners will need to know the mission, authorities and capabilities of the CTF element. This will influence the orders that are given to subordinate elements with reference to which military organizations will be tasked to work with or provide support to the CTF element.

(3) (U) Strategic planners will need to know the command relationships in the country where the CTF element will be deployed.

(a) (U) The USG C2 element in the country of deployment is US military.

(b) (U) The USG C2 element in the country of deployment is the US COM

(c) (U) The USG C2 responsibility is shared between the US COM and the senior military commander in country.

(4) (U) Strategic planners must understand the unique and special qualifications, capabilities and resources that the CTF element and their interagency partners will bring to the Commander.

(5) (U) The establishment and implementation of memorandums of agreement or memorandums of understanding between DOD and the various participating Departments or Agencies should alleviate many of the coordination and operational issues that will arise.

c. (U) The following non-exhaustive list highlights some operational planning considerations for the JFC:

(1) (U) Operational planners must know and understand the mission and authorities associated with the CTF element. Issues with C2 and tasking authorities can arise when a CTF organization is deployed to a combat zone. Clear reporting and tasking authorities should be established before the CTF element deploys. The CTF element must support to the JFC while performing the work they are assigned by their parent organization.

(2) (U) Coordinate and de-confliction the military organizations CTF effort with the US Embassy in the country of operation. Planners should request information and points of contact with existing interagency CTF entities and activities that are presently active in the operational area. Planners should request information related to political restrictions on CTF related activities to include personnel associated with the HN government. Discussions with the Deputy COM, FBI Legat, and Treasury Department Attaché are usually a good way to identify any interagency CTF activities in country.

(3) (U) Coordinate with the leadership of the CTF element to determine the division of effort between military and interagency participants involved with CTF and how that work will be used to support the JFC's objectives.

(4) (U) Know when and how to request personnel, resources and equipment from each of the supporting interagency partners. Planners should request information on the pay grades and occupational specialties that may be expected. Planners should be made aware of any use of contractor employees that may be sent in lieu of Federal employees.

(5) (U) Be made aware of any special waivers or qualifications that may be required before interagency personnel can be allowed to participate in certain military activities. This is especially true in situations where interagency participants may be asked to deploy with military units during combat operations or to participate in interrogations. Compatibility of law enforcement and regulatory training with military training requirements must be considered.

(6) (U) Know the deployment durations for interagency participants and when to submit follow on request to replace departing personnel. Each interagency partner will have their own policy concerning overseas deployments and deployments to hazardous duty areas. Planners should expect to see deployment durations ranging from 90 days to more than one year.

(7) (U) Coordinate with the force development, logistics, and financial management staff to determine what levels of support the military organization will be capable of providing to the CTF element, especially the interagency participants. Determine if the CTF element requires a separate military unit identification code [UIC].

(8) (U) Identify the requirements for interagency personnel to access military systems, facilities and which interagency personnel will be given access to those systems.

(9) (U) Know the restrictions and abilities of interagency personnel to support or conduct field operations in support of military operations. Planners must consider transportation and movement requirements for personnel in within the operational area.

(10)(U) Reporting requirements and information sharing. Operational planners should make every effort to identify common interests between DOD and the interagency community. CTF elements should be given authority to nominate targets and request intelligence collection support based on the availability of assets. CTF elements should also be given the authority to request support to engage targets, when feasible, and within the authority of the military units being asked to perform the engagement. CTF elements often require the authority to write and submit their own intelligence information reports.

(11)(U) Chains of command and tasking authority between the military and interagency participants in the interagency CTF element should be clear. Direct liaison authority for the CTF element with units in theater must be carefully and clearly spelled out to avoid inadvertent bypasses of military chains of command.

d. (U) The following non-exhaustive list highlights some interagency planning considerations for the JFC:

(1) (U) Interagency personnel should be brought into the planning process as soon as possible. Military planners should consult with interagency personnel to determine the authorities and capabilities of each agency along with initial recommendations on how to employ those capabilities. Military planners should take the time to identify specific skills and capabilities that the interagency participants will bring. The planners should also ask for any limitations on the use of the interagency participants to include carrying personal weapons, travelling to locations where site exploitations are being performed, meetings away from the work location, travelling with military units outside secure areas and other situation the planners may be aware of

(2) (U) Most interagency partners have limited manpower, budgets, or infrastructure to support foreign operations that are not directly related to their mission and responsibilities. Almost all USG agencies use volunteers for overseas deployment. Most interagency partners do not have a dedicated pool of deployable personnel to draw from. Requests for interagency support should be made as soon as the decision has been made to establish and employ an interagency CTF element. DOD should expect to provide significant funding, facilities, information technology, transportation, force protection, logistical support to support this effort.

(3) (U) Establishing clear lines of communication between the participating interagency organization and the military organization can minimize coordination and information sharing issues. Reach back is greatly facilitated when the interagency partner agrees to provide a specific point of contact to work with and support the CTF element.

(4) (U) Interagency personnel that are assigned to forward deployed locations that have an established US Mission are often subordinated to the COM. Interagency personnel may also be subordinated to their Department or Agency Attaché that is assigned to the US Mission. Planners should check with forward deployed commanders to determine the current C2 relationship between the US military commander and the COM. Interagency personnel and entities do not report to nor can they be tasked by military commanders without an applicable MOA. Interagency support should be properly coordinated with the interagency partner providing the support. Interagency personnel in previous organizations have demonstrated exceptional flexibility in support military organizations.

(5) (U) Interagency personnel are typically volunteers that have significantly shorter deployment capabilities than military personnel. It is not unusual for interagency personnel to be limited to 90 day rotations. Some agencies will grant longer rotations but planners should be aware of each agency's rotation policy.

(6) (U) Military organizations will usually provide the bulk of the travel, local transportation, meals, security, logistical support, information technology support, replacement ammunition, and operating facilities.

7. (U) The Counter Threat Finance Organization

a. (U) CTF planning will identify the organizations and entities that will be required to conduct CTF action and activities. CTF organizations may include various combinations of:

- (1) (U) US Military.
- (2) (U) Interagency organizations.
- (3) (U) Multinational organizations.
- (4) (U) IGOs.
- (5) (U) HN.

b. (U) Planning for a CTF element is based on three basic structures:

(1) (U) Organic CTF element established within a military staff at the CCMD or JTF level. The CTF staff is comprised of active duty or reserve military personnel, DOD civilians, and contractors. This CTF staff is not a standalone entity and will be integrated into the regular military staff and will respond to the JFC's direction and requirements.

(2) (U) CTF element comprised of DOD and interagency personnel operating at a foreign deployed location within a military area of operation. This type of CTF organization is typically requested by DOD and established by the NSC. Examples of this type CTF organization are the ITFC and the ATFC. The CTF staff will be comprised of interagency personnel, DOD personnel, and possible civilian contractors working for the interagency or DOD. This CTF element will probably be lead or co-lead by a civil USG agency member and a DOD military officer or civilian. C2 relationships and tasking authorities are unique to each element established.

(3) (U) CTF element comprised of DOD and interagency personnel operating outside a military area of operation, probably at a CCMD HQ. This CTF element may be integrated into an interagency task force (IATF) or JIACG at the CCMD. This CTF element often provides administrative support such as CTF related training and military staffing; operational guidance or direct support to CTF elements that are forward deployed into an operational area. The CTF staff will be comprised of interagency personnel, DOD personnel, and possibly contractors working for a USG agency or DOD. This CTF element will probably be lead or co-lead by a civil USG agency member and a DOD military officer or civilian.

c. (U) Planning should begin immediately after the decision has been made and a request submitted through OSD to the required interagency organizations to establish a Joint DOD/interagency CTF element at a forward deployed location.

(1) (U) Planners must identify and obtain documents that authorize or direct the establishment of a CTF element. Includes reviews of requests from CCMDs, Joint Staff orders or directives, OSD policy or directives, information related to the CTF elements mission, tasks, scope of work and source of funding. Planners should work with the Staff Judge Advocate to create memorandums of agreement or memorandums of understanding for the operation of the CTF element.

(2) (U) Planning to create personnel manning documents. Planners must determine how many people with specific skill sets and experience are required to perform the mission. DOD does not currently have a military occupational skill identifier or specialty code to identify personnel with CTF training or experience. Planners must be able to determine which military branch of service will be required to fill each position and if those positions must be filled by active or reserve military personnel, DOD civilians or contractors. There may be a specific requirement for personnel from a specific military branch of service, but this is usually not the case. Most military personnel that fill these positions will be individual agumentees that are assigned to the CCMD for periods ranging from 90 days to 1 year. Planners must be able to estimate the amount of time that it will take to receive the initial group of military CTF personnel as well as their follow on replacements. Significant problems can arise if there is not enough overlap between personnel that are being replaced and their replacement. Planners must determine how long DOD personnel will be deployed on each rotation. Each USG department or agency will establish their own staffing and rotation policies. Military planners must know what the interagency staffing and rotation plan is.

(3) (U) Establish an operating time frame for the CTF element. This will include stand up dates, initial deployment dates, fully operational capability dates and estimated date the CTF element will be withdrawn and disbanded.

(4) (U) Establishing a scope of work for the DOD participants in the CTF element and a requested scope of work for the interagency participants. Identify specific tasks that may require DOD acceptance of interagency organization training such as interviews with detainees. Federal law enforcement agents receive training and many have experience in conducting criminal interviews. Federal law enforcement officers training, experience and skills are comparable to military interrogators. Interagency personnel must have clear expectations of their role and duties before they deploy.

(5) (U) Requesting direct liaison authority with interagency organizations.

(6) (U) Planning to establish funding support for the CTF element.

Chapter III

(7) (U) Planning to submit requirements for interagency support. This will include types and numbers of persons and skill sets required along with any special equipment, communications equipment, or access to an interagency database.

(8) (U) Identify training requirements for interagency personnel to deploy into a combat zone.

(9) (U) Identify security clearance requirements, reciprocity, and access among DOD and interagency partners.

(10)(U) Determine which capabilities the CTF element will be need and how those capabilities will be employed against the adversary. The CTF element must be prepared to act as coordinators, synchronizers, and liaison to interagency partners, multinational organizations, and HN nation CTF related organizations.

(11)(U) Detailed planning is required to deploy interagency personnel and assets into a military theater of operations. This planning includes DOD coordination with the senior military commander in theater, COM/country team, multinational forces, and the HN. The DOD/interagency CTF element should be deployed using a military order. The ATFC/ITFC were deployed using fragmentary orders to the orders that deployed USCENTCOM to each location. This task typically will be the responsibility of the CCMD who controls the AOR where the CTF element will be deployed.

CHAPTER IV OPERATIONS (U)

"Whereas in decades past, criminal organizations were largely domestic or regional in scope, and due to their centralized nature the arrest of a single key member was sometimes enough to dismantle them, today's global criminal syndicates operate transnationally and are comprised of loose networks that cooperate intermittently but maintain their independence. And unlike their predecessors, they employ sophisticated technology and financial savvy... We must break the financial infrastructures of transnational criminal networks, and build international consensus and cooperation."

GEN James Jones
October 2010

1. (U) Introduction

(U) CTF should be considered and included when planning and conducting military operations. CTF TTP can provide enhanced information on the activities, organization, placement, vulnerabilities, and capabilities of an adversary. CTF personnel should ensure that they are aware of all ongoing and planned operations to provide commanders with information that could lead to the engagement of threat financial operators, assets or facilities.

2. (U) Unified Action

a. (U) DOD operations against CTF targets will be based on the persons, assets, and facilities that are being considered for engagement. Some targets are better engaged by DOD elements and some CTF targets must be engaged through interagency, multinational or HN organizations. All of the challenges to unified action will clearly hold for CTF, and may be magnified because:

(1) (U) DOD is not always the lead agency. As such, the designs, timelines, operational tempo, tactics, rules and procedures, and objectives of the military commander will not have primacy in the planning and execution of CTF.

(2) (U) Since CTF is not a traditional area of endeavor for the military, the JFC may find the challenges of unified action magnified due to a lack of understanding as to who the mission partners are, what their roles and functions are, what their planning and objectives timelines are, what their capabilities are, and what their resources, capacities and authorities are. These challenges may be compounded if the mission partners do not understand these same things about the military.

b. (U) Military organizations will improve their ability to unilaterally and jointly engage CTF targets through increased experience and training in CTF operations.

3. (U) Differences between Military and Interagency Participants

MILITARY FORCE AND INTERAGENCY PARTNER DIFFERENCES IN THE OPERATIONAL AREA

- Planning Timelines (Days versus Months/Years)
- Event/Action Focused versus System/Process Focused
- Tactic, Techniques, and Procedures/Doctrine versus Rules of Evidence
- Rules of Engagement Rules and Rules for Escalation of Force

Interagency Organizations are not Expeditionary, They are Enduring

a. (U) Much has been written about the differences between the military and the interagency community and how a JFC can be more successful in leveraging these differences. This paragraph highlights a few additional key differences that are most important to CTF operations.

b. (U) Perhaps most importantly and fundamentally, military and interagency partners missions in the operational area differ. A JFC's mission is expeditionary, or transitory; while, the missions of interagency partners in the operational area are typically more enduring. Whereas the military almost exclusively enters an operation with a clear intention to redeploy after the successful conclusion of operations, some interagency partners in the operational area will stay on. These partners will have had a presence in the country or area for decades, perhaps longer, and intend to remain in the area to work on a continuous basis. Many interagency organizations have a capacity building role and a small footprint in the country where military operations are being conducted. These interagency organizations often operate with minimum personnel and limited budgets. Interagency organizations may have little to no surge capability. Differences arising from the disparate missions can manifest in the following ways:

(1) (U) **Planning Timelines (Days versus Months/Years).** Military organizations at the lowest levels may see future operations as 72 hours out, but planners at the JTF level will plan 6 months to a year in advance. CCMD and Joint Staff levels perform strategic plans multiple years in advance. Military targeting and engagement can take place relatively quickly or it can take months depending upon the complexity of the operation. Interagency organizations can take a considerable amount of time to prepare and develop a case that will justify and support their engagement. If there is a significant difference between military and interagency organizations over time, it is primarily in the time it takes to prepare and conduct an operation. For example, the military may believe that the best way to conduct CTF is to capture/kill key threat finance facilitators, interdict smuggling, and raid suspected wire remitters. By contrast, interagency partners may view building reporting and enforcement capacity in the HN government and financial institutions as the most effective way to conduct CTF. While these two ideas are not mutually exclusive, they are also not mutually supportive. The joint force is likely to see

little immediate benefit to its CONOPS from other USG agency efforts to improve the banking system. Conversely, interagency participants may see little immediate benefit in improving the government and institutional capacity from the military's efforts to dismantle the adversary's financial network. They will also be concerned with tracking changes in threat financing and an adversary's financial network as a result of these actions view the other's efforts as a supporting effort to their main efforts.

(2) (U) **Event/Action-Focused versus System/Process-Focused.** The military tends to be very event or action focused and views a system or process as a means to that end. The military typically wants just enough discussion to be able to agree to act. Conversely, because of the enduring nature of their mission, interagency partners tend to focus on developing consensus and cooperation, which they may view as important as, or more important than, the end result of the system or process. As a result, the military may view interagency participants as indecisive while interagency partners may view the military as reckless, who can destroy the hard-earned trust they have built with the host-nation institutions.

c. (U) There are two other operational differences between the military and interagency partners in the operational area, stemming from divergence in their respective missions that are significant to CTF. They are:

(1) (U) **TTP/Doctrine versus Rules of Evidence.** The military operates under US law, policy, doctrine, TTPs and orders which govern its behavior. Civilian mission partners, especially those in law enforcement, are bound by the rules of evidence, which are inviolable and, if breached, will result in unusable evidence. Neither set of guidance is better than the other; both sets serve different purposes. However, rules of evidence support rule of law and security sector reform. ROE and TTPs should be aligned with the rules of evidence when conducting operations with an interagency organization. Consideration of rules of evidence is not only important in operations conducted with law enforcement personnel, but also in military operations that are intended to support subsequent prosecution in civilian courts.

(2) (U) **Rules of Engagement and Rules for Escalation of Force.** Both military and law enforcement are trained to employ lethal force, but with very different purposes and missions. Military ROE and Rules for Escalation of Force provide the framework under which they can close with and destroy the enemy with the least force necessary and the least possible collateral damage. For law enforcement, rules for escalation of force often emphasize the rule of law to preserve life, liberty, and property for later adjudication. Both serve different purposes and neither is more or less right than the other. Careful consideration and deconfliction of the rules in effect for each participant should be addressed prior to execution.

d. (U) In consideration of these differences as well as several others outlined in JP 3-0, *Joint Operations*, JP 3-08, *Interorganizational Coordination During Joint Operations*, and elsewhere, the JFC may want to ensure experienced military law

Chapter IV

enforcement personnel are represented on the planning and operations organizations of the CTF staff.

4. (U) Command and Control

"Tracking funds as they travel through the global financial system demands both interagency and international cooperation to develop intelligence collection, storage, and dissemination policies. Since 9/11, both US and international intelligence agencies have restructured to reflect this current threat environment. Tremendous strides have been made to stop the flow of funds to illicit actors, but the international community must continue to emphasize the importance of financial intelligence in order to constrain terrorists' operating environment and pursue individual threats."

Matthew Levitt
Follow the Money
Georgetown Journal of International Affairs
Winter/Spring 2011

a. (U) **Command Relationships (External).** One of many differences between the US military and civil partners (US and foreign) is that civil partners often rely upon their headquarters (HQ) as an action organization (rather than just a policy or strategy organization). The Pentagon does not conduct operations, but organizations of the US Department of Treasury HQ take actions fundamental to its mission. As such, it is critically important to establish clear lines of communication and defined mechanisms for coordination with all of the action arms of the mission partners who share responsibility for CTF. DOD does not exercise control or authority over the actions or personnel of another Department of the USG. This will be true regardless of the operating location for interagency personnel. Joint CTF elements are established to perform tasks and activities that will be mutually beneficial to all participating organizations. When a joint DOD/USG interagency organization is stood up, the chain of command, lines of communication, and tasking authority must be clearly delineated and agreed to prior to the joint CTF organization being deployed.

b. (U) Many factors will weigh on the design of the C2 of a DOD CTF element. Important factors include:

- (1) (U) How many other missions/responsibilities the JFC is assigned;
- (2) (U) The complexity of the operating environment;
- (3) (U) The number of mission partners, as well as their respective experience and requirements; and
- (4) (U) The JFC's working relationships with mission partners.

c. (U) There are **several organizational constructs** the JFC could employ for the C2 of CTF:

(1) (U) **Staff Element.** The JFC could retain responsibility for CTF and task an organization of his staff. Depending on the nature of the specific mission and operational environment, the JFC may elect to create an entirely new cell on the staff, or place the responsibility in an existing staff section (intelligence, operations, plans, etc).

(2) (U) **Service Component.** The JFC could assign the mission to an existing Navy, Army, Air Force, or Marine Corps component. Per doctrine, to establish unity of command and effort, the component with the preponderance of CTF forces to be tasked and the ability to effectively plan, task, and control CTF will normally be assigned the mission. However, the JFC will always consider the nature, and duration of the operation, force capabilities, and the C2 capabilities in selecting a commander.

(3) (U) **Functional Component.** The JFC could assign the mission to an existing functional component. The JFC should normally assign the mission to the functional component whose responsibilities most overlap with the requirements of CTF, according to the specifics of the adversary and environment. The JFC should also ensure appropriate operational forces are assigned and support is apportioned from other components to execute CTF.

(4) (U) **Deployable Cell.** The CDR may consider utilizing the threat finance cell (TFC), which are described in the *Counter Threat Finance Roadmap*. The JTF commander could then use the TFC to augment the CTF mission under any of the above C2 structures. If the CDR envisions using the TFC in such a manner, the TFC should be appropriately manned, trained and equipped for potential deployments and organized in a way that allows a capability without impeding the TFC's support of the CDR's persistent CTF requirements.

5. Threat Finance Cell

a. (U) The most common technique for promoting cross-functional collaboration is the formation of centers, groups, bureaus, cells, offices, elements, boards, working groups, and planning teams and other enduring or temporary organizations that manage specific processes and accomplish tasks in support of mission accomplishment. These centers, groups, bureaus, cells, offices, elements, boards, working groups, and planning teams facilitate planning by the staff, decision making by the commander, and execution by the HQ. Although cross-functional in their membership, most centers, groups, bureaus, cells, offices, elements, boards, working groups, and planning teams fall under the principal oversight of the staff directorates.

b. (U) A cell is a subordinate organization formed around a specific process, capability, or activity within a designated larger organization of a JFC's HQ. A cell usually is part of both a functional and traditional staff structures. An example of a cell within the traditional staff structure could be an IO cell subordinate to operations branch within the J-3 directorate. An example of a cell within a functional staff structure could be a current operations cell within the JOC.

c. (U) As described in the *Counter Threat Finance Roadmap*, TFCs can be established at any level based on available personnel resources. Expertise on adversary financial activities can be provided through the creation of TFCs at brigade HQ and higher. The TFC would include a mix of analysts and subject matter experts on law enforcement, regulatory matters, and financial institutions that would be drawn from DOD and civil USG agency resources. The TFC's responsibilities vary by echelon.

d. (U) At division and brigade, the TFC is responsible for:

(1) (U) Providing threat finance expertise and advice to the commander and staff.

(2) (U) Assisting the G-2 in the development of intelligence collection priorities focused on adversary financial and support systems that terminate in the unit's area of operation.

(3) (U) Consolidating information on persons providing direct or indirect financial, material and logistics support to adversary organizations in the unit's area of operation.

(4) (U) Providing information concerning adversary exploitation of US resources such as transportation, logistical and construction contractors working in support of US facilities, exploitation of NGO resources, and exploitation of supporting HN personnel.

(5) (U) Identifying adversary organizations coordinating or cooperating with local criminals, organized crime, or drug trafficking organizations.

(6) (U) Providing assessments of the adversary's financial viability – ability to fund, maintain, and grow operations – and the implications for friendly operations.

(7) (U) Developing targeting package recommendations for adversary financial and logistics support persons for engagement by lethal and nonlethal means.

(8) (U) Notifying commanders when there are changes in the financial or support operations of the adversary organization, which could indicate changes in adversary operating tempo or support capability.

(9) (U) Coordinating with and sharing information with other TFCs to build a comprehensive picture of the adversary's financial activities.

e. At the operational level, the joint force J-2 is responsible for developing and maintaining an understanding of the operational environment, which includes economic and financial aspects. If established, the TFC supports the J-2 in developing and maintaining an understanding of the economic and financial environment of the HN and

surrounding countries in order to assist in the detection and tracking of illicit financial activities, understanding where financial support is coming from, how that support is being moved into the area of operation and how that financial support is being used. The TFC:

(1) (U) Works with the J-2 to develop threat finance related PIR and establish threat finance all source intelligence collection priorities. The TFC assists the J-2 in the detection, identification, tracking, analysis, and targeting of adversary personnel and networks associated with financial support across the area of operations.

(2) (U) The TFC coordinates with tactical and theater TFCs and shares information with those entities as well as multinational forces, HN and as appropriate and in coordination with the joint force J-2, the IC.

(3) (U) The TFC, in coordination with the J-2, establishes a financial network picture for all known adversary organizations in the area of operations; establishes individual portfolios or target packages for persons identified as providing financial or material support to the adversary's organizations in the area of operations; identifies adversary financial TTPs for fund raising, transfer mechanisms, distribution, management and control, and disbursements; and identifies and distributes information on fund raising methods that are being used by specific groups in the area of operations. The TFC can also:

(a) (U) Identify specific financial institutions that are involved with or that are providing financial support to the adversary and how those institutions are being exploited by the adversary.

(b) (U) Provide CTF expertise on smuggling and cross border financial and logistics activities.

(c) (U) Establish and maintain information on adversary operating budgets in the area of operation to include revenue streams, operating costs, and potential additions, or depletions, to strategic or operational reserves.

f. (U) Targets identified by the operational level TFC are shared with the tactical TFCs. This allows the tactical TFCs to support and coordinate tactical units to act as an action arm for targets identified by the operational level CTF organization, and coordinate tactical intelligence assets and sources against adversary organizations identified by the operational level CTF organization.

g. (U) Multi-echelon information sharing is critical to unraveling the complexities of an adversary's financial infrastructure. Operational level CTF organizations require the detailed financial intelligence that is typically obtained by resources controlled by the tactical organizations. Information obtained from tactical sources may require IC or HN sources to gain access to the source of the documents or to financial accounts and communications accounts. Tactical level CTF will require help in identifying and

Chapter IV

tracking financial support operations that initiate outside of their areas of operations and terminate in their areas of operation.

h. (U) The operational level TFC facilitates the provision of USG and multinational organizations support at the tactical level. This is especially true for USG agencies that have representation at the AMEMB.

i. (U) Tactical level TFCs will require support from the operational level to obtain HN political support to deal with negative influencers that can only be influenced or removed by national level political leaders - including Governors, Deputy Governors, District Leads, Agency leadership, Chiefs of Police, Shura Leaders, elected officials and others persons serving in official positions; HN security forces, civilian institutions, and even NGO's/charities that may be providing the adversary with financial and logistical support.

j. (U) The TFC should be integrated into the HQ battle rhythm. Battle rhythm discipline and vetting by the Chief of Staff helps ensure events have a necessary purpose and defined inputs and outputs to support the commander decision-making. A proposed battle rhythm event that has no output and only provides generic situational awareness, or an information brief outside the decision-making process may not belong on the battle rhythm. Battle rhythm events should follow the following criteria:

(1) (U) Name of board or cell: Descriptive and unique.

(2) (U) Lead staff section: Who receives, compiles, and delivers information.

(3) (U) When/where does it meet in Battle Rhythm: Allocation of resources (time and facilities), and any collaborative tool requirements.

(4) (U) Purpose: Brief description of the requirement.

(5) (U) Inputs required from: Staff sections, centers, groups, bureaus, cells, offices, elements, boards, working groups, and planning teams required to provide products (Once approved by COS, these become specified tasks)

(6) (U) When? Suspense for inputs.

(7) (U) Output/Process/Product: Products and links to other staff sections, centers, groups, bureaus, cells, offices, elements, boards, working groups, and planning teams.

(8) (U) Time of delivery: When outputs will be available.

(9) (U) Membership: Who has to attend (Task to staff to provide participants and representatives).

For more information on cross-functional collaboration and cells, refer to JP 3-33, Joint Task Force Headquarters.

FINANCIAL WARFARE

Financial warfare complements military operations as well as information operations. When combined with advances in social network mapping, it can give a highly detailed picture of an elite's communication and financial structure that can be used for targeting. Communication and software tools now exist to analyze connections in vast networks of heterogeneous information, such as financial transactions, mobile telephone calls, e-mail, and air travel. This gigantic information pool can be a source of knowledge about a nation's elite, where they stash their money, who they talk to, and their position in a social hierarchy. The key to doing this lies in constructing overlays of these datasets to visualize the various connections.

Paul Bracken
Financial Warfare

www.fpri.org/enotes/200709.bracken.financialwarfare.html

6. (U) Operational Area

a. (U) Adversary finance organizations can have global reach and are generally not geographically constrained. While one CCDR may be given global responsibility for military support of CTF operations, JFCs, such as those in Iraq and Afghanistan, will be geographically constrained and resourced to prosecute CTF in their operational area. Because of this, the JFC might find that the end-user of threat finance exists in his operational area. However, much of the threat finance network, including potentially key nodes, will extend beyond the operational area into areas where CTF focus and capability may be lessened. As such, establishing appropriate communications, information sharing, and coordination relationships across the geographic boundaries will be essential to successfully prosecuting CTF. Further, it is important to include members of the USG, such as FBI, Treasury, ICE, or DEA, in the organizational structure of a CTF unit, because these organizations have capabilities and authorities outside of the JFC's operational area.

b. (U) The JFC needs to be fully appraised of the areas where the military and the intelligence community have limited or no visibility of the adversary's financial system. For example, the JFC needs to understand if countries neighboring his operational area are "black holes" for threat finance, where the US and its allies have no visibility, no corresponding banking relationships, or where the institutions are not part of international financial enforcement regimes. Additionally, the JFC needs to fully appreciate those areas where military actions will be politically unacceptable. For example, if threat finance networks are believed to be using the institutions of a political or military ally, it may be impossible for the military to pursue the network inside the ally's borders even if several key nodes exist there.

FINANCIAL SANCTIONS

Blocking bank accounts of key groups and individuals puts the spotlight on them and thereby increases the risks to any company or government doing business with them. Financial sanctions legitimize additional actions, both financial and non-financial, which can ratchet up more pressure. This is where financial warfare and military strategy converge. Most people think of financial warfare as a substitute for military action, which it is, up to a point. But after a point it becomes a complement rather than a substitute.

Paul Bracken
Financial Warfare

www.fpri.org/enotes/200709.bracken.financialwarfare.html

7. (U) Types of Activities and Operations

(U) Military support to CTF is not a distinct type of military operation. Rather, it represents a military activity against a specific capability of an adversary. Additionally, CTF can support several types of military operations. They include:

a. (U) **Major Operations.** CTF can reduce or eliminate the adversary's ability to pay its troops and procure weapons, supplies, and intelligence. Cutting off funding which the adversary uses to pay troops may reduce the morale and effectiveness of the operational force, even if it is not able to keep it from being fielded altogether. However, adversaries with robust strategic and operational reserves will be better able to mitigate US and allied CTF efforts.

b. (U) **Arms Control and Disarmament.** CTF can be used to disrupt the funding and financing of trafficking in small arms weapons; improvised explosive device (IED) or WMD proliferation and procurement; research to develop more lethal, or destructive, weapons; hiring technical expertise; or providing physical and operational security. Additionally, CTF can be used to disrupt the fund/value remittances associated with transfers of small arms or chemical, biological, radiological, and nuclear materials that are against international agreements or conventions.

c. (U) **Nation Assistance**

(1) (U) **Security Assistance.** While not traditionally considered a part of security assistance, military CTF personnel or US Military contractors could provide training to HN CTF and/or Law Enforcement personnel as well as provide CTF capabilities as a defense-related service under Security Assistance.

(2) (U) **Foreign Internal Defense.** CTF personnel can provide training to HN CTF and/or Law Enforcement personnel as well as provide CTF capabilities to assist the nation in its fight against subversion, lawlessness, and insurgency.

d. (U) **Combating Terrorism.** CTF can be used to interdict or disrupt financing to Terrorist Groups, thereby preventing, deterring, preempting, and responding to terrorism.

e. (U) **DOD Support to Counterdrug Operations**

(1) (U) The US Military may conduct training of HN police. CTF can also contribute to building partner nations capacities.

(2) (U) The primary, if not sole, motive of drug trafficking organizations and drug traffickers is profit. For drug trafficking organizations, their huge financial assets are the key node. Money is the vital source of their power, without vast amounts of money they cannot suborn governmental entities (e.g., judges, police), pay informers and "enforcers," or buy weapons and precursor chemicals. Money is the lifeblood of transnational criminal organizations and CTF can be the most effective weapon in the US "arsenal" for defeating them. Attacking the flow of drug profits via CTF raises planning and operational costs and risks associated with drug trafficking, potentially reducing drug-traffickers' profits.

For more information, refer to JP 3-07.4, Joint Counterdrug Operations.

f. (U) **Enforcement of Sanctions.** CTF covers all forms of value transfer to the adversary, not just currency and funds. DOD organizations can employ measures and provide assistance to organizations that are interdicting the movement of goods and/or any associated value remittance as a means to enforce sanctions.

g. (U) **Counterinsurgency (COIN).** CTF can be used to counter, disrupt, or interdict the flow of value to an insurgency, thereby reducing its operational effectiveness. Additionally, CTF can be used against corruption, as well as drug and other criminal money-making activities that fund, or fuel insurgencies and undermine the legitimacy of the HN government. In such cases, CTF is aimed at insurgent organizations as well as other malevolent actors in the environment.

h. (U) **Peace Operations.** In Peace Operations, CTF can be used to stem the flow of external sources of support to the conflict parties, thereby helping to contain and reduce the conflict. Additionally, CTF can be used to bolster the legitimacy of the government by reducing crime and corruption and to build capable government institutions that are able to conduct their own CTF operations.

8. (U) **Military Support Tasks to Counter Threat Finance**

(U) Military support tasks to CTF can fall into four broad categories:

a. (U) **Support Civil Agency and HN Activities (Including Law Enforcement)**

(1) (U) **Provide Protection.** US military forces may provide:

Chapter IV

(a) (U) Overwatch for law enforcement or HN military CTF activities. This may include perimeter security for operations, aerial overwatch, and intelligence indications and warnings.

(b) (U) Protection for civil agency or HN military movements. This may mean providing close protection or convoy security.

(2) (U) **Provide Logistics.** US military forces may provide:

(a) (U) Transportation, especially tactical movement-to-objective support, to law enforcement or HN military CTF activities. This may include providing secure single vehicle movements of key individuals, providing convoys, and executing aerial lift (fixed and rotary wing) for personnel, equipment, evidence, or prisoners.

(b) (U) Supply services, including but not limited to food, equipment, medical materials and/or care, mortuary services, or contracting support for civil agency or HN CTF activities.

(c) (U) Basing, including housing, workspaces, engineering support, and physical security for civil agency or HN CTF personnel.

(3) (U) **Provide C2, Communications, and Intelligence Support.** US military forces may provide:

(a) (U) Information technology (IT) support to civil agency or HN CTF personnel. This support may include provision of hardware and software, configuration support, networking, account administration and information assurance.

(b) (U) Communications support to civil agency or HN CTF personnel. This support may include provision of hardware and encryption, configuration support, networking, and bandwidth, and information assurance.

b. (U) **Direct Military Actions**

(1) (U) **Capture/Kill.** US military forces may, with the support of mission partners as necessary, conduct operations to capture or kill key members of the threat finance network. Such operations may require the use of SOF, conventional ground forces, maritime interdiction forces, or strike/attack aircraft (including fixed wing, unmanned, and rotary aircraft).

(2) (U) **Interdiction of Illicit Value Transfers.** US military forces may, with the support of mission partners as necessary, conduct operations to interdict value transfers to the adversary. This may be a raid to seize cash from an adversary safe house, maritime interdiction operations to stop the smuggling of licit goods used in TBML, or C2 flights to provide aerial surveillance of drug smuggling aircraft in support of law enforcement interdiction.

(3) (U) **Training HN Forces.** US military forces may, with the support of mission partners as necessary, provide training to HN CTF personnel. Such training may include special operations training for tactical organizations, analyst training, and training for operations and planning staffs.

c. (U) **Intelligence Collection.** US military forces may conduct all source intelligence operations, which will deal primarily with the collection, exploitation, analysis and reporting of intelligence. These operations may involve deploying intelligence personnel to collect HUMINT, the operation of ships at sea and forces ashore to collect signals intelligence (SIGINT), open source intelligence (OSINT) and geospatial intelligence (GEOINT), and the flying of (both manned and unmanned) aircraft with various sensors and intelligence collection payloads.

d. (U) **Operations to Generate Intelligence**

(1) (U) Occasionally, US military forces may conduct operations either with SOF or conventional forces designed to provoke a response by the adversary's threat finance network for the purpose of collecting intelligence on that network. These operations are pre-planned and carefully coordinated with the intelligence community to ensure the synchronization and posture of the collection assets as well as the operational forces. An example would be a show of force at a known drug and weapons bazaar to collect signals and imagery intelligence about the adversary's response.

(2) (U) Such operations can be particularly useful in understanding the adversary's threat finance system. For example, if the JFC and staff believe drugs are critical to threat finance, yet the adversary takes little noticeable action or makes no significant reaction to a show of force at a key drug bazaar, a closer examination of the underlying belief may be warranted.

9. (U) Operations Reporting

Whenever the military is conducting operations, whether they are directly supporting CTF or not, the JFC needs to ensure that routine/conventional reporting from operations is available to intelligence personnel. Further, the JFC and staff needs to ensure that the reporting reflects PIRs and other intelligence requirements. Maneuver units, pilots, civil affairs teams, and all other military personnel operating in the environment forward operating base are sources of information, which increase the JFC's ability to answer PIRs and information requirements. This requires all personnel to be familiar with the PIRs and reporting requirements to be enforced on subordinate units.

10. (U) Operations Considerations for the Joint Force Commander

(U) The following is a list, not an exhaustive one, of some operational issues the JFC engaged in CTF should consider:

a. (U) The JFC and staff should establish operating procedures and protocols that are simple, general, and open to review and modification to accommodate the authorities that participating agencies and nations bring with them. The JFC, in conjunction with appropriate organizations of the HN, should also clearly understand the role, responsibilities, and authorities of the HN on whose territory it operates including those related to CTF.

b. (U) Ideally, the JFC and agency and national representatives will have control (OPCON, TACON, or another arrangement) to commit dedicated resources to operations and mission outcomes, likely requiring an Executive Branch mandate and relief from restrictions on application of resources, and cabinet level agreement and/or MOAs/MOUs among participating agencies and nations. JFCs often do not have the authority to commit resources but use reach-back and networking to attain necessary assets and guidance when needed.

c. (U) The JFC, in consultation with the staff and representatives from the mission partners, should specify the least cumbersome and restrictive system for information sharing.

d. (U) The JFC should ensure the unit has the internal organizational capability to administratively support LNOs to leverage their expertise.

e. (U) Whatever CTF mission or line(s) of operations is assigned, dedicated resources to be provided from each participating agency and/or nation should be specified in advance, with the authority to employ those resources assigned to conduct CTF operations. When this authority does not reside under the JFC, reachback and networking can serve this purpose.

CHAPTER V

INTELLIGENCE AND FINANCIAL INFORMATION (U)

“Defense Intelligence shall provide accurate and timely warning of threats and of foreign capabilities and intent to national and defense decision makers to allow for consideration of the widest range of options. While Defense Intelligence must be timely, it also must be substantive, thorough, contextual, and useful in form and format.”

Department of Defense Directive 5240.01
DOD Intelligence Activities

1. (U//FOUO) What the Joint Force Commander Needs to Know

a. (U) Information and intelligence on threat financial networks has the potential to provide JFCs with a better understanding of one of the most important support functions for threat networks. Therefore, the JFC and staff planning efforts should consider threat finance information along with other mission sets such as adversary planning an ambush or emplacing an IED in order to enhance the understanding of the operational environment.

b. (U//FOUO) CTF efforts are heavily dependent on intelligence activities because of the need to detect and identify financial activities and persons of interest. CTF analysts require current and detailed information as well as historical data if they are going to be successful in identifying, detecting, tracking, and analyzing the methods being utilized by threat financial operators and to provide JFCs and interagency partners with sufficient information to engage and disrupt the adversary’s ability to operate. JFCs should review their staff’s internal capabilities to ensure that CTF related skills sets are present and actively participating in the staff planning effort. CTF is a non-traditional military activity and requires personnel having specific training and experience in threat finance. Valuable threat financial intelligence has been lost in the past because units did not know how to report financially related information or did not think that reporting finds of money or items of value were of interest to the military intelligence staffs. CTF intelligence that is collected at the tactical level is ultimately consolidated and used in the development of strategic intelligence that will drive command and policymaking decisions which will determine the level of effort and success against threat finance targets.

c. (U) The identification of units and organizations that require financial intelligence and appropriate information sharing arrangements is essential. CTF elements that are assigned to the JFC should identify the military and interagency organizations within the operational area that have a CTF role or mission. Coordination should be conducted with each of these organizations, which would include organization identification, contact information, interagency affiliations, HN affiliations, multinational affiliations, CTF personnel, CTF mission and capabilities, and CTF intelligence and information requirements. CTF analysts to analysts exchange should be considered to

Chapter V

improve the flow of communications between the CTF elements. It is not unusual to sit in on or to participate in the other organizations meetings and briefings

d. (U) Reachback and coordination with USG agencies should be coordinated and agreed upon prior to the unit being deployed to the operational area. These organizations often require careful and extensive coordination to determine the level of participation and information sharing they will be able to provide and which types of activities they can support. This effort is typically originated and coordinated at the CCDR level and above and will ensure forces on the ground receive the support they need and that they understand what the supporting organizations need from them. Civil agency personnel have unique and valuable skills sets, which can contribute to the JFC's overall efforts.

e. (U//FOUO) Threat financial activities can be difficult to detect and track because of how they are conducted. Funding transfers are often performed across multiple, possibly overlapping, systems (e.g., electronic, hawala, or courier networks), that typically are not subject to surveillance, by the USG or our allies or they get lost with the millions of routine financial transactions performed across the world every day. The transfer of funds may occur well outside the operational area and then be couriered into the operational area using one or more persons across multiple tracks. While it can take months to track a financial network and its operations, the long-term impact of well-targeted and effective CTF interdiction efforts is worth the investment. CTF analysts should collect information and then understand the context of what that information reveals. Daily reporting provides a snapshot of activities and CTF analysts should take those snapshots and prepare a comprehensive analysis of which functional tasks those activities are associated with. Following the money usually means following the person with the money.

f. (U) If CTF is going to be used as an effective force multiplier, JFCs should identify intelligence requirements for threat finance related activities in order to establish collection priorities. Money and other items of value provide the means to conduct the operations and day-to-day activities being performed by adversary leaders and tactical commanders. Following the money may lead to the adversary leadership, but interdicting money flows will invariably adversely impact his ability to conduct operations. Interdict the money and significantly and negatively impact that adversary leader ability to conduct his operations.

g. (U//FOUO) Collection of threat finance information will require additional training for personnel who collect intelligence and conduct interrogations. Threat finance is an area in which few military personnel have training or experience. Collection of information is based on knowing what to look for, where to look for it and when to look for it. High-level financiers are rarely found operating in areas of fighting, or on the battlefield. While finance may be the lifeblood for implementing adversary plans and operations, safety and security are essential requirements for successfully conducting the vast majority of financial transactions and related management and accounting activities.

h. (U) There are a number of things a JFC will need to know about the adversary's financial network and functional organization if his objective is to disrupt or destroy those capabilities. This includes but is not limited to:

(1) (U//FOUO) Identifying the key personnel associated with the threat financial function. What is their contact information; what are their duties and responsibilities; who do they report to; and what, if any, financial, political, tribal, religious and family ties do they have with the government of the HN and of the countries that surround the HN? What is the relationship between the adversary financial operators and the rest of the adversary organization?

(2) (U//FOUO) Determining how threat financial support networks are organized and controlled and how the money flows through the network from the point of origin to the end user. What are the key nodes in the network? Changes in the distribution of funds through the network can be an indicator of many things to include the establishment of new operational cells, pending adversary offensive operations or a shift in geographic operating areas.

(3) (U//FOUO) Determining which venues the adversary financial operators work from and what areas that they support.

(4) (U//FOUO) Determining the adversary's cost to operate. What are their fixed and overhead costs? What are their operational costs? What are their special operations costs? Plans and operations drive the requirement to acquire funding. Costs requirements drive fund raising efforts and most funding streams are only capable of producing a certain amount of money. Changes in funding requirements can force the adversary to increase fund raising efforts, which can create undue pressure on the local population and the economy or force the adversary to use new fund raising schemes. Either of these courses of action can expose the adversary financial operators to law enforcement and intelligence collectors.

(5) (U//FOUO) What are their sources of funding (local, area, regional, international, and multinational) and how and when is that money collected?

(6) (U//FOUO) Identifying which financial and natural resources and assets are being exploited by the adversary financial operators (HN, multinational, and US-provided).

(7) (U//FOUO) Which funding sources provide the greatest source of revenue to the adversary and what alternatives does the adversary have if that funding source is interdicted?

(8) (U//FOUO) How do adversary financial operators transfer and move funds? What are the capabilities of the adversary networks to support surge type operations? This is critical in countries like Afghanistan because external funding is essential to the fight. The limited infrastructure of Afghanistan also has an impact on funding flows and

Chapter V

adversary financial operators have to develop methods to distribute money over vast and often remote areas.

(9) (U//FOUO) Where do the adversary financial operators maintain their money reserves and who are the personnel that are responsible for maintaining them? What will it take to gain access to those money reserves?

(10)(U//FOUO) What are the vulnerabilities in the threat financial networks? What are the expected outcomes when financial interdiction operations and activities are successful?

(11)(U//FOUO) What will the political ramifications be for interdicting well connected and corrupt government officials that are diverting funds to the adversary while enriching themselves?

(12)(U//FOUO) Developing an understanding of how the adversary is applying the financial resources that it has available.

(13)(U//FOUO) Identifying where, and on what, the adversary spends their money, as well as other uses for that money (e.g., possible additions to strategic or operational reserves; money transfers to affiliate, or associate adversary, organizations; or investments). The real power of money and other financial resources is displayed at the point where money is converted to materials, weapons, supplies, transportation and the other things that money was created to do.

i. (U) CTF staff organizations need detailed, timely and accurate financial intelligence to inform the planning and decision-making process. Analysts can present the JFC with a reasonably accurate scope of the adversary's financial capabilities if they have a thorough understanding of the adversary's financial requirements and what the adversary is doing to meet those requirements. This financial and network analysis helps focus CTF efforts, and is critical in prioritizing competing demands for scarce collection and operational resources. Much of the information related to the financial requirements for the adversary can be developed as a part of the joint intelligence preparation of the operational environment (JIPOE).

2. (U//FOUO) Planning

a. (U//FOUO) A review of the baseline intelligence and the JIPOE should be conducted to determine the existing intelligence gaps regarding the adversary's financial networks, operations and personalities. If necessary, the J-2 should prepare and submit new or revised PIRs related to threat finance for the JFC's approval when gaps are identified. If approved, the intelligence collection manager will prioritize their efforts, align assets, and assign collection tasks based on the PIRs. Collection managers should inform the JFC on the capability ability to collect information on threat finance targets based on the PIRs. Collection efforts against threat finance require continual focus when possible. Detection of threat financial activities can take a long period of time and the

failure to quickly find and identify adversary activities can sometimes lead to a reduction of effort against CTF targets. It is important to remember collectors should have access to financial intelligence to be able to collect against it. In some situations, military CTF organizations (e.g., TFC) will require the assistance of their civil agency counter parts to work with the HN or other nation where threat finance operations are active, to gain access to information from civilian financial institutions and records.

b. (U//FOUO) During the planning process CTF staffs should prepare courses of action that include military and civil engagement options. These options will be based on the capabilities that each can bring to bear on the adversary if sufficient information is obtained to enable their use. For example, the JFC should promulgate clear guidance as to whether CTF will be pursued by the organizations under his command primarily, as a law enforcement effort in support of other organizations or entities, or as a military effort. This decision will drive the structure and function of the intelligence enterprise to support CTF, since intelligence to support law enforcement should be developed and treated quite differently than intelligence developed for military operations. Intelligence is typically not used as evidence in court. The classification level of intelligence that is prepared for prosecutors should be at a level that is usable in court. Evidence obtained during military operations must be handled, documented, and accounted for in accordance with law enforcement standards and parallel reconstruction completed. Parallel reconstruction will involve DOD and law enforcement entities working together through the sharing of information, coordination of planning and strategy, and preservation of collected items for evidentiary purposes. While each organization has a different mission, the ultimate goal shared by both is to disrupt and dismantle illicit threat finance activities. Finally, the JFC should evaluate the intelligence collection assets available and their suitability in meeting his requirements and request additional assets as necessary.

AL QAEDA'S MONEY SINCE 9/11

We have learned much since 9/11 about how al Qaeda raises, moves, and stores money, but our understanding is still somewhat speculative. The US intelligence community is forced to extrapolate from current information to fill in the gaps in our knowledge. Detainees have confirmed the basic sources of al Qaeda funding and methods of moving money, and have provided insights into changes in al Qaeda's financing since 9/11. Moreover, al Qaeda adapts quickly and effectively, creating new difficulties in understanding its financial picture. Intelligence challenges remain and are likely to continue, although the picture is clearer today than ever before. As al Qaeda becomes more diffuse—or becomes essentially indistinguishable from a larger global jihadist movement—the very concept of al Qaeda financing may have to be reconsidered. Rather than the al Qaeda model of a single organization raising money that is then funneled through a central source, we may find we are contending with an array of loosely affiliated groups, each raising funds on its own initiative.

**National Commission on Terrorist Attacks upon the United States
Monograph on Terrorist Financing**

3. (U//FOUO) Collection

a. (U) Collection operations acquire information about the adversary and other relevant aspects of the operational environment and provide that information to intelligence processing and exploitation elements. Collection disciplines complement each other, and the collection manager should resist favoring or becoming too reliant on a particular sensor, source, system, or technique.

b. (U//FOUO) HUMINT is one of the most important means to obtain financial intelligence, especially at the tactical level. Financial activities revolve around the relationships and interactions between people. These interactions are often performed in person and require human observation to obtain insight into what is transpiring. These relationships and interactions are translated into communications, transactions, and activities that result in financial activity. Threat finance activities usually do not involve the movement of large formations of people or equipment that can be detected by their physical movement, electronic signature, and placement on the battlefield. Threat financial activities are easily mixed in with normal commercial transactions or cross border traffic that may only be detected by the information provided by a human source. Finding people that have participated in or have personally observed these financial activities first hand and that are willing to provide that information can be a challenge. The timeliness and reliability of the source of information may be the difference between being able to target key adversary financial personnel and not targeting them. Source directed requirements can be leveraged to further exploit promising, authoritative, and proven HUMINT sources for additional or follow-on intelligence about financial networks and sources and methods of threat finance. Members of threat groups that have participated in actions or activities that resulted in fund raising can be excellent sources of information. Bankers, farmers, merchants, and other businessmen may be useful sources of information about the sources and methods of threat financing as well as the costs of routine items, a piece of information that is essential for accurately estimating the operating costs of adversaries.

(1) (U//FOUO) Another potentially important source of financial intelligence is detainees and enemy prisoners of war. Interrogation of detainees can provide a wealth of detailed and sometimes timely intelligence about adversary financial operations depending upon the detainees' level of involvement in threat finance related tasks and activities. The individual's role in the organization or their proximity to financial activities will determine what they know about the financial activities of the adversary. For instance, it may be appropriate for a low-level fighter detained on the battlefield to provide information on who they are paid by, what their salary is, what their bonuses are, how often and where they are paid; how they are trained; what resources (e.g., housing, uniforms, food) they are provided with and what, if any, fund raising activities they have engaged in. Captured individuals who are engaged in threat finance may be able to provide great detail about financial operating methods and sources of income but their knowledge may be limited to one level above and one level below themselves in the threat finance organization and that knowledge will diminish over time or become

irrelevant if the adversary adjusts their operating methods. Because the threat finance network is so complex, diversified, and distributed, the analyst will need to build a composite picture of the network from snapshots and snippets of information rather than from a single, authoritative source with knowledge of the entire network. Integrating CTF analysts with interrogators is essential. Because the type of intelligence that is appropriate to obtain is highly dependent on the individual being interrogated, close coordination can help tailor the questions appropriately and immediate feedback can be crucial to further interrogation and vetting intelligence.

(2) (U//FOUO) Tactical questioning provides a very limited ability to identify persons of financial interest or to uncover financial operations. Tactical questioning is performed over a very short period of time and is typically oriented towards force protection and identifying immediate threats. Tactical questioning can be a useful tool for financial intelligence if the units involved know ahead of time that they may encounter a situation of financial importance.

c. (U//FOUO) Other forms of intelligence can also be obtained with traditional intelligence collection management procedures and processes. Intelligence support to CTF does not require specialized collection management procedures even if some of the specific intelligence requirements are highly technical or specific.

(1) (U//FOUO) SIGINT Tasking. SIGINT, electronic intelligence and communications intelligence, provides excellent current information on the communications between persons involved with threat finance activities. CTF analysts should develop an understanding of where personnel associated with threat financial activities are operating and how they communicate before developing requests for SIGINT support. One of the issues for CTF analysts will be the vast amount of information that can be generated through SIGINT sources and being able to read and interpret that information in a timely manner for use in current and future operations.

(2) (U//FOUO) Geospatial Intelligence (GEOINT) Tasking. Imagery (electro-optical/Infrared, RADAR, and/or full-motion video) to support CTF can be tasked via standard collection management processes. CTF analysts should develop an understanding of where and when the threat financial activities are being performed and the indicators of threat finance activities that can be observed. Availability of collection assets, weather, environmental conditions, and visibility of the desired targets are all issues that affect the timeliness of the response.

d. (U//FOUO) Site exploitation for financial intelligence can provide critical information on the financial health of an adversary. The presence of cash, abundant ammunition, new and modern weapons, sophisticated personal protection equipment, night vision goggles, computers, laptops, phones, billing/shipping records, ledgers, and high quality communications equipment are all strong indicators of financial support and capability. CTF analysts should maintain a continuous record of site exploitations to be able to evaluate increases (or decreases) in the adversary's threat potential, or capabilities, and to ascertain financial, and other materiel, distribution patterns, and

Chapter V

networks. Chapter V of the US Army Asymmetric Warfare Group's *Counter Threat Finance Handbook* provides an excellent outline of the tactical considerations for site exploitation.

e. (U//FOUO) Biometric exploitation of the individuals and items collected (e.g., hawala ledgers, receipts, computers) on the site can provide useful information as to their identity, past activity, and/or current role in the adversary organization. This may be especially true if the individuals involved work on multinational facilities or are involved with contracts that provide support to multinational forces.

f. (U//FOUO) Document exploitation, especially of ledger, can provide detailed intelligence of operating budgets in the operational area, to include revenue streams, operating costs, and potential additions, or depletions, to strategic or operational reserves, as well as threat finance networks, sources, payees, and pecuniary amounts. JFCs should ensure that sufficient and trained personnel are used in the exploitation of documents and electronic media. These are time consuming tasks that require expertise in translation, document exploitation methods, and financial expertise. CTF analysts should match information obtained from documents and media exploitation to existing intelligence to provide JFCs with a better understanding of the adversary's financial operations and possibly to identify targets. Document exploitation should be performed by CTF organizations at higher levels of command having the time, staffing, and ability to fuse various information sources to support this type of work.

"As for the needs of the jihad in Afghanistan, the first of them is financial. The mujahidin of the Taliban number in the thousands, but they lack funds. And there are hundreds wishing to carry out martyrdom-seeking operations, but they can't find the funds to equip themselves. So funding is the mainstay of jihad. ...And here we would like to point out that those who perform jihad with their wealth should be certain to only send the funds to those responsible for finances and no other party, as to do otherwise leads to disunity and differences in the ranks of the mujahidin."

**Shaykh Sa'id Mustafa Abu'l-Yazid
al-Qaida Leader in Afghanistan**

4. (U//FOUO) Processing and Exploitation

a. (U//FOUO) Processing and exploiting financial intelligence at the joint task force, regional command or division level and below is exceptionally difficult because of staff limitations, the fast pace of operations and the tremendous number of adversary personnel that may be encountered. Organizations like the ATFC and the ITFC have considerably larger staffs and have the responsibility to support CTF operations across the operational area. It is important to point out the processing and exploitation of financial intelligence by military CTF personnel is primarily to support military operations and second to support law enforcement, regulatory or political actions, and activities.

b. (U//FOUO) Tactical CTF organizations will typically have little time or expertise to analyze information on financial transfers, currency exchange rates, routing, and other significant aspects of CTF which can be highly specific and technical. Additional processing and exploitation may be required to assist analysts who are not well versed on such subjects. Exploiting the attributes, or information, that describe the data, also known as meta-data, may assist with pattern, trend, and/or network analyses. As with all steps, particular care needs to be taken to ensure analysts and intelligence professionals understand the effects, impacts, and limitations of processing and exploitation to prevent compounding errors in analysis.

5. (U//FOUO) Analysis and Production

a. (U//FOUO) Military CTF analysts, especially at the lower levels of command, are focused on using financial information to support targeting. This requires analysts to develop intelligence which will tell them: who the adversary financial operators are, which groups they support, the operating areas they support, the sources of funding for the groups in their operating areas, how the adversary manages and controls their finances, how the adversary transfers and moves funds, to whom, how, and for what, the adversary distributes and disperses their funds, where the threat financial networks are vulnerable and how to best engage those networks.

b. (U//FOUO) Threat finance analysis is often complicated by a number of factors to include:

(1) (U//FOUO) Threat financial intelligence is often sparse and has limited specific details.

(2) (U//FOUO) Empirical data on the business and financial practices of adversaries, or threat networks, are scarce, or in short supply. Very little data is available that would allow analyst to conclude that the adversary has performed the same task the same way two times in a row.

(3) (U//FOUO) Valuable threat financial intelligence has been lost in the past because units did not know how to report relevant financial data, or did not think that reporting discoveries of money, items of value, financial documents, and related materials were of interest to military intelligence staffs.

(4) (U//FOUO) Significant variations in the way different adversary organizations conduct the same tasks, such as kidnapping or extortion.

(5) (U//FOUO) Tasks and procedures associated with each fund raising activity are typically subject to the expertise and whim of the leader of the group. Constant replacement of leaders means a constant change in operating procedures if the leader of the group is in control of the financial activities of the group.

Chapter V

(6) (U//FOUO) Western ways of looking at financial operations often do not match up with the situations encountered in non-western areas (e.g., the Middle East, Africa, and Afghanistan).

For a more detailed description of Analytical Techniques used in CTF, refer to Appendix C, “Analytical Techniques”

6. (U//FOUO) Dissemination and Integration

a. (U) There is nothing regarding CTF intelligence requiring significant changes to dissemination and integration processes and procedures, but two issues, not unique to CTF, have been raised which warrant additional comment.

b. (U) First, where units are executing CTF and are submitting materials, intelligence, and media, up the chain of command or to other agencies or departments for further exploitation, special care and effort should be taken to ensure the executing unit is included in the dissemination of any resultant intelligence. There is anecdotal evidence that units are not receiving the intelligence generated from their missions. This has multiple effects. First, the importance of the operations that the unit is conducting is questioned. Second, the value in submission for exploitation without feedback is minimized, causing a critical source of intelligence to dry up. Third, the unit is not able to conduct subsequent operations based on the intelligence gathered in previous operations.

c. (U//FOUO) The second issue requiring additional discussion is the difficulty of data integration. There is no single, user-friendly, information management tool, relational database, or information technology infrastructure that the CTF community can leverage to analyze and exploit fused data from disparate data sources in an integrated fashion. Text based information databases or information libraries only provide access to information but do little to help in the detailed analysis of the information. Specialized software that can store and manipulate information and then export that information to other specialized software is essential. The ability to detect trends and patterns is based on the ability to collect and review intelligence over an extended period of time. Information sharing is performed on a regular basis by CTF organizations. Receiving feedback on how information is used is often difficult to obtain. The JFC and his staff should remain diligent to ensure integration is occurring across the board. In high operational tempo environments with limited manpower and resources, it becomes too easy to lapse into default channels, databases, and reports. Diligence by the JFC and the key intelligence leaders on the staff can ensure that intelligence is being shared with all appropriate stakeholders. It is essential to remember that the efforts of partner organizations are often far better suited to the CTF mission and that the pay-off of integrating intelligence with them in the past has been beneficial.

d. (U//FOUO) **Products**

(1) (U//FOUO) **Financial Intelligence Products for JFCs.** CTF products may include: answering requests for information, analytical presentations concerning specific activities of adversary personnel, information briefings, additional information added to targeting packages, nomination packets for targeting adversary personnel, briefings on current threat financial situations, briefings on threat financial operations, briefings on the local economy or resources that are being exploited by adversaries, providing recommendations on how to engage financial targets, research on subjects referred to the TFC by the JFC and other products as necessary. CTF analysts should work with the JFC's staff to determine the best manner of presenting information to the JFC (e.g., map graphics versus flow and link charts).

(2) (U//FOUO) **Financial Intelligence Products for Policy Makers.** These products might focus adversary current and potential economic, or financial, strengths and weaknesses; HN economic conditions and financial system capabilities; high-level government and police corruption (or cooperation). Policy makers are looking for information that will help them determine how to employ current resources, request additional resources, request support from other USG departments or agencies, request changes to the law or regulations, or request support from the HN.

(3) (U//FOUO) **CTF Support to JIPOE.** Integrating CTF-related intelligence into the JIPOE should give the JFC and the staff a more holistic appreciation of the strengths, weaknesses, capabilities, and gaps of both the adversary and the operational environment. Identifying these will be critically important to selecting and rejecting courses of action.

(4) (U) **Financial Order of Battle (FINOOB) Framework.** Order of battle is the identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force.

(a) (U) DOD has traditionally used order of battle to assess the capabilities of its adversaries. By assessing common elements found in our adversaries' financial operations—such as composition, disposition, strength, personnel, tactics, and logistics—commanders can gain an understanding of what they might encounter while executing an operation and identify vulnerabilities of the adversary.

(b) (U) A comprehensive and standardized framework for a FINOOB is needed for targeting an adversary's financial infrastructures for major vulnerabilities. This FINOOB is designed to seamlessly integrate with, and not replace, other orders of battle (e.g., Air, Naval, Electronic). Additionally, this describes the elements of a financial system of a generic adversary organization. The existence of an element in the FINOOB does not indicate that a corresponding element will exist within every adversary organization nor should it suggest sufficient fidelity of information and intelligence exists to fully describe all elements. The FINOOB can assist greatly in integrating CTF-related

Chapter V

intelligence into the JIPOE. As with all other orders of battle, the framework should be adapted and tailored to describe the adversary.

For a more detailed description, refer to the Counter Threat Finance Roadmap.

CHAPTER VI
ASSESSMENT

"The amount of assets blocked under the public designation process is not, however, a primary measure of effectiveness of antiterrorism programs.... In addition, the blocking of terrorist organizations' assets, with the notable exception of the Taliban, tends to be a small amount of funds.... While freezing the funds of terrorists can be used as a tool against terrorist organizations, it is by no means the only or most effective means to disrupt these organizations."

***Disrupting Threat Finances:
Using Financial Information to Disrupt Terrorist Organizations
Wesley J.L. Anderson***

1. (U) Background

a. (U) Assessment is a process that measures progress of the joint force toward mission accomplishment. JFCs continuously assess the operational environment and the progress of operations, compare them to their initial vision and intent, and adjust operations based on their assessment. The assessment process is continuous and directly tied to the JFC's decisions throughout planning, preparation, and execution. Staffs monitor key factors that can influence operations and provide the JFC timely information needed for decisions. Successful JFCs devise ways to continually update their understanding of the operational environment and assess their progress toward achieving assigned objectives without mistaking activity for progress.

b. (U) JFCs should know the importance and use of CTF capabilities within the context of measurable results for countering adversaries and should embed this knowledge within their staff. By assessing common elements found in adversaries' financial operations, such as composition, disposition, strength, personnel, tactics, and logistics, JFCs can gain an understanding of what they might encounter while executing an operation and identify vulnerabilities of the adversary.

c. (U) Adversaries cannot conduct high tempo operations without significant financial and logistical support. Movements of personnel, weapons, ammunition, explosives, and technology must be financed, or paid for. Terrorist financing incorporates two distinct sets of financial activities; fund-raising through licit, or illicit channels, and financial facilitation through hawala networks and other money service providers, or the international banking system.

(1) (U) The first activity involves the provision of funds required to carry out, or support terrorist operations. This includes raising funds to pay for such mundane items as food, lodging, transportation, reading materials, audio-video equipment, and IED precursors; training; and propaganda. Funds can be raised through illicit means, such as drug and human trafficking, arms trading, smuggling, kidnapping, robbery, and arson. Funds raised in this fashion must be "laundered" to enter the legitimate international

financial system and are more susceptible to being detected with traditional anti money-laundering tools.

(2) (U) Alternatively, funds can be raised through ostensibly legal channels. Terrorist organizations can receive funds from legitimate humanitarian and business organizations and individual donations. Charities raising funds for humanitarian relief in war-torn regions may or may not know their funds are supporting terrorist activities. Corrupt individuals at charities or at recipient organizations may divert funds to terrorist organizations. This appears to be one of the main means through which al Qaeda raises funds. Legitimate funds are commingled with illicit funds destined for terrorists, making it extremely difficult for governments to track terrorist finances in the formal financial system⁵. Such transactions are perfectly legal until they can be linked to a criminal, or terrorist, act⁶. These sums of money may also be small relative to the massive volume of financial transactions that move through international financial systems; they are, therefore, extremely hard to detect in the absence of other indicators, regarding the identity of the persons involved. Profiling the identity of the individuals making these transactions raises a number of legal and civil liberties issues, making it a difficult task to accomplish⁷.

(3) (U) The second activity involves employment of hawala networks and other money service providers, as well as the international banking system to transfer funds, finance commercial and capital transactions, or launder ill-gotten gains from drug-trafficking and other criminal money-making activities. Financial-service providers may be either witting, or unwitting, participants; and they facilitate the global proliferation and procurement of weapons, WMD and IED parts, components, and technology

d. (U) To be successful in CTF operations, the JFC should be proactive, assessing threats, understanding the structure and adaptive abilities of adversaries, and responding with resources and flexibility to head off their next move.

e. (U) Also, taking a proactive approach to pursuing an illicit financier or adversary threat finance operative and applying intense pressure will often force the target into the open. The best CTF actions facilitate and anticipate the mistakes of the network. CTF actions may occasionally be wrong, but the illicit financial network need only make one mistake to be apprehended. Therefore, the targeting team should always be aware of local and regional threat finance indicators, trends, and patterns and be ready to pounce.

2. (U) Metrics

a. (U) A metric can be defined as a standard of measurement or the statistical analysis and measurement of a system with a focus on the results or consequences of actions taken. Metrics require the collection of intelligence and operational information in a manner, which can be converted to some form of statistics. These statistics are then used as part of the analytical process to report results and to determine how well efforts

have been expended against the adversary. Metrics are used for several purposes, including but not limited to:

(1) (U) Analyzing how effective the combined efforts of DOD, other USG agencies, multinational partners, and HN organizations are against the financial support networks of the adversary;

(2) (U) Identifying the scope or magnitude of a problem;

(3) (U) Determining the resources to be allocated against a problem set; and

(4) (U) Determining if efforts will be continued against a problem set.

b. (U) Information used to generate metrics should be current and relevant to the actions and operations being undertaken against adversaries. This usually requires coordination with intelligence organizations to ensure that CTF information is included in their regular intelligence collection routines.

c. (U) JFCs use metrics to show progress, identify problem areas in their campaigns and operations against adversaries, identify areas of focus, and to request additional resources, if necessary. Policy makers use metrics to enable informed decision-making; (e.g., to prioritize threats and to take necessary actions, including the funding and resourcing of successful programs and initiatives, at the expense of unsuccessful ones).

d. (U) Intelligence provides the background information needed to detect, identify, define and track the problem set. Operational information provides context for the JFC to take actions to engage the problem set and the outcomes of those actions.

e. (U) Metrics should be based on information which is critical to understanding the impact of operations against adversaries. Too much focus on actions against key threat finance personnel and not enough attention on degrading the networks capabilities and resources may yield misleading and inaccurate assessments. For instance, removal of key leaders would only be an important metric if the adversary was not able to replace those leaders and pursue their objectives, something which is rarely the case.

f. (U) The collection of information to prepare metrics should be conducted in a consistent and continuous manner using common and established information requirements.

g. (U) Military metrics on threat finance often will not be highly accurate because much of the information analysts have is vague and lacks the detail to create the necessary statistics. This often means only an estimate or subjective judgment can be rendered.

Chapter VI

h. (U) Metrics on threat finance may appear to be of little value because it is very difficult to obtain fast results or intelligence that can be immediately actionable. Actions against financial networks may take months to prepare, organize, and implement, due to the difficulty of collecting relevant detailed information and the time lags associated with processing, analysis, and reporting findings on threat financial networks.

i. (U) Analysts preparing DOD metrics should only attempt to account for efforts that include DOD participation. Combining the efforts of multiple agencies to determine the “Whole of Government” effort will require a central repository of information and tasking from an organization like the Terrorist / Insurgent Finance Working Group, TF sub- counterterrorism security group or a Joint Intelligence Task Force for CTF in order to perform this analysis.

j. (U) Baseline information is needed to establish a frame of reference, to generate reliable estimates, to demonstrate cause and effect, and to measure program, or campaign, effectiveness.

3. (U) The Focus of Assessment

a. (U) In order for an assessment to help the JFC determine the level of success an operation is having, the assessment needs to answer at least two fundamental questions:

(1) (U) How successfully is the military accomplishing the actions/tasks/missions it is executing?

(2) (U) How much has the action/behavior of the adversary changed in a direction that meets the desired, or intended, objective?

b. (U) Traditionally, the military has been very good at monitoring and assessing the success of assigned actions, tasks, and missions. However, in CTF, where the actions, tasks, or missions may not be neatly aligned with traditional skills and may challenge organizations to operate in new fields where they may lack experience, assessing the success of actions, tasks, and missions may warrant additional scrutiny by the JFC.

c. (U) Ultimately, the JFC succeeds by getting (cajoling, coercing, forcing, manipulating) the adversary to behave in certain ways (i.e., stop funding operating forces). Assessing how much the adversary’s actions or behaviors have changed in response to CTF operations is the critical element to assessing mission success. Inevitably, the adversary will adapt to CTF actions in unforeseen ways. The JFC’s staff should assess the adversary’s behaviors based on the JFC’s desired end-state and determine whether the adversary’s behavior is moving closer to that end-state.

d. (U) While it is clear the second of the two questions above is the more important, it alone will be insufficient to help the JFC change strategy or tactics, alter the tempo, or reallocate resources to succeed. This means the effort of those conducting the

assessment cannot be fully geared towards answering the second question to the exclusion of all others. The actual balance of effort will vary from mission to mission and will depend on several factors, including:

- (1) (U) Types of actions, tasks, and missions DOD is called upon to conduct;
- (2) (U) Degree of interdependence with other mission partners (e.g., USG agencies, HN, NGOs, IGOs);
- (3) (U) Complexity of the operating environment;
- (4) (U) Geographic span of the threat finance network; and
- (5) (U) Number of sources of threat finance funding.

e. (U) As such, the JFC will need to carefully monitor not only the information contained in the assessments but the process of the assessment itself to ensure it is delivering the types and quality of information needed to inform decision-making.

4. (U) Strategic Metrics Preparation

a. (U) Preparing a consolidated, whole-of-government set of strategic metrics for threat finance will be extremely challenging and highly subjective until comprehensive collection and analysis procedures are established between DOD and other USG agencies. Persons tasked with preparing metrics should consider some of the following information prior to performing their analysis.

b. (U) Strategic metrics are generated from all-source intelligence and tactical actions against adversaries. There are no current dedicated data collection systems supporting the presentation of fact-based, objective reporting on actions against the full spectrum of threat financial networks.

c. (U) Defining the scope of the metrics for threat finance is difficult. Threat finance is a broad term encompassing at least three different categories of networks (e.g., terrorist, insurgents, drug trafficking organizations). These categories are fundamentally distinct and it is not recommended they be combined into a single system for reporting. There are multiple adversary networks from each of these categories operating in each of the GCC AORs. In most cases, information on the networks has not been developed to the point key functional nodes, operating methods, key personnel and vulnerable points have been fully identified or engaged.

d. (U) Actions taken against one organization or network may have no impact on the other organizations in the same category or in the other two categories. Actions taken against financial personnel and resources of a well-organized and resourced adversary may have a time delay before an adverse impact is achieved or noticed. Depending upon

Chapter VI

the size and financial assets of the adversary, the impact of operations may not be felt for one or more reporting periods.

e. (U) The JFC will need the staff, subordinate organizations and national intelligence systems to begin collecting specific information and intelligence and to begin conducting actions against adversaries to generate the statistics to support metric development and reporting.

f. (U) Terrorist networks, insurgent groups, and drug trafficking organizations share a number of TTPs in common, especially as they strive to sustain or grow their respective organizations. Data requirements, regarding budget operations and accounting practices, for example, transcend the motivations and objectives of these disparate yet, overlapping, threat groups. Suggested information and intelligence – common to all three threat groups – needed by the JFC includes but is not limited to:

- (1) (U) Listing of adversary groups by name;
- (2) (U) Total number of adversary groups by geographic operating regions;
- (3) (U) Functional organization, nodes, and key personnel identified, located and mapped;
- (4) (U) Detection and identification of relationships among adversaries;
- (5) (U) Total number of reported actions, incidents, and financial activities associated with adversaries by type, direction of support flows, group and geographic locations; and
- (6) (U) Reported actions or incidents associated with adversaries for this reporting period.

g. (U) Extant products such as those produced within the JIPOE process should contain the required information and intelligence and should be mined before tasking staff or subordinates to re-create it.

h. (U) The following are examples of tactical metrics:

- (1) (U) Detection and identification of adversaries;
- (2) (U) Detection and identification of functional organizations and chains of command;
- (3) (U) Detection and identification of key personnel for targeted adversaries;
- (4) (U) Detection and identification of threat financial networks and their associated operating areas;

- (5) (U) Number of financial activities associated with adversaries;
- (6) (U) Detection and identification of previously undetected fund raising methods used by adversaries;
- (7) (U) Detection and identification of previously undetected financial resources exploited by, or associated with, adversaries, to include locations, estimated value, and resource vulnerability;
- (8) (U) Detection and identification of cooperative relationships identified among adversaries;
- (9) (U) Current number of persons and organizations being “targeted”;
- (10)(U) Identified changes in adversary operations; and
- (11)(U) The number of actions that were taken against targeted adversaries.

DRUGS AND TERRORISM

Terrorist groups, therefore, increasingly need new sources of funds, and the drug business fills this need perfectly. The UN estimates that the international drug trade generates \$322 billion revenue annually, making drugs by far the most lucrative illicit activity. According to the UN, revenues from other types of illicit transnational activity, such as arms trafficking and alien smuggling, are small by comparison. Drug trafficking generates many different revenue streams, including the taxing of farmers and local cartels, as well as the provision of security for all aspects of production, trade, and distribution. Terror organizations do not, in general, require massive sums of money for their operations; nonetheless, they must finance recruiting, training, infrastructure, government bribes, equipment, and logistics. The Madrid train bombing by al-Qaeda or an affiliate was funded almost entirely by the sale of illicit drugs.

**Countering Transnational Threats
Matthew Levitt and Michael Jacobson**

5. (U) Assessment Considerations for the Joint Force Commander

The following is a list, not an exhaustive one, of some assessment issues the JFC engaged in CTF should consider:

- a. (U) The JFC and staff should consult with participating agencies and nations to establish a set of metrics which are appropriate to the mission or lines of operation assigned to the CTF organization.

Chapter VI

b. (U) The JFC and staff should consult with participating agencies and nations to determine which metrics are already being collected and reported upon which are appropriate to the mission or lines of operation assigned to the CTF organization.

c. (U) The JFC and staff should consult with other organizations, units, and commands engaged in CTF to determine which metrics are already being collected and reported upon which are appropriate to the mission or lines of operation assigned to the CTF organization.

d. The JFC and staff should consider possible unintended consequences that may occur when the metrics being measured are moving toward a desired trend. For example, a measure of effectiveness (MOE) may be to diminish threat finance generation from licit sources. The desired trend could be a decreasing trend in such areas as donations from businesses or financial support from NGOs. However, an unintended consequence that may occur is that funding could start coming from other sources such as drug trade, theft, or kidnappings for ransom. Consideration of possible unintended consequences will allow the JFC to be more successful disrupting an adaptable adversary that will change their tactics when their original tactics have been interdicted.

6. (U) Assessment Framework

There has been a longstanding need for MOEs focused on diplomatic, informational military and economic efforts in places prone to conflict. Traditionally, USG agencies have tended to measure outputs, such as the number of schools built, miles of roads paved, or numbers of insurgents killed. Outputs, however, measure what is done and not what is achieved. Outcomes, or "effects" indicate the success or failure of project or mission efforts, and seek to measure the attainment (progress toward/away) of conditions that engender stability and self-sustaining peace.

For more information on assessment, refer to JP 5-0, Joint Operation Planning and Commander's Handbook for Assessment Planning and Execution

For a list of illustrative MOEs, refer to Appendix D, "Illustrative Measures of Effectiveness."

CHAPTER VII

OPERATIONAL IMPLICATIONS (U)

"The importance and use of CTF capabilities within the context of measureable efforts for countering our adversaries must become embedded knowledge within DOD. CTF concepts and doctrine will be applied throughout the full range of relevant DOD intelligence, planning, and operational activities, where appropriate."

**Department of Defense
Counter Threat Finance Roadmap**

1. (U) General

Improved command emphasis on CTF operations has realized some success in Afghanistan, Iraq, and elsewhere. However, stovepipe organizational constructs, still maturing CTF policies, insufficient doctrine, and inadequate training continue to hamper successful CTF operations. Full and effective implementation of CTF requires development and adoption of doctrine, organization, training, materiel, leadership, personnel, and facilities (DOTMLPF) solutions. Specifically, more work needs to be done to codify CTF within DOD, analyze existing doctrinal processes and publications to determine needed modification, provide organizational recommendations to support process change, and develop CTF training modules for JFCs, staffs, and subordinate echelons. This chapter discusses how changes within the DOTMLPF framework can enhance the effectiveness of CTF operations.

2. (U) Doctrine

a. (U) Currently there is no CTF doctrine within the DOD. DODD 5205.14, *DOD Counter Threat Finance (CTF) Policy* describes the need for doctrine for CTF but that effort will take time and will require significant coordination and comment from the CCMDs and Services.

b. (U) Considerations for further development or revision of joint doctrine include the following:

(1) (U) CTF is a non-traditional military activity that requires a higher level of coordination and integration of operations with the military and civil partners, and the HN where operations are being conducted. CTF should be of interest to JFCs at all levels of command because threat finance personnel and money flow from local and international points of origin to the battlefield. DOD will have to develop the procedures and negotiate the agreements that are needed to integrate DOD efforts with those of other USG agencies and not just share information. CTF will require political, military, law enforcement and regulatory actions to be successful.

(2) (U) A more thorough discussion is needed concerning CTF techniques and procedures in pertinent joint operations and functions including the JOPP as described in

Chapter VII

JPs 3-0, *Joint Operations*, and 5-0, *Joint Operation Planning*. This discussion could include CTF vignettes and considerations for making CTF a main effort during certain phases of a joint operation/campaign. These keystone documents should address the growing importance of the role of CTF in irregular warfare, COIN, and stability operations. Identification of CTF challenges that are unique to the various types of military operations can help planners adapt to emerging circumstances more quickly.

c. (U) Extensive discussions of interorganizational coordination are included in JPs 3-08, *Interorganizational Coordination During Joint Operations*, 3-33, *Joint Task Force Headquarters*, 3-57 *Civil Military Operations*, and 3-24, *Counterinsurgency Operations*, including a discussion of organizational approaches. These discussions should also highlight the importance of unified action when conducting CTF in the operational area. The discussion should address processes and organizational approaches that will create opportunities to fully integrate all counter financial operations into the accomplishment of joint operation/campaign objectives. In particular, CTF processes, should improve the speed, focus, and coordination of efforts among military and non-military organizations. CTF organizations will have to work very carefully with civil military operations (CMO) organizations to ensure that the CMO organizations are not perceived as acting as intelligence collectors for CTF. That perception within a local community would be catastrophic to civil military operators. CTF organizations should make an extra effort to glean information from CMO reporting and activities without directly involving the CMO staff in day-to-day collection of information.

d. (U) Identifying and incorporating compatible assessment techniques and procedures utilized by various CTF agencies and organizations will benefit assessment planning. Assessment needs to address virtually all of the above mentioned JPs. Preparation for and assessment of CTF should also be addressed in JPs 2-01, *Joint and National Intelligence Support to Military Operations*, and 2-01.3, *Joint Intelligence Preparation of the Operational Environment*.

e. (U) The importance, complexity, and breadth of CTF indicates the potential need for a new JP on CTF. This handbook could provide the core content. JP candidates that merit inclusion of CTF discussions include:

- (1) (U) JP 1, *Doctrine for the Armed Forces of the United States*.
- (2) (U) JP 1-06, *Financial Management Support in Joint Operations*.
- (3) (U) JP 2-01, *Joint and National Intelligence Support to Military Operations*.
- (4) (U) JP 2-01.2, *Counterintelligence and Human Intelligence Support to Joint Operations*.
- (5) (U) JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment*.

- (6) (U) JP 3-0, *Joint Operations*.
- (7) (U) JP 3-07.4, *Joint Counterdrug Operations*.
- (8) (U) JP 3-08, *Interorganizational Coordination During Joint Operations*.
- (9) (U) JP 3-24, *Counterinsurgency Operations*.
- (10)(U) JP 3-33, *Joint Task Force Headquarters*.
- (11)(U) JP 3-57, *Civil Military Operations*.
- (12)(U) JP 5-0, *Joint Operation Planning*.

3. (U) Organization

a. (U) As described in DODD 5205.14, DOD is responsible for supporting USG entities and partner nations in their efforts to deny, disrupt, or defeat and degrade adversaries' ability to use global licit and illicit financial networks to negatively affect US interests. A primary organization within DOD for this purpose is the Threat Finance Exploitation Unit. The TFEU is an interagency USCENCOM initiative that works with DOD and non-DOD intelligence, law enforcement, and regulatory agencies. It shares and deconflicts information and focuses on individuals or organizations that may be helping to financially support threats to national security. TFEU personnel are trained in the CTF field to ensure counter-finance intelligence reports are addressed and recorded. The TFEU was originally created for CTF activities in Iraq. However, its organizations and functions have been adopted by the other CCMDs and tailored to specific circumstance in their AORs.

b. (U) The Joint Staff should ensure that CTF is conducted in a uniform manner across the CCMDs. The development of multiple CTF efforts that do not synchronize would not be acceptable. CTF reaches across the globe and as such should be tracked across the AORs of multiple CCMDs. CTF processes and procedures should be developed to enhance the tracking of persons and activities across international boundaries and across continents. This indicates the potential requirement for a TFC in the Joint Staff. The placement of full-time liaison or operational staffs within the other Departments and Agencies that the DOD works with on CTF should be considered. Liaison officers typically do not bring the operational capabilities of their parent units. Placing CTF analysts within the staffs of other departments and agencies could greatly enhance the CTF efforts the entire USG. This type effort is already in place in a number of Departments or Agencies and would in most cases require establishment of memorandums of agreements between the departments and agencies involved.

c. (U) Establishment of TFCs at Units below the Division / JTF level are not practicable at this point in time, however, it is highly recommended that CTF trained

Chapter VII

personnel be integrated into the staffs at the Division or JTF level. CTF efforts at the tactical level are critical and this is the level of command that coordinates the efforts of the various Brigade Combat Teams and Marine Expeditionary Units / Forces.

4. (U) Training

a. (U) Training is necessary to ensure proper implementation of CTF. However, current CTF training within DOD is decentralized with little standardization or oversight. USSOCOM is currently spearheading efforts to develop standardized training courses that will have the consensus of the CTF community of interest. As part of this effort, new Universal Joint Task List (UJTL) items are being developed to reflect specific CTF UJTL that should be reflected in CTF training.

b. (U) Over the longer term, incorporation of CTF into functional training at Service schools should be considered to more fully integrate CTF into the JOPP.

c. (U) Another venue beneficial to CTF training is participation in joint exercises that have USG agency participation. Interagency partner participation in CTF scenario events and story lines will provide the JFC and staff greater understanding of non-DOD capabilities that can be employed in CTF efforts. Near-term opportunities include mission rehearsal exercises such as the Exercise UNIFIED ENDEAVOR series that have CTF events embedded for 2011, with greater CTF injects anticipated for 2012 and beyond.

d. (U) CTF training should be institutionalized across the force. To date, no well-understood, non-negotiable core curriculum has emerged. The result has been a variety of courses being delivered to meet unit or service specific needs where recipients exit the courses with widely variant understanding and abilities. This has also meant considerable effort and resources have been expended to develop training to support a unit or service's specific needs because no standard curriculum exists.

(1) (U) CTF training should be comprehensive. The core curriculum will address the training requirements throughout individuals' careers and throughout the deployment cycle of units. The CTF curriculum should consider the full range of military operations CTF should support from sanctions enforcement to COIN to defense in depth of the homeland.

(2) (U) CTF training should be tailorable. The core curriculum should be adaptable to a unit's specific mission or environment. Additionally, any effective instructor will need to tailor the curriculum to the requirements and experiences of the intended audience (e.g., special operations, JTF planners, intelligence analysts).

(3) (U) CTF training should be modular. Not all individuals or units will require all aspects of the CTF curriculum. A modularized curriculum will enable leaders to tailor the training of their units and subordinates to the roles and missions with which they will be tasked.

(4) (U) CTF training should be flexible in terms of delivery. The curriculum should accommodate the full spectrum of delivery from intensive, instructor-led, face-to-face instruction at the NATO School to on-the-job-training (OJT) for forces in garrison to computer-based delivery for users in remote or band-width austere environments. Further, the curriculum should be flexible enough to allow for inclusion of new and emergent instructional technologies.

(5) (U) CTF training should be supported by handbooks, training circulars and other publications. These publications will serve to update best practices from operational experience as well as share experience and lessons learned across different disciplines and field with the express purpose of ensuring the CTF curriculum and the resulting training are dynamic and relevant to the needs of the individuals and units. The Asymmetric Warfare Group's Tactical CTF Handbook and Army's CTF Training Circular are examples of the types of publications, which can support CTF training.

5. (U) Materiel

A common database for CTF needs to be identified within DOD. If an extant database is chosen, then there is minimal impact, adapting the given data structure to incorporate the needed fields and processing existing datasets for integration. When selecting a database, careful deliberation will need to be paid to balancing the requirements of security and maximum availability of information with the wide array of users throughout the DOD and other USG agencies; including local, state, federal and international law enforcement; and multinational partner nations.

6. (U) Leadership and Education

a. (U) CTF and -related planning, capabilities, TTP, and coordination needs to become an integral part of joint professional military education (JPME) and service education programs including Capstone, Keystone, and Pinnacle programs. This education should include planning considerations for early CTF efforts. Our military leadership, given the current global environment, may significantly benefit from education that provides them with the knowledge necessary to analyze how to better utilize counter financial operations as an integral part of ongoing military efforts.

b. (U) The creation of an educational curriculum focused on CTF is in its infancy stage. Currently, the National Defense University (NDU) staff has agreed to non-resourced injects into the Chief Financial Officer Academy and into the curriculum of some electives that focus on stability and reconstruction at the Industrial College of the Armed Forces.

c. (U) CTF should be included within the JPME curriculum to ensure exposure to CTF across the forces and develop a fundamental understanding of the role of CTF in defeating adversaries. While a separate block of instruction for CTF may not be warranted, CTF should be included in planning and operations blocks of instruction

Chapter VII

especially as they relate to the conduct of irregular warfare. CTF should also be addressed in the context of military operations and civil organization activities. Fully resourced inclusion in the NDU curriculum and JPME II will require more formalized staffing.

d. (U) **Career Progression Education**

(1) (U) **Entry.** Entry level personnel require education on CTF, especially in those career fields most likely to be assigned to CTF billets, including but not limited to intelligence and finance. CTF education for entry-level personnel should focus on the fundamentals of CTF, including what CTF is and why it is important, the unique considerations of analyzing, planning, and executing CTF, as well as lessons learned and TTPs related to CTF.

(2) (U) **Mid-Career.** Military professionals receiving education during the middle of their careers should receive instruction on CTF which builds on the entry-level education they received and which leverages their operational and staff experiences. This education will include more in-depth development of the specific techniques and methods adversaries use to finance operations, US and multinational capabilities in the CTF fight, USG and international organizations involved in CTF including their culture, roles, authorities, and structures.

(3) (U) **Senior.** Senior leaders, including flag and general officers, require education on CTF to inform strategy selection and policy development as well as force generation and employment decisions. This training should be included as part of the CAPSTONE and PINNACLE series of courses. These courses will introduce CTF to those senior leaders with limited or no previous exposure. It will also explore the specific difficulties of conducting CTF with and in support of USG and international mission partners, especially including civil agency roles and authorities as they relate to CTF.

7. (U) **Personnel**

Military personnel with CTF expertise should be identifiable in the military personnel system. A unique military occupational specialty would be desirable, however, an additional skill identifier would be an acceptable alternative. It is also critical for CTF to be included in the career progression for military personnel. Assignments to military organizations outside of the soldier's career path can harm the soldier's chances for promotion and further assignments. If standing units for CTF are to be established, tracking personnel with training and expertise throughout the DOD, including the Reserves and National Guard, will be a required mechanism to ensure the training and expertise over the course of a service member's career is best utilized.

8. (U) **Facilities**

CTF personnel should be integrated into the staff at all levels of command and as such there will be no impact on facilities.

APPENDIX A COLLECTION GUIDELINES (U)

"Jihad needs a lot of money, and the Jihad battlefields need much money. ...Jihad with money is also an obligation. And here we, in the battlefield in Afghanistan, are lacking a lot of money and a weakness in operations because of lack of money, and many mujahideen are absent from Jihad because of lack or absence of money with which they can carry out Jihad. Even many brothers...who want to sacrifice themselves for the cause of Allah, we cannot prepare them because of lack of money."

**Shaykh Sa'id Mustafa Abu'l-Yazid
al-Qaida leader in Afghanistan**

1. (U) Background

a. (U) This appendix outlines a notional set of collection guidelines emphasizing current theaters of operation. It can be modified to meet specific or general requirements as necessary. Intelligence collection efforts are based on several information requirements, which include but are not limited to the PIRs, HUMINT requirements, source directed requirements, and evaluations of reporting. JFCs should understand that the interagency community is dependent upon information gathered by the military for leads that may lead back to the United States. Collection efforts should focus as much on how the threat financial networks operate as looking for individual persons within the network. Collection requirements will change between levels of command and may not smoothly transition from the higher headquarters to the lowest headquarters in a chain of command. Collection emphasis will change as the situation on the ground changes with force protection being the highest priority. Listed below are more detailed questions of interest, which if successfully answered, can facilitate CTF operations. This information is passed on to personnel that are responsible for obtaining the information.

b. (U) The ability of the collection systems to obtain and provide this information is based on a number of factors which may include:

(1) (U) The priorities established by the JFC.

(2) (U) Availability of personnel and systems to collect the required information.

(3) (U) Providing geospatial and timing information on where to focus the collection systems.

(4) (U) The availability of a TFC to work with and coordinate with information collectors.

(5) (U) The training and experience of the personnel conducting the collection of information.

(6) (U) Presence and levels of activity of adversary personnel and operations in the collectors operational area.

(7) (U) Finding and accessing public records.

(8) (U) Access to commercial information and company records.

(9) (U) The availability of translators and HN subject matter experts.

c. (U) The collection of information should serve as many organizations as possible. Common information requirements often include:

(1) (U) Positive identifiers of adversary personnel to include names and aliases, physical description, biometric information.

(2) (U) Positions, job titles, and functional areas.

(4) (U) Tribal affiliation.

(5) (U) Contact information, home addresses, work locations.

(6) (U) Responsible areas for all persons who are involved in financial and logistics activities.

(7) (U) Relationships between adversary personnel and other people are included.

(8) (U) Provide data to the interagency community anytime there is a trace leading back to the United States or a US person or entity.

(9) (U) Provide military grid reference system coordinates up to 10 digits, whenever possible.

2. (U) Collection Requirements

Collection requirements for CTF may include but are not limited to the following:

a. (U) Who are the financiers and donors that provide money to adversary groups?

(1) (U) Who are the local financiers (e.g., have the ability to donate money from their personal wealth, money from the proceeds of an organization they own or operate, or those who raise money to provide a portion of that money to adversary groups)?

(2) (U) What businessmen and wealthy families pay protection money to be able to operate without interference? Who is going beyond the cost of doing business to support the insurgents?

(3) (U) Who are the in-country, but outside the local area financiers?

(4) (U) Who are the foreign financiers? What is the originating source of the funds outside of the operational area and how is that money brought in?

(5) (U) Who are local persons and businesses that raise money, donate money, or that solicit money to give to adversary groups?

(6) (U) Who are persons and businesses that are outside the local area and that are sending money to adversary groups in the operational area?

(7) (U) What is the predominate currency provided to groups receiving the money?

(8) (U) How much money is each financier providing, how often is their provision, who is the money is given to and dates, times and location the transaction took place?

(9) (U) How do the financiers transfer funds to the groups that they support?

(10)(U) What are the political and tribal connections utilized by the financiers to protect their activities?

b. (U) What methods do adversary groups use to raise money? The following activities are some of the methods that are used to raise money but more information is needed on exactly how groups are executing each of these funding schemes to make money. Additionally, more needs to be known about what percentage each funding scheme contributes to the overall financial income of the groups:

(1) (U) Black market operations (e.g., sales of stolen goods).

(2) (U) Gray market operations (e.g., sale of legal but unlicensed goods like counterfeit digital video disks and clothes).

(3) (U) Drug trafficking and sales of pre-cursor chemicals.

(4) (U) Contractor support to the multinational bases (profits shared with insurgents).

(5) (U) Weapons and ammunition sales (includes explosives and IEDs).

(6) (U) Homemade explosives production and sales.

(7) (U) Donations from the Diaspora community across the world.

(8) (U) Donations from local businesses.

(9) (U) Solicitation, local (e.g., visits to mosques, businesses, villages asking for donations).

(10)(U) Solicitation, international (e.g., members of the group, family members, and supporters of the group) travel around to ask for money often in wealthier countries where there are significant expatriate communities or which have strong ideological affinity (e.g., Irish communities in the US for Irish Republican Army and/or Sinn Fein).

(11)(U) Night letters and village shakedowns.

(12)(U) Sales of animals and animal hides.

(13)(U) Loan fraud (taking out government loans and not paying them back).

(14)(U) Illegal roadblocks.

(15)(U) Kidnapping.

(16)(U) Extortion of persons and organizations (e.g., demands for money that if not met will result in the victim's murder, kidnapping, business shutdown, family harm, or public exposure).

(17)(U) Extortion of trucking companies.

(18)(U) Extortion of construction contractors.

(19)(U) Investments in businesses.

(20)(U) Control of legitimate businesses.

(21)(U) Theft, smuggling and sale of raw materials such as chromate ore, copper ore, uranium, gems, and timber.

(22)(U) Theft and sale of international aid (ranging from food to farming equipment).

(23)(U) Zakat collection - who is collecting the money and where is the money going? (Zakat is similar to tithing or giving alms.)

(24)(U) How much money is being made by each fund raising method, how often are the funds collected and where does the collected money go? Even minor bits of information can be helpful.

(25)(U) Identification of corrupt government officials that assist the insurgents by providing money, supplies, weapons, transportation, protection, or safe haven.

c. (U) Who are the money facilitators in the group? Facilitators manage, transfer, smuggle, move, handle, store, payout and distribute money but they are not the people that raise the money. Names, contact information, and operation locations for financial facilitators. The most effective engagement is to remove the financiers. Facilitators provide the trail back to the source.

(1) (U) Identify the persons in the group that manage and control the money for each group. Are pictures or a physical description available? Is information on their family members or close friends available? Who decides how the money is spent and who is responsible for handing out the money.

(2) (U) Operating locations and routes used by persons that transport or smuggle money between money providers and the operating cells that receive the money. Knowing how, when, and approximately how much money is transported is critical.

(3) (U) Identification of businesses that transfer or exchange currency in support of the adversary networks (primarily hawalas and money exchanges/changers but they also use banks).

(4) (U) Determine where groups store their money and how much money is usually kept on hand.

(5) (U) Do not expect a source to know account numbers unless they are personally involved in the process of depositing or withdrawing funds, accounting for or managing the money in those accounts. Information to collect includes the location and the names and contact numbers of the hawala, moneychanger or the banks used. Sources should also be able to provide general timeframes and amounts of money moved and the names of the people involved in the activity. Business cards are a great way to get contact information for hawala owners.

(6) (U) What are the names, positions, offices worked in and locations for corrupt officials that facilitate funding for the insurgents?

d. (U) How are adversaries managing and controlling their money?

(1) (U) Information is needed on the role the primary traditional/tribal decision-making bodies (e.g., shuras) play in raising, controlling, budgeting, managing, and distributing funds to the subordinate groups under their control.

Appendix A

(2) (U) More details are needed on how the shadow governance operates, its roles and responsibilities in providing financial and logistical support to the operating cells, the work that their supporting staffs perform, and how they receive and distribute money to the operating cells in their areas. What types of shuras or commissions have the insurgents set up to control and distribute their resources.

(3) (U) More information is needed about the support interface between the shadow governors and the provincial and district commanders who are the recipients and managers of the money given to their groups.

(4) (U) What are the names, positions and locations of the people that decide how money will be distributed within the organization? What is the frequency and amount of distribution? What guidance do adversary commanders receive on how to spend the money that they are given?

(5) (U) Whom do insurgents coordinate with and submit requests to when they need money? Approximately, how long does it take money to reach the requestor once a funding request has been approved?

(6) (U) What are the names and locations of the bookkeepers and accountants; to whom do they report financial information? Where are their books and records kept?

(7) (U) What are the names and contact information of the auditors that check the bookkeepers?

e. (U) How are adversary personnel moving their money between operational areas and safe havens or between AORs?

(1) (U) What locations and facilities in safe havens distribute money to the adversary personnel in the operational areas? Which groups are using each facility? How do insurgents exploit the facility for their use?

(2) (U) Which traditional/tribal decision-making bodies (e.g., shuras) are providing financial support to operations in the operating area?

(3) (U) What routes do the adversary personnel use to cross the border and how often do the adversary personnel come to these locations to pick up funds?

(4) (U) What are the names and locations of the hawalas and money exchange offices used to move money to the adversary personnel in the operational area? How much money is usually transferred at one time using the hawalas? Which days are monies transferred using the hawalas or money exchange offices?

(5) (U) What are the names of the couriers used by each adversary group to move money? What routes do these couriers typically use? What cover stories do the couriers use if stopped? What are the locations that the courier usually pickup and drop

off money? What types of markings are used on couriers' cars? What days of the week do the couriers travel to each location?

(6) (U) What is the name of the person for whom each courier works? How does this person coordinate the pickup and drop off of money between the person providing the money to the courier and the person receiving the money from the courier?

f. (U) Where are the adversary personnel spending their money?

(1) (U) Money is useless unless there is somewhere to spend it. Adversary personnel have to carefully watch how they spend their money. The more information available about where adversary personnel spend their money and the costs of operating, the easier it is to determine how much money is being channeled into the operating area and how much money is required to conduct operations.

(2) (U) What types of items can be bought in the local markets that could be used to support a adversary group other than basic foodstuffs and clothes?

(3) (U) What types of items in the local markets do not match up with the average local consumer? Remote control doorbells and garage door openers (when few people have garage doors), remote controlled toys, repair parts such as washing machine timers when no one uses electric washing machines, electrical supply stores when there is little electrical utility support in the area.

(4) (U) What is the location of local weapons dealers, what are they charging for weapons, ammunition, magazines, and repair parts? Who supplies the weapons dealers? Do the weapons dealers demand cash on delivery or do they extend credit to their customers? Weapons, communications, and transportation comprise the greatest operating costs for adversary cells; their payroll costs are minimal in comparison.

(5) (U) What is the local cost for renting a home, compound or building for use as a safe house, bomb factory or storage location?

(6) (U) Where do the adversary personnel get their vehicles, fuel for the vehicles and get repairs made to their vehicles?

(7) (U) Where can the adversary personnel buy computers and other forms of electronic media? What are the going costs for these items in the operating area?

(8) (U) Where can the adversary personnel buy cell phones and cell phone charge cards in the operating area? What are the costs to buy a cell phone and what are the costs of the charge cards?

(9) (U) How much money does it take to build the typical IED used in the operational area? What are the costs for the most important components in the IED? Where are the adversary personnel buying the components? How are the adversary

Appendix A

personnel buying and paying for the IED components? What are the costs of buying a finished IED versus construction?

APPENDIX B

FINANCIAL INSTITUTIONS AND TRANSFER SYSTEMS (U)

1. (U) Regulated/Formal Financial Institutions

a. (U) Banks

(1) (U) A bank is a financial intermediary that accepts deposits and channels those deposits into lending activities, either directly or through capital markets. Although it varies from country to country, banking is generally a highly regulated industry. Individuals must present identification to open an account and verify their identity before making transactions. There are a number of different types of banks to include retail (commercial banks), investment banks, Islamic (Saharia) banks, private and corporate banks.

(a) (U) Retail banks include the offshore, community and savings banks, as well as the community development banks, building societies, postal savings banks, ethical banks, and Islamic (Saharia) banks

(b) (U) Banks that are established and operated within a HN are susceptible to internal political pressure and can easily be compromised to perform illegal actions in support of corrupt government officials or to support threat entities that are backed by compromised government officials.

(c) (U) Compromised bank officials have the ability to perform illegal financial transactions and then remove documentation of those transactions.

(d) (U) Compromised bank officials have the ability to establish “ghost” accounts to cover the storage or transfer of funds for criminal, insurgent or terrorists “clients”

(e) (U) Foreign banks that maintain a correspondent business relationship with United States banks can be influenced by US designations and sanctions.

(f) (U) Loan fraud and embezzlement of bank funds continues to be a lucrative source of funding for corrupt government officials and threat personalities.

(2) (U) In the United States, the BSA, “requires businesses to keep records and file reports that are determined to have a high degree of usefulness in criminal, tax, and regulatory matters” Businesses are required to report cash payments of over \$10,000 from a single buyer (either in a single transaction or over the course of two or more related transactions) and the presence of a foreign bank account or other financial account. Title III of the US PATRIOT Act, the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001 amended the BSA to require financial institutions, including commodity pools operators, commodity trading advisors

Appendix B

and futures commission merchants, as well as banks, to establish AML programs. AML programs must consist of:

- (a) (U) “the development of internal policies, procedures, and controls;”
- (b) (U) “the designation of a compliance officer;”
- (c) (U) “an ongoing employee training program;” and
- (d) (U) “an independent audit function to test programs.”

(3) (U) Title III also required financial institutions to submit Suspicious Activity Reports to the Department of Treasury and to verify the identity of customers by having procedures in place for checking customer’s names against lists of known or suspected terrorists or terrorist organizations. Under Title III, financial institutions are also required to enact “enhanced due diligence policies, procedures, and controls” to reasonably ensure that transactions are not the result of money laundering. These due diligence policies must include:

(a) (U) “Reasonable steps” to ascertain the identity of the “nominal and beneficial owners” of the account and whether the person is a senior foreign political figure. If the individual is a senior foreign political figure, the AML program must include “enhanced scrutiny” to determine and report if the funds are the result of political corruption.

(b) (U) “Reasonable steps” to ascertain the funding source of the account and the “purpose and expected use of the account.”

(c) (U) Reviewing the account information to make sure it is “consistent with the information obtained about the client.”

(d) (U) Reporting “known or suspected money laundering or suspicious activity conducted to, from or through the private banking account.

b. (U) **Credit Unions**

(1) (U) A credit union is a cooperative financial institution that is owned and democratically controlled by its members. Members elect a board to run the credit union and all members, regardless of account size, can run for a board position. Although credit unions are typically smaller than banks, they vary greatly in size and scope worldwide. Credit unions are nonprofit organizations and any excess earnings are used to offer members “more affordable loans, a higher return on savings, lower fees or new products and services.”⁸ Credit unions offer a full range of financial services, including money transfers, and allow members flexibility and control over their financial institutions, making them popular throughout the world.

(2) (U) In Afghanistan and much of the Muslim world, credit unions are called Islamic investment and finance cooperatives (IIFCs) in order to comply with Islamic lending practices. Many IIFCs provide Sharia-compliant financial services, enabling them to lend to Muslim women.

c. (U) **Financial Markets**

(1) (U) Financial markets are a means of providing critical short- and long-term liquidity to the global financial system and facilitate the consummation of international commerce. Financial markets consist of **spot and forward foreign exchange markets**, where foreign currencies are purchased and sold, or traded, at a specified price and with a promise for immediate delivery, or for delivery sometime in the future (usually not to exceed 90 days); **money markets**, where short-term debt, or money-market, instruments, such as Treasury bills, commercial paper, bankers' acceptances, certificates of deposit, federal funds, and short-lived mortgage- and asset-backed securities commercial paper, are purchased and sold, or traded; **capital markets**, where long-term financial instruments, such as long-term debt and equity securities are purchased and sold, or traded; and **futures markets**, where standardized futures contracts to purchase (sell) commodities, such as precious metals, oil, agricultural products, or financial instruments are traded at a specified price and with a promised delivery date set for some time in the future. While trading futures contracts, such as for oil, gold, or foreign currencies is, inherently speculative; speculation, to profit from fluctuations in prices, irrespective of their underlying value, occurs in all financial markets. Short selling is one kind of speculative activity.

(2) (U) Money markets are channels for obtaining (providing) short-term finance (short-term borrowing and lending) with original maturities of one year or shorter time frames.

(3) (U) Insurgent and terrorist groups have invested money into various financial markets to provide long term financial support to their organizations. In one instance an Iraqi Former Regime member was operating his own stock brokerage.

(4) (U) Insurgent and terrorist groups have made investments in financial markets prior to conducting attacks to influence the trading of the stock of the victim of the attack.

(5) (U) Capital markets are channels for obtaining (providing) long-term finance (long-term borrowing and lending) with original maturities in excess of one year. Capital markets may be classified as primary markets, where business enterprises (companies) and governments can raise long-term finance, and secondary markets, where long-term debt and equity securities are traded. In primary markets, new stock or bond issues are sold to investors via a mechanism known as underwriting. In the secondary markets, existing securities are sold and bought among investors or traders, usually on a securities exchange, over-the-counter, or elsewhere. The price at which these transactions occur reflects the market value.

(6) (U) The foreign exchange market is a global, worldwide decentralized over-the-counter financial market for trading currencies. The core of the money market consists of interbank lending--banks borrowing and lending to each other using commercial paper, repurchase agreements and similar instruments. Stock and futures exchanges are centralized entities, where long-term securities and futures contracts are traded. Stock exchanges are located throughout the world (e.g., New York Stock, London, Tokyo, Hong Kong, Shanghai); changes in stock market indices are regarded as barometers and leading indicators of overall economic activity.

d. (U) Insurance Companies

(1) (U) Insurance is a form of risk management used to hedge against the risk of an uncertain event. Insurance is defined as the equitable transfer of the risk of a loss, from one entity to another, in exchange for payment. The insurer is the company selling the insurance. The policyholder, or the insured, is the person or entity who buys the insurance policy. There are over 7000 insurance companies in the US and the insurance industry collects more than \$1 trillion in premiums each year.

(2) (U) Insurance fraud occurs “when someone knowingly lies to obtain some benefit or advantage to which they are not otherwise entitled or someone knowingly denies some benefit that is due and to which someone is entitled.” The total cost of insurance fraud, not including health insurance, is estimated at over \$40 billion per year. Insurance fraud is used by terrorist financiers and other adversary networks to raise funds. For example, one terrorist finance network attempted to engage in insurance fraud by burning down a cigarette shop that it owned and then attempting to recover cash in their fire insurance policy.⁹ Common insurance fraud schemes include:

(a) (U) False or exaggerated claims.

(b) (U) Premium diversion – an insurance agent embezzles insurance premiums by keeping clients’ premiums instead of sending them to the insurance company.

(c) (U) Disaster fraud schemes - False or exaggerated claims by policyholders, claims filed by individuals residing hundreds of miles outside the disaster-zone, bid-rigging by contractors who falsely inflate the cost of repairs, charity fraud scams designed to misappropriate funds donated for disaster relief.

(d) (U) Workers’ compensation fraud.

2. (U) Unregulated/Informal Financial Institutions (Hawala)

a. (U) Hawala means trust; also known as hundi, it is an informal value transfer, or remittance, system consisting of money brokers, or hawaladars, that are primarily located in the Middle East, North Africa, the Horn of Africa, and South Asia. An

estimated \$2 trillion dollars, or approximately two percent of all international financial transactions, are transferred using a traditional hawala system.¹⁰

b. (U) Unlike other remittance systems, hawala relies on personal and professional relationships to “[transfer] money without actually moving it.”¹¹ For example, a sender in the US who wishes to send money to a recipient in Pakistan could do so through a hawaladar in exchange for a fee. The sender gives the hawaladar the money he wishes to send, plus the additional service fee. The US hawaladar who adds these monies to his financial reserves, contacts his counterpart in Pakistan and instructs him to provide the money to the recipient. The Pakistani hawaladar transfers the requested funds from his own financial reserves and reconciles the balance with his US counterpart the next time there is a Pakistani customer who wants to send money to the US. Although the sender’s money never actually leaves the US, value has still been transferred to the recipient in Pakistan.

c. (U) Hawala is popular for several reasons. It provides an extremely reliable method of financial transfers to regions that have unreliable banking sectors or are too rural to easily access a bank. Hawala does not use bureaucracy or paperwork, making it both efficient and anonymous. Finally, hawala is cost effective. Hawaladars have little to no overhead and senders can evade taxes and take advantage of competitive exchange rates.

d. (U) Typically hawala transactions take place outside the formal financial sector’s legal and regulatory frameworks, enabling terrorist and adversary organizations to transfer funds virtually undetected and with impunity. Ineffective regulation and inconsistent record keeping methods make catching abuses of hawalas by criminals and insurgents difficult. Hawaladars keep very good records on their debits and credits to other hawalas but keep few written records about each transaction and often conduct transactions in multiple currencies or with other items of value, making money laundering easy and concealable.

e. (U) However, in some countries, hawala is actually regulated by local governments, and hawaladars are licensed to perform their money brokering services. Since 9/11, there has been a growing trend towards increased regulation and oversight of hawaladars and hawala activity in a number of countries in the world. In particular, the FATF recommendations, regarding AML/CFT have been at the heart of this push.

3. (U) Money Service Businesses

a. (U) Money Services Business (MSB) includes any person doing business, whether or not on a regular basis, or as an organized business concern, in one or more of the following capacities: Currency dealer or exchanger; Check casher; Issuer of traveler’s checks, money orders or stored value; Seller or redeemer of traveler’s checks, money orders or stored value; Money transmitter; or US Postal Service. The term "money services business" does not include: banks, as that term is defined in 31 CFR 103.11(c); or persons registered with, and regulated or examined by, the Securities and Exchange

Appendix B

Commission or the Commodity Futures Trading Commission. For the complete regulatory definition of "money services business," see 31 C.F.R. 103.11(c).

(1) (U) MSBs may or not be regulated. In the United States, international money transfers involving the United States are subject to monitoring by the Department of Treasury's FinCEN and OFAC, which "enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of WMD, and other threats to the national security, foreign policy or economy of the United States."

(2) (U) In other parts of the world, many countries do not regulate, or provide inadequate oversight of, MSBs. For example, some countries do not vet applicants for MSB licenses, enabling criminal organizations to place front men in positions of MSB ownership and opening the door for operations where there are major, and intentional, compliance deficiencies, omissions and evasion, to launder dirty money freely through the MSB. It is believed that a number of Mexican MSBs are owned and controlled in this way.

(3) (U) MSBs operators, located in countries of the developing world, where there is massive and uncontrolled corruption, can generally be bribed to facilitate the international transmission of dirty money. Should the money launderer cleverly choose a company that is either a branch of, or closely linked to, a network with European and/or North American affiliates, then he or she can gain access to their financial systems.

(4) (U) AML/CFT Compliance for MSBs in many jurisdictions is either poor or substandard; external audits by government regulators are rarely conducted; MSB money laundering does not result in indictments, and in general, the operators have free rein to accept funds without worrying about source of funds inquiries; compliance departments of some MSBs transferring funds do not refer to relevant sanctions lists, because it may not be mandatory in their jurisdiction(s) or no significant punishment is meted out for violations.

b. (U) **Money Exchanges.** A money or currency exchange is a business that specializes in the exchange of one currency for another in exchange for a service fee. A money exchange office is usually located at an airport, travel agency, train station, bank, or anywhere else where people are likely to need to exchange currencies. Service fees may vary from location to location and exchange rates fluctuate based on currency markets. Money exchanges often provide hawala like services in addition to exchanging currencies. Money exchanges and hawalas are often found in the financial section of the local bazaars and markets.

c. (U) **Wire Service Remitter/Wire Transfer**

(1) (U) A wire service remitter or a wire transfer is a method of electronic funds transfer between two individuals or parties. A wire transfer can be made from one bank account to another bank account or through a transfer of cash at a cash office.

(2) (U) A bank-to-bank wire transfer is an exceptionally reliable method of international money transfer. Both the recipient and the sender must prove their identity. A fee for the service is normally collected from the sender as well as from the recipient. The price of a wire transfer via a bank varies greatly, depending on the bank and its location.

Intentionally Blank

APPENDIX C

ANALYTICAL TECHNIQUES (U)

1. (U//FOUO) Developing a Functional Organization Chart for Adversary Networks

a. (U) Functional analysis is an advanced and unique form of analysis that incorporates law enforcement, industrial work mapping processes and military intelligence techniques. Functions are tasks or activities performed by the members of the network and provide a service or capability to the group. People who perform these tasks can be grouped, aligned, or placed together to maximize their collective efforts. The focus of this appendix is to provide JFCs with an understanding of how analysts can develop and provide a reasonable assessment of the functional structures of a adversary group, the locations the organization operates from, where certain tasks are performed and the positions and jobs that are performed by the members of the adversary. Functional analysis can be performed with existing tools and limited training.

b. (U) Successful adversary organizations will, over time, establish recognized functional organizations. Chains of command, operating, accounting and security procedures, lines of communication, financings and material support mechanisms will be formally or informally established to support each functional group. Personnel will be selected and assigned to these groups based on their educations, skills, training, and contacts. Variations will occur within the functional groups as leadership changes, but their basic mission and capabilities will probably remain reasonably consistent. Duplication of effort is sometimes necessary to ensure the survival of the group to prevent single points of failure within the group.

c. (U//FOUO) Drastic or dramatic changes in the operation of the functional group will be noticeable to the adversary organization and may be noticeable to the local community, security forces and everyone collecting information on the group. Drastic changes for no apparent reason can reduce efficiency, expose operations to scrutiny, increase costs, and create discontent within the group. CTF analysts should note changes in the behavior of functional groups and make an attempt to understand why those changes occurred.

d. (U//FOUO) Functional organization charts and map overlays are excellent targeting support tools that give analysts the ability to accomplish some of the following tasks:

(1) (U) Tracking the flow of money and materials from the point of origin to the end user.

(2) (U) Track the flow of communications between members of the group

(3) (U) Identify key nodes within the functional organization. Nodes represent the tangible elements within a system that can be targeted for action, such as people,

Appendix C

places, or things (e.g., materiel or facilities). Key nodes are critical for the overall operation of the adversary network. The operating location may change frequently, but the tasks and the people remain basically the same.

(4) (U) Differentiate between the actual power brokers and the people advertised as key leaders.

(5) (U) Identify the key locations that the functional element is drawing support from. This includes plotting routes using personal association to geographic locations.

(6) (U//FOUO) Confirm source reporting on how adversary organizations are setup and operate.

e. (U//FOUO) A combination of link/flow charts and map graphics are excellent tools for the development and maintenance of a functional organization chart. Data for the link charts should be taken from the combined database used to collect information on the adversary groups to avoid missing the identification of links to other groups or persons. These charts should be set up in a manner that allows them to be updated on a frequent basis. Link type charts set up to map work flows and relationships between the members of the group are an excellent way to map out an organization for analysts and develop an understanding of how the functional groups work together.

f. (U) Link charts can depict pathways but they are not suitable for tracking recurring activities within the functional group, such as monthly movements of money through the group. These types of actions will have to be recorded using other methods, such as spreadsheets that can be used to record activities and perform calculations.

g. (U) It is highly recommended analysts transfer the information from their link charts to map graphics to show the functional groups' lay down in the operational environment. Information displayed on map graphics should be time-oriented. Time analysis provides a simple and effective way to track the movements of multiple personnel. This time analysis can provide directions of movement and help to establish operating areas for individuals and the functional group. Displaying all of the information available on a group at one time can sometimes skew the analysts' perception of what is happening in an area. Reviews of functional movements over time through an area can provide insight into how the group is operating and adapting to the current situation on the ground.

h. (U//FOUO) The functional areas may be combined and arrayed across the operational environment in any number of ways. The following are examples of functional elements within a network:

(1) (U//FOUO) Command and control.

(2) (U//FOUO) Administration.

(3) (U//FOUO) Personnel (recruitment/placement).

(4) (U//FOUO) Plans and operations.

(5) (U//FOUO) Training.

(6) (U//FOUO) Direct action, cells that conduct operations.

(7) (U//FOUO) External operations; infiltration, exploitation of other groups within the political boundaries of the country hostilities are occurring in.

(8) (U//FOUO) International operations.

(9) (U//FOUO) Intelligence.

(10)(U//FOUO) Internal security.

(11)(U//FOUO) Finance.

i. (U//FOUO) Analysts should try to determine who are the adversary functional leaders and key personnel.

j. (U//FOUO) CTF analysts should pay attention to the size and geographic dispersion of the group they are studying and targeting. Functional leaders in smaller groups will typically have to handle more functional responsibility than they would in larger groups. It is easy to support a few people who are located nearby but tasks become more risky, complicated and require additional personnel, as more people need to be supported by the function. For example, one paymaster may suffice for a small cell but not for a group with 1,000 members spread over 5,000 square kilometers. The “troop-to-task ratio” would quickly become overwhelming.

k. (U) Key personnel are the individuals who are responsible for overseeing and conducting the daily business associated with a functional area. The group’s actions are based on their directions. These individuals will have an intimate knowledge of how the function is performed, how it interfaces with other functional areas and the importance of the function to the group as a whole. Key personnel are often lower level operators who may be more important than individuals listed as high value targets.

l. (U) Analysts should avoid focusing exclusively on high value individuals versus the job, role, or function the individual has in the organization (i.e., not thinking “If we can capture/kill Figure X...” versus, “If we can stop their ability to buy weapons.”). The removal of high value individuals typically will have minimal impact on the overall function of the organization if that person has a competent supporting staff. Individuals come and go but the work remains as long as the entity continues. However, the significance of loss of leadership to the organization should not be underestimated, as the loss of leadership may cause the organization to lose purpose, and therefore momentum.

Appendix C

m. (U//FOUO) Each of the functional areas listed above will have positions or job titles (some formal, some not) that let everyone in the organization know who is responsible for those functions in any given area of operation. CTF analysts will have to develop an understanding of the roles and responsibilities of persons who hold certain job titles in an organization. This information is very important when building the functional organization chart.

n. (U//FOUO) People who perform similar, complementary, or dependent functions tend to form relationships or networks within the organization. These relationships become recognized and more formal over time. The relationships can be based on the chain of command, geographic area, mutual support, family ties or trusted suppliers, among other things. This information is very important in determining key nodes within the organization.

o. (U//FOUO) Functional subject matter experts tend to develop relationships or networks outside the organization. Adversary functional experts often have to reach outside the group to perform their tasks. External contacts often will not have the same level of OPSEC or dedication to effort that the members of the adversary group will have and can provide an opportunity for intelligence gathering.

p. (U//FOUO) The span of control for adversary commanders and managers is an excellent method of verifying the accuracy of reporting and the actual number of people associated with each leader in the adversary organization. Link charts can quickly identify flaws in reporting when the span of control is too large for one individual. Sources, because of cultural tendencies or in an effort to make themselves seem more important or knowledgeable, often will say they or their colleagues work for key or senior leaders, when in fact there may be several individuals in between them. Where a link shows individuals have a span of control which far exceeds their abilities/capabilities, the reporting and sources the link chart is derived from needs to be re-examined.

q. (U//FOUO) Geographic dispersion of a group typically will increase the need for additional personnel, an increase in the layers of leadership, command or management. Functional elements are usually geographically placed for a reason, which includes, but are not limited to:

(1) (U//FOUO) Access to transportation or routes into the adversary's operational area.

(2) (U//FOUO) Access to markets, money, material, or equipment.

(3) (U//FOUO) Providing financial and logistics support to specific operating cells.

(4) (U//FOUO) Providing direct access to the organizations leadership.

(5) (U//FOUO) Proximity to family.

(6) (U//FOUO) Proximity to tribal or religious areas that can provide resources and protection to the functional group.

(7) (U//FOUO) Functional groups tend to communicate more with other functional groups involved in the same activity.

2. (U) Basic Social Network Analysis

Once an analyst develops a network which they believe accurately and adequately represents the actual threat finance network, social network analytics can be applied. Based on social network analysis, analysts can calculate features for different nodes of the network, (e.g., closeness, betweenness). The use of the values can help illuminate social criticality within the network. As with any technique, the analyst needs to be trained how to employ the technique and what the values mean so they may be appropriately applied and used. An additional consideration with social network analysis in this context is selection. Because the analysts chose which elements are in the network and how they are connected, they should be diligent when reviewing the results of social network analysis to determine whether the results are a reflection of their selection bias (the social network analysis echoes what they believe to be correct about the network because they created the network) or a reflection of the network operating in the real world. Social network analysis should not be used to conduct a functional analysis of a network. Adversary groups will often operate in a manner that uses “cutouts” or stand-ins to perform tasks that may expose group members to collection. These personnel often have a minimal role in the organization and may be considered expendable. Functional groups and social groups often have separate and distinct members which may or may not connect.

3. (U//FOUO) Tracking Value Transactions

a. (U//FOUO) Value transactions refer to the exchange of anything of value (e.g., money, drugs) for something else of value (e.g., weapons, food). Value transactions include any form of trade or barter of items that can be converted into material, services, or other forms of support to an adversary. Transactions may be conducted face to face or completed electronically over several thousand miles.

b. (U) Value transactions will be conducted continually as long as the adversary has a need for money or items of value. Tracking value transactions is one of the most important components in “following the money.” Value transactions can follow a physical path or a virtual path. The primary goal is to stop the transaction at some point before the transaction can be completed. Secondary goals are to interdict the persons involved in the transaction, seize the items or money involved in the transaction or to identify (sometimes surreptitiously so as to sow internal distrust and tensions), stem the

Appendix C

flow from the sources of the item's of value, and monitor the transactions to determine who else may be involved.

c. (U//FOUO) Value transactions can provide critical information on:

- (1) (U) How networks are organized to obtain financial support.
- (2) (U) The persons and organizations directly or indirectly involved in supporting the network.
- (3) (U) The organizations that are used as enablers by the financial networks.
- (4) (U) Methods used to move items of value.
- (5) (U) Account numbers.
- (6) (U) Identification of primary sources of support.
- (7) (U) Identification of facilitators.
- (8) (U) Financial trends and patterns.
- (9) (U) What is being purchased (e.g., imports of used vehicles and other materials used in the manufacture of IEDs).

d. (U//FOUO) Tracking value transactions is a time consuming effort requiring dedicated, trained and experienced personnel with supporting automated tools. CTF analysts at lower echelon organizations should be aware of how financial transactions are tracked but may have limited time and resources to conduct this task. The information required to perform transaction tracking may not be accessible to military collectors and analysts and will require the assistance of HN, multinational, or interagency partners' personnel. Transaction tracking can be combined with functional network analysis to verify data and to strengthen the financial relationships identified as the result of functional analysis.

e. (U) The following information is important when analysts are tracking value transactions to establish trends, patterns and perform predictive analysis. Analysts will typically only discover a few of these pieces of information.

- (1) (U) Identities of the adversary group and the sender and receiver associated with the transaction. Expect the people involved in the transaction to use an alias or a third party to perform the transaction
- (2) (U) Communications between the sender and the beneficiary. Phone numbers, e-mail addresses, fax machine numbers.

(3) (U) Methods used to transfer the items of value between the sender and the receiver.

(4) (U) Times and dates that transactions occur.

(a) (U) Information on the dates that transactions occur will determine if the analyst can be in position to interdict the transaction or to follow the money and items if the transaction has already been completed.

(b) (U) Noting the dates of transactions between the sender and receiver will help establish the frequency of transfers between the sender and the receiver. Is this the first, second or third transaction between the sender and the recipient?

(c) (U) Some transactions are nearly instantaneous and some will take several days. The determining factor is usually the transfer medium selected.

(d) (U) Some transactions, such as internet or telephone transfers between individuals may not be time relevant. A transaction may sit dormant waiting for the recipient to complete the transaction.

(5) (U) The anticipated path the transaction will follow is based on the following:

(a) (U) Where did the transaction originate from?

(b) (U) Which route will the transaction take?

(c) (U) Where will the transaction terminate?

(d) (U) Account numbers for the sender and the beneficiary. Account numbers provide information similar to the numbers on a highway.

(e) (U) Establishing the starting and end point of the transaction will provide the direction of travel for the items of value between the sender and the receiver.

(f) (U) The sender of the transaction may or may not be able to direct the path of the transaction. This may be up to the person or entity conducting the transaction.

(6) (U) National currency used in the transaction.

(7) (U) Quantity of money involved in the transaction.

(8) (U) Description of the items, the quantity of the items and an estimated value of the items in the transaction.

Appendix C

f. (U//FOUO) CTF analysts may be required to determine the importance of time in the transaction. Time may or may not be a critical factor in the transaction:

(1) (U//FOUO) If the transaction is being performed to support a specific adversary event, timing may be critical.

(2) (U//FOUO) If the transaction is a regular financial transfer to the group, the urgency of the transfer may not be critical.

(3) (U//FOUO) If the transaction is face to face, timing is very important for the persons performing the transfer and for the CTF analysts trying to track the transfer.

(4) (U//FOUO) If the transaction has already been completed, the CTF analysts may use the information to identify the next transaction between the sender and recipient.

g. (U//FOUO) Many adversaries carefully track and manage their funds and assets and will document these transactions in written or computer ledgers or through some type of accounting system. Seizure of these ledgers should be a priority.

h. (U//FOUO) The seizure of financial ledgers is only the beginning of what can become a labor intensive effort. Financial experts should review all ledgers that are seized. Ledger data must be combined with intelligence information to be of value.

i. (U//FOUO) The Treasury Department uses specific terms for the parties involved in transactions that involve funds transfers through financial institutions. The following information is from FinCEN:

(1) (U//FOUO) Originator: The individual or organization that initiates the fund transfer, or the sender.

(2) (U//FOUO) Beneficiary: The ultimate party to be credited or paid as a result of the funds transfer, or the receiver.

(3) (U//FOUO) Originator's Financial Institution: The financial institution receiving the transfer instructions from the originator and transmitting the instructions to the next party in the funds transfer

(4) (U//FOUO) Beneficiary's Financial Institution - the financial institution that is to credit or pay the beneficiary party

(5) (U//FOUO) Additional Financial Institutions to those listed above that may be required to effect the transaction.

j. (U//FOUO) Tracking value transactions requires as much detail as the source of the information can provide. When approaching a foreign government or other USG

agencies for support in tracking value transactions, submitting general information is generally not sufficient and any such request will only result in wasted time and delays.

k. (U//FOUO) Value transactions should be tracked one segment at a time. This means that each transaction or transfer between at least two people is reviewed. There will be many instances where the complete transaction may consist of a chain of several transfers crossing international boundaries over several time periods (e.g., hours, days, weeks). This is common for compartmented cells; donors seek to separate themselves from the recipient and complex criminal schemes to launder funds

l. (U//FOUO) It is not unusual for targeted persons to travel internationally to conduct their banking. For instance, it is not unusual for Iraqis to do their banking in Jordan and a number of Afghans do their banking in the United Arab Emirates, Qatar, and Pakistan. This is often due to safety and stability concerns about Afghan and Iraqi banks but may also be performed to take advantage of strict privacy laws or financial institutions sympathetic to the adversary group.

m. (U//FOUO) It is a common practice for targeted persons to use the bank accounts of friends and family to conduct financial transactions. Therefore, it is also important to identify the banks, bank branch names or identifiers, bank employees, bank account numbers, account types and transactions associated with the accounts of as many family members as possible. Adversary personnel often use accounts established using the HN currency to avoid exposure to US sanctions and designations.

n. (U//FOUO) Value transaction information is available from commercial sources, interagency partners, multinational organizations or HN government agencies. Transaction information from commercial financial institutions can be accessed in a number of ways:

(1) (U//FOUO) Any investigative agency within the USG can ask FinCEN to complete an Egmont request as the Egmont FIU.

(2) (U//FOUO) Requests can be made through the Federal Reserve Banks for financial information available through Fedwire [Federal Reserve Wire Network], CHIPS [Clearing House Interbank Payments System], or SWIFT [Society for Worldwide Interbank Financial Telecommunications], which is operational in 109 countries.

(3) (U//FOUO) Intelligence organizations that are capable of clandestine information collection.

(4) (U//FOUO) Information voluntarily provided by persons associated with the financial institution of interest.

o. (U//FOUO) Types of value transactions include but are not limited to:

(1) (U//FOUO) Teller/automated teller machine deposits.

Appendix C

- (2) (U//FOUO) Teller/ automated teller machine withdrawals.
- (3) (U//FOUO) Debit card transactions (deposits, withdrawals, purchases).
- (5) (U//FOUO) Sale of items by targeted persons or organizations.
- (6) (U//FOUO) Cash value card purchase or use.

p. (U//FOUO) Methods of conducting value transactions include, but are not limited to:

- (1) (U//FOUO) Wire transfers.
- (2) (U) Mobile banking.
- (3) (U//FOUO) Loans.
- (4) (U//FOUO) Courier (delivery of funds by a third party).
- (5) (U//FOUO) Direct transfers (person to person delivery of funds).
- (6) (U//FOUO) Hand offs (movement of funds between intermediaries).
- (7) (U//FOUO) Letters of Credit"

q. (U//FOUO) Transaction histories of numbered accounts in financial institutions may provide the following types of information:

- (1) (U//FOUO) Cumulative amount of funds being deposited into, or withdrawn from, an account over time.
- (2) (U//FOUO) Average amount of recurring deposits, or withdrawals, in general.
- (3) (U//FOUO) Average amount of deposits, or withdrawals, by depositor.
- (4) (U//FOUO) Frequency of deposits, or withdrawals.
- (5) (U//FOUO) Regularity or consistency of deposits, or withdrawals.

r. (U//FOUO) The following information is required to reconstruct transactions between numbered accounts in financial institutions or money service businesses. The more information gathered about a transaction, the greater the chances of identifying value transactions between a sender and a recipient of interest:

- (1) (U//FOUO) Sender Name.

- (2) (U//FOUO) Sender location (City, Province / State, Country).
- (3) (U//FOUO) Sending financial institution.
- (4) (U//FOUO) Sending account number.
- (5) (U//FOUO) Recipient Name.
- (6) (U//FOUO) Recipient location (City, Province/State, Country).
- (7) (U//FOUO) Receiving financial institution.
- (8) (U//FOUO) Receiving account number.
- (9) (U//FOUO) Date of transaction.
- (10)(U//FOUO) Type transaction.
- (11)(U//FOUO) Transaction medium.
- (12)(U//FOUO) Amount of transaction.

(13)(U//FOUO) Transaction number (generated by the sending financial organization).

s. (U//FOUO) The following information is required to reconstruct transactions between sender and recipient when numbered accounts are not used. In this situation, the sender is the person holding the items of value and the recipient is the person who will obtain the items of value. The more information that is gathered about a transaction, the greater the chances of understanding how items of value are moved:

- (1) (U//FOUO) Sender Name.
- (2) (U//FOUO) Sender location (City, Province/State, Country).
- (3) (U//FOUO) Sending money service business.
- (4) (U//FOUO) Recipient Name.
- (5) (U//FOUO) Recipient location (City, Province/State, Country).
- (6) (U//FOUO) Receiving money service business.
- (7) (U//FOUO) Date of transaction.

Appendix C

(8) (U//FOUO) Type transaction.

(9) (U//FOUO) Transaction medium.

(10)(U//FOUO) Item(s) of value transferred.

(11)(U//FOUO) Amount of transaction.

(12)(U//FOUO) Transaction number (generated by the sending financial organization).

t. (U//FOUO) Transactions may be structured in multiple steps involving both witting and unwitting persons and organizations.

u. (U//FOUO) When tracking multi step transactions it is important to remember some of the following things:

(1) (U//FOUO) Identify the sender, by name.

(2) (U//FOUO) Identify the recipient, by name.

(3) (U//FOUO) Identify all persons who are directly involved in the transaction, their names and locations.

(4) (U//FOUO) Identify the responsibilities of each person involved with each step in the transaction.

(5) (U//FOUO) Identify each location that handles the money or material associated with the transaction. Be specific: get an address, a grid coordinated, anything that will identify as closely as possible the origination point of the transaction.

v. (U//FOUO) Other multi-segment value transactions can include:

(1) (U//FOUO) Bulk cash courier. Money is physically carried by a courier between the donor and the recipient. There may be a series of couriers involved or it could be just one courier. This type of transfer has significant limitations, including the weight and bulk of the currency.

(2) (U//FOUO) Account to account transfer (one time). Direct connection between the sender and receiver of the funds using established financial institutions.

(3) (U//FOUO) Deposit from a money service business to an account in a financial institution. (Hawala/Western Union/Moneygram to bank).

(4) (U//FOUO) Account to account transfer, multiple transfers.

(5) (U//FOUO) Wiring funds through a money service business to an account in a financial institution (bank).

4. (U//FOUO) Public and Adversary Entity Records Infrastructure

a. (U//FOUO) The public records infrastructure refers to the collection of government and private records maintained to track births, deaths, marriage, divorce, personal identification (national identification cards, passports), education, training, law enforcement and judicial matters, health matters, welfare, rationing, financial activities, certifications and licensing, property ownership, financial transactions, tax collections and hundreds of other records used in documenting activities related to people and entities. Public records are an excellent source of positive identification information in countries that maintain that type of information.

b. (U//FOUO) CTF analysts need be able to take information found in record keeping systems and match that information to adversary personnel the military unit is interested in pursuing.

c. (U) US law enforcement officers and investigators receive training on and are dependent upon finding, accessing and obtaining information from, and analyze information held in public records.

d. (U) One challenge in developing countries, where DOD often operates, is few government organizations maintain easily accessible, current, accurate, extensive or historical records on the activities of the people that live in that country. Some of the government departments will keep secret records.

e. (U//FOUO) In industrialized and modern societies, record keeping by government, public, and private agencies is essential to maintain order and stability. Military personnel may not have direct access to these systems, but working in partnership with law enforcement entities, as well as regulatory and political institutions, this information may be obtained.

f. (U) It is important for CTF analysts to understand the importance of identifying any public records keeping system that is available in their operational area. Analyst should identify the system and determine who is responsible for maintaining the records. Analysts should make a determination of the possible intelligence value of the information and act accordingly to obtain that information when possible.

g. (U//FOUO) Access to government and private records varies greatly between different countries. Obtaining the needed information may take time and considerable effort. Some countries will require documents like a subpoena or search warrant, while others will only require coordination with the right government department. CTF analysts should work with HN personnel to identify as many public records keeping systems as possible, how those systems are used, and the type of information that is

Appendix C

contained in the records, where the records are maintained, and how to obtain information contained in the records.

5. (U) Notional Criminal/Terrorist Enterprise Business Model

a. (U) Figure C-1 illustrates the economic and financial activities of a notional criminal/terrorist enterprise, as it foments violence in order to achieve its objective; whether it is for financial gain and/or ideology. It shows that the enterprise is active in interconnected, white, grey, and black markets for goods and services, fixed and variable factors of production, and financial capital assets. The diagram also displays select targets to disrupt the enterprise and its operations.

b. (U) The graphic suggests that criminal/terrorist business enterprises successfully raise and receive funds, maintaining a reliable, steady flow of revenues from multiple sources, including quasi-legitimate business operations, grey market sales, criminal money-making activities, laundered investments, and financial backers. They incur current, capital, and other operating expenses to maintain and grow profitable, self-sustaining threat organizations virally over time and space, disbursing funds and arranging payments for bribes, purchasing physical capital assets and equipment, employing human capital, procuring raw materials, intermediate goods, and other inputs, and engaging in a myriad of other planned and unplanned commercial transactions.

c. (U) It is possible the notional criminal/terrorist business enterprise may experience a negative net cash flow, if operating expenses exceed revenues. This unprofitable state of affairs can, and may, continue, as long they can liquidate existing financial reserves to cover expected and unexpected expenses. However, over the long haul, this situation is not tenable; if the criminal/terrorist enterprise cannot sustain itself, by generating sufficient revenues to cover expenses, it may go out of business and cease to exist

d. (U) Finally, the diagram illustrates potential opportunities and challenges for disrupting and dismantling threat networks. The bright red starbursts point to potential lethal and nonlethal operations to create effects against the network.

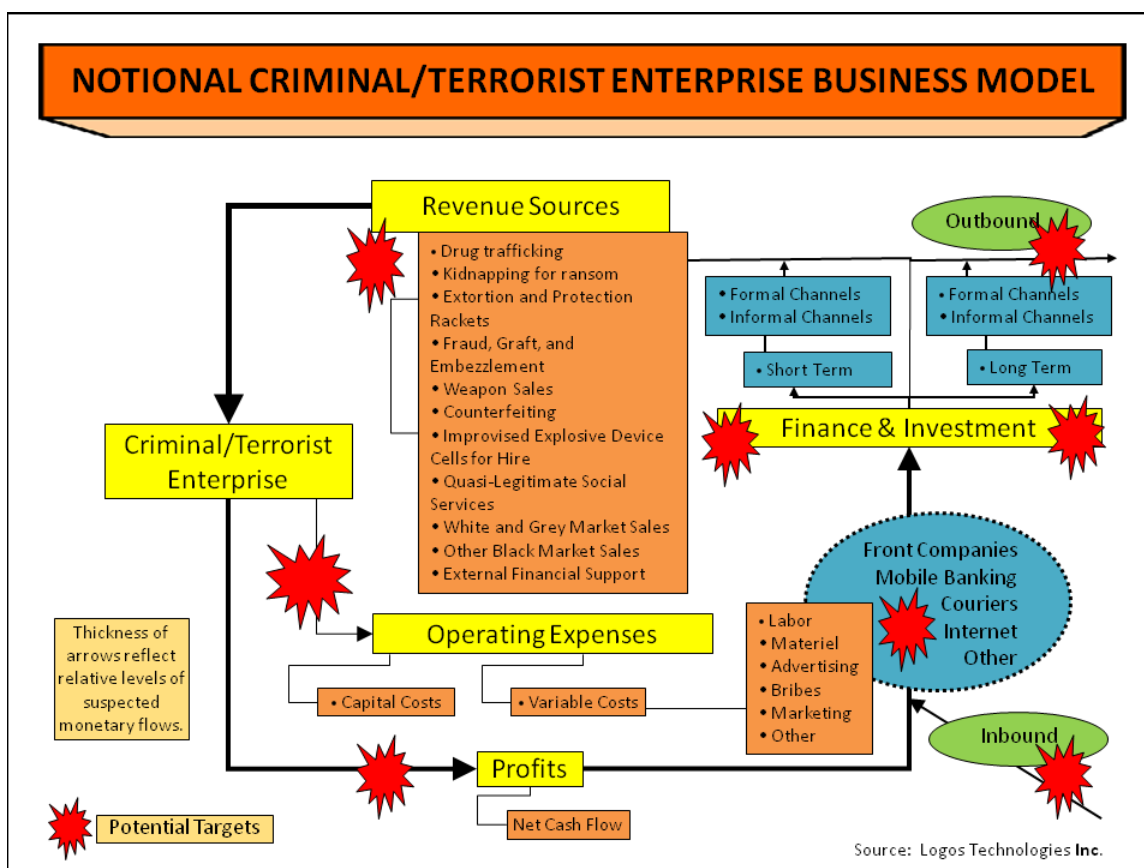


Figure C-1. (U) Notional Criminal/Terrorist Enterprise Business Model

Intentionally Blank

APPENDIX D

ILLUSTRATIVE MEASURES OF EFFECTIVENESS (U)

1. (U) Framework

The framework that follows is an example of a hierarchical metrics system of outcome-based goals, indicators, and measures. Once collected, the measures/criteria can be aggregated to provide indications of trends toward the achievement of goals over time. These metrics, although not all-inclusive, should provide both a baseline operational- and strategic-level assessment tool for JFCs and policymakers who seek to diagnose potential obstacles to CTF, and to track progress from the point of detection, deterrence, disruption and its ultimate elimination. In addition, this metrics system is designed to help identify the contributing factors to threat finance and to gauge the capacity of indigenous institutions in overcoming them. The intention is to enable JFCs and policymakers to establish realistic goals, bring adequate resources and authorities to bear, focus their efforts operationally and strategically, and enhance prospects for attaining an effective CTF capability.

2. (U) Methodology

a. (U) **Outcome:** Detection and degradation of threat finance network: Existing political and financial infrastructure central to adversary support and activities are identified; an effective CTF strategy combined with whole-of-government efforts dismantle the enabling environment for terrorism.

b. (U) **Decompose the outcome**

(1) (U) Breakdown the outcome into usable sections:

- (a) (U) CTF strategy (capability).
- (b) (U) Political and financial infrastructure are identified (capacity).
- (c) (U) Enabling environment (conditions).
- (d) (U) Whole-of-government (authority).
- (e) (U) Terrorist/criminal support (dependent variable).

(2) (U) **What needs to be answered?**

(a) How effective is the whole-of-government effort in CTF and counterterrorist strategy?

Appendix D

(b) (U) How effective is intelligence in identifying political and financial networks providing support to terrorist networks as well as providing the data necessary for building adversary profiles?

(c) (U) How does the enabling environment (set of interrelated conditions), such as fiscal, organizational, legal, informational, political, and cultural conditions, impact state and international actors in countering threat finance in a sustained and effective manner?

(d) (U) Are the drivers of conflict and their connection with threat finance (corruption, impunity, and criminalization of state institutions) being diminished?

(e) (U) Is the institutional capability, capacity, and authority to CTF being strengthened?

3. (U) Measure of Effectiveness: External Destabilization - Diminished

(U) **Indicator:** Does interference by foreign states or transnational actors (e.g., diasporas, political movements, trans-border communications media, illicit commercial enterprises, private security forces, terrorist networks) fuel conflict or undermine CTF efforts? **Measures/criteria and preferred trends:**

a. (U) Flow of funding from foreign states or transnational actors to violent factions. **Decreasing trend.**

b. (U) Flow of weapons from foreign states or transnational actors to violent factions. **Decreasing trend.**

c. (U) Number of foreign fighters detected or observed (by affiliation). **Decreasing trend.**

d. (U) Number (type and impact) of armed incursions by neighboring states. **Decreasing trend.**

e. (U) Number (type and impact) of armed incursions by non-state actors from neighboring states. **Decreasing trend.**

f. (U) Evidence of organizational linkages between diasporas or affinity groups and warring factions. **Decreasing trend.**

4. (U) Measure of Effectiveness: External Drivers of Conflict - Diminished

a. (U) **Indicator:** What is the extent of funding for armed opposition groups from Diaspora populations and affinity groups? **Measures/criteria and preferred trends:**

(1) (U) Flow of funding from foreign states or transnational actors to violent factions. **Decreasing trend.**

b. (U) **Indicator:** What is the extent of funding for armed opposition groups from Diaspora populations and affinity groups? Measures/criteria and preferred trends:

(1) (U) Dollar value of arms transferred to the target country by foreign governments (by recipient). **Decreasing trend.**

(2) (U) Amount of financial or in-kind support provided by foreign governments for armed opposition groups. **Decreasing trend.**

5. (U) Measure of Effectiveness: Threat Finance Generation from licit sources - Diminished

(U) **Indicator:** What is the extent of funding for insurgents from licit sources? Measures/criteria and preferred trends:

a. (U) Extent of state sponsors funding insurgents. **Decreasing trend.**

b. (U) Donations from individuals or businesses. **Decreasing trend.**

c. (U) Amount of financial support or in-kind support from charities and NGOs. **Decreasing trend.**

d. (U) Number of charitable organizations lacking documentation to show charity is actively fundraising with the general public. **Decreasing trend.**

e. (U) Identification of business fronts whose funds deposited are in great excess of receipts generated. **Increasing trend.**

f. (U) Multiple business entities layered to conceal ownership or individual participation. **Decreasing trend.**

6. (U) Measure of Effectiveness: Criminalization of State Institutions - Diminished

(U) **Indicator:** Do parallel or informal governing structures sustained by illicit revenue exist within formal government institutions? Measures/criteria and preferred trends:

a. (U) Political leaders/ruling elites are involved in, or linked to, criminal looting of natural resources, drug trade, human trafficking, money laundering, and smuggling of arms or contraband. **Decreasing trend.**

Appendix D

b. (U) Public perception that organized crime has a substantial influence on the development of national policies, operation of ministries, and allocation of resources. **Decreasing trend.**

c. (U) Known criminals or individuals linked to crime syndicates occupy key government positions. **Decreasing trend.**

d. (U) Extent to which government expenditures are hidden or are unaccounted for. **Decreasing trend.**

e. (U) Militias/paramilitary groups are allied with government officials or Regional/Local Power Brokers, who benefit from illicit revenues and criminal activity. **Decreasing trend.**

7. (U) Measure of Effectiveness: Economic Incentives for Threat Finance - Diminished

(U) **Indicator:** Are there economic incentives to continue threat finance? **Measures/criteria and preferred trends:**

a. (U) Government officials profit from arms trafficking, drug trafficking, money laundering etc. **Decreasing trend.**

b. (U) Faction leaders and government officials profit from the control of trade in commercial goods made illicit by international sanctions. **Decreasing trend.**

c. (U) Amount of relief supplies expropriated by armed opposition groups. **Decreasing trend.**

d. (U) Number of businesspersons and wealthy families paying protection money to be allowed to operate without interference. **Decreasing trend.**

8. (U) Measure of Effectiveness: Political impact of illicit wealth - Diminished

a. (U) **Indicator:** What is the magnitude of economic activity taking place in illicit markets? **Measures/criteria and preferred trends:**

(1) (U) Estimated percentage of GDP accounted for by illicit economic transactions. **Decreasing trend.**

(2) (U) Estimated amount of revenue generated by looting of natural resources. **Decreasing trend.**

(3) (U) Gap between prices for a market basket of essential goods and services in open markets versus prices for the same items and services in gray markets. **Decreasing trend.**

b. (U) **Indicator:** Are public offices corrupt? Measures/criteria and preferred trends:

(1) (U) Ranking on international indices of corruption. **Decreasing trend.**

(2) (U) Existence of incentive structures that reward smuggling, rent-seeking, looting of natural resources or other forms of large-scale criminal activity/corruption. **Decreasing trend.**

(3) (U) Public perception of the degree of corruption and abuse of office by government leaders (by identity group). **Decreasing trend.**

(4) (U) Degree to which local and international companies alter their investment plans due to the prevalence of corruption. **Decreasing trend.**

(5) (U) Percent of citizens reporting that a 'gift' or informal payment is required to obtain a government service. **Decreasing trend.**

(6) (U) Percent of citizens reporting that a 'gift' or informal payment is required to obtain a government job. **Decreasing trend.**

(7) (U) Percent of citizens reporting that a 'gift' or informal payment is required to avoid arrest or a fine by police or to pass through a police checkpoint. **Decreasing trend.**

(8) (U) Percent of businesses reporting that a 'gift' or informal payment is required to obtain a construction permit. **Decreasing trend.**

(9) (U) Percent of businesses reporting that a 'gift' or informal payment is required to obtain an import license. **Decreasing trend.**

(10)(U) Percent of businesses reporting that a 'gift' or informal payment is required to obtain an operating license. **Decreasing trend.**

(11)(U) Public perception of the extent of corruption in public offices. **Decreasing trend.**

c. (U) **Indicator:** Are there links between government officials and criminal syndicates? Measures/criteria and preferred trends

(1) (U) Known criminals or individuals linked to crime syndicates occupy key government positions. **Decreasing trend.**

Appendix D

(2) (U) Number of senior government officials implicated by foreign governments or international law enforcement bodies (e.g. Interpol) in transnational criminal activity. **Decreasing trend.**

d. (U) **Indicator:** Do warring or armed opposition groups generate illicit revenue? Measures/criteria and preferred trends:

(1) (U) Armed opposition groups maintain spheres of influence where they exercise de facto authority to collect taxes or exploit criminalized economic activity, etc. **Decreasing trend.**

(2) (U) Estimated amount of revenue generated by opposition groups by looting natural resources, drug production, collection of taxes, smuggling networks, trafficking in cultural/historical artifacts, etc. **Decreasing trend.**

9. (U) Measure of Effectiveness: Institutional Performance (Host Nation) - Strengthened

a. (U) **Indicator:** How effective are independent oversight systems in ensuring the integrity of state revenues and expenditures and preventing diversion by predatory power structures? Measures/criteria and preferred trends:

(1) (U) A means for regular independent audits of state fiscal operations exists. **Increasing trend.**

(2) (U) Percentage of state-entity budgets/fiscal operations audited. **Increasing trend.**

(3) (U) Percentage of questionable financial practices investigated, prosecuted, and punished. **Increasing trend.**

b. (U) **Indicator:** How effective are controls on money-laundering and suspicious financial-transactions? Measures/criteria and preferred trends:

(1) (U) Strength of legal and administrative systems for monitoring and adjudicating cases of money laundering and suspicious financial transactions. **Increasing trend.**

(2) (U) Number of cases of money-laundering, suspicious financial transactions investigated and number of convictions. **Increasing trend.**

(3) (U) Amount of assets seized as a result of enforcement of suspicious financial transaction laws. **Increasing trend.**

(4) (U) Identification of businesses that transfer or exchange currency in support of the insurgent networks (primarily **hawalas** and money exchanges/changers) **Increasing trend.**

c. (U) **Indicator:** Is privatization of publicly owned businesses conducted transparently and with safeguards to deter their capture by predatory? Measures/criteria and preferred trends:

(1) (U) Presence of a transparency mechanism that includes, for example, public posting of offers of public property, bids and tenders for the purchase of such property, identity of purchasers, financing of sales, and any modifications to legal language regarding the subsequent use of property required (e.g., right of resale, restrictions on the use of assets). **Increasing trend.**

(2) (U) Percent of privatization sales/transfers compliant with a transparency regime. **Increasing trend.**

(3) (U) Public disclosure of transfers that includes book and market value of assets, transferred and identity of individuals and groups acquiring assets, and percentage of privatized firms whose equity is publicly traded and whose operations are officially reported. **Increasing trend.**

10. (U) Measure of Effectiveness: Administration of Justice (Host Nation) - Strengthened

(U) **Indicator:** Does the criminal justice system perform essential functions effectively? Measures/criteria and preferred trends:

(U) Criminal laws and criminal procedures address contemporary criminal activity and provide effective means of law enforcement for terrorist financing, trafficking, transnational and organized crime, extradition, mutual legal assistance, cyber crime and etc. **Increasing trend.**

11. (U) Measure of Effectiveness: Performance of Security Forces (Host Nation) - Strengthened

(U) **Indicator:** Are the intelligence services effective? Measures/criteria and preferred trends:

a. (U) Availability of actionable intelligence and other information regarding the illicit transit of goods and services across the borders. **Increasing trend.**

b. (U) Laws/rules/principles are codified to regulate intelligence services exist. **Increasing trend.**

Appendix D

c. (U) Extent to which threats to internal and external security have been prevented or disrupted because of intelligence-led operations. **Increasing trend.**

d. (U) Extent to which prosecution and conviction for crimes relating to threats to internal or external security have been supported by intelligence services. **Increasing trend.**

12. (U) Measure of Effectiveness: Support for Whole-of-Government - Strengthened

(U) **Indicator:** Is the level of DOD support to interagency partners and partner nations adequate and relevant when it comes to countering threat finance operations? Measures/criteria and preferred trends:

a. (U) DOD supports the necessary civil USG agency personnel, funding, communications, facilities, support personnel, training, transportation, and capacity building (By region). **Increasing trend.**

b. (U) DOD acts as a force multiplier for interagency partners from the Department of Treasury, DOS, DOJ, DHS, and other potential future interagency partners. **Increasing trend.**

c. (U) DOD works with USG interagency partners to ensure that efforts are also aligned with the needs and concerns of partner nations. **Increasing trend.**

d. (U) DOD closely coordinates with interagency partners (DHS, DOS, DOJ, Department of Treasury and etc) and deconflicts potential CTF targets to ensure that highly sensitive ongoing investigations and operations are not compromised. **Increasing trend.**

e. (U) DOD relies on existing statutory authorities to implement CTF-related tasks **Increasing trend.**

13. (U) Measure of Effectiveness: Intelligence and Resource Sharing - Strengthened

(U) **Indicator:** Does CTF Intelligence provide useful intelligence to warfighters and planners? Measures/criteria and preferred trends:

a. (U) Availability of actionable intelligence and other information regarding the illicit and licit activities surrounding threat finance. **Increasing trend.**

b. (U) Adversary organizations detected and identified. **Increasing trend.**

c. (U) Detection and identification of functional organizations, chains of command, and key personnel detected and identified for targeted adversary organizations. **Increasing trend.**

d. (U) Detection and identification of previously undetected financial resources exploited by, or associated, with adversary organizations, to include locations, estimated value, and resource vulnerability. **Increasing trend.**

e. (U) Detection and identification of threat financial networks and their associated operating areas. **Increasing trend.**

f. (U) Effectiveness in collaboration, information sharing and systems interoperability. **Increasing trend.**

g. (U) Contribution to the JIPOE in terms of intelligence assessments, estimates, and other intelligence products in support of the JFC's decision-making. **Increasing trend.**

14. (U) Measure of Effectiveness: Counter Threat Finance Support for Law Enforcement - Strengthened

(U) **Indicator:** Is law enforcement getting support against top-priority transnational threats and is it sufficient to meet the needs? Measures/criteria and preferred trends:

a. (U) Percent of enforcement agencies receiving technical assistance. **Increasing trend.**

b. (U) Percent of law enforcement officials receiving CTF training. **Increasing trend.**

c. (U) Number of TFC advisors embedded in Law Enforcement Agencies. **Increasing trend.**

d. (U) Level of coordination in law enforcement investigations especially when jointly supported by domestic and international legal authorities. **Increasing trend.**

e. (U) Number of counterdrug and counterterrorism activities engaged (by region). **Increasing trend.**

15. (U) Measure of Effectiveness: Organization, Training, and Support of Threat Finance Cells - Strengthened

(U) **Indicator:** Does each CCMD have the capability to establish a dedicated TFC? Measures/criteria and preferred trends:

a. (U) DOD level of financial and analytical support to interagency CTF efforts. **Increasing trend.**

Appendix D

b. (U) Extent of USSOCOM sponsored activities to improve DOD CTF doctrine, organization, training and equipment. **Increasing trend.**

c. (U) Ability of TFC personnel to deploy and augment JFC staffs in the event of a major combat operation. **Increasing trend.**

d. (U) Percent of TFC personnel receiving training from institutions other than DOD (e.g., FBI, DEA, ATF). **Increasing trend.**

APPENDIX E

TRAINING AND EDUCATION (U)

1. (U) Introduction

(U) Because CTF is not a traditional military mission, because the US will not always be the lead agency conducting CTF, and because the skills needed to conduct CTF can degrade over time if not used, training and education of personnel engaged in CTF is a critical element to mission success. Leaders, staff, and advisors who understand adversary finance systems, know how to plan and conduct operations to dismantle those systems, and can assess how CTF operations are impacting the adversary, can maximize CTF activities, prevent lost opportunities, effect adversary financial networks, and potentially save lives. Training and education are necessary to develop the essential skills and knowledge within the DOD to properly conduct CTF operations.

2. (U) Individual Training

a. (U) JFCs and leaders need to ensure their units and subordinates have received adequate training to accomplish the missions and task that will be expected of them. Instructional training may include formal courses but will also include unit-level training needed to accomplish the tasks and produce the results needed for mission success.

b. (U) **Intelligence.** In general, intelligence personnel will need the most in-depth and advanced training as relates to CTF.

(1) (U) **Intelligence analysts** require training on the basics of threat finance; reading reports for financial context; functional network analysis; relationship mapping; geospatial and temporal proximity analysis; basic financial institution operations; transaction tracking; adaptation of SIGINT to threat finance; introduction to document and media exploitation, introduction to interagency organizations, operations and capabilities; support to interrogations that have threat finance associations; target development; engagement options for threat finance. Finally, intelligence analysts require training to adapt well-established intelligence and law enforcement procedures to the development of evidence, which can be used in criminal prosecutions at home and abroad.

(2) (U) **Intelligence collectors** require training on threat functional organizations; operating techniques used by groups in the collectors operational area; relationship development and network mapping; developing an understanding of the local economy, markets, bazaars and sources of materials and supplies; identification of paths and movement tracking; persistent observation to identify trends and patterns; collection of cost data and cost of living data; identification of corrupt government officials; identification and tracking of exploited NGO's and charities; indicators and warnings of threat financial activity; how to ask questions about financial processes using a basic financial operating template; financial interview techniques; how to identify illicit fund raising activities; where and how to find financial institutions. As a part of this training,

Appendix E

collectors should increase their awareness of the specific tactics used by threat finance organizations as well as specific collection requirements relating to CTF.

c. (U) **Operations**

(1) (U) Combat arms personnel who will conduct operations in support of CTF (whether led by the military or other mission partners) require training on sensitive site exploitation TTPs (including intelligence collection and preservation of evidence and chain-of-custody). Additionally, those combat arms personnel who will be conducting CTF operations with USG and international mission partners may benefit from additional training on differing roles and authorities, as well as differing ROE and rules for the escalation of force.

(2) (U) **Military law enforcement** personnel, including uniformed and civilian agents, who will be conducting investigations on and building cases against threat finance organizations require training on TTPs for adapting well-established law enforcement and investigative techniques to CTF missions. They also require training on identifying the structure, function, and behavior of threat finance organizations as well as the specific tactics used by those organizations.

d. (U) **Planners.** In general, planners need intermediate level training as it relates to CTF. CTF training for planners will include best practices for threat financial operating methods, threat functional organizations, threat operations within the operational area, threat finance engagement techniques, coordinating with USG and international mission partners and designing courses of action, which can support CTF led by other mission partners including those, which potentially lead to prosecutions and trials. As part of this training, planners should increase their awareness and appreciation of the ways which CTF can support overall military objectives and conversely the ways which traditional military missions can support CTF objectives.

e. (U) **Finance.** Personnel involved in finance, uniformed and civilian, require training on using DOD financial systems to spot and identify where battlefield finance may be supporting adversary funding. Additionally, training for personnel involved in finance should increase their awareness of the structure, function, and behavior of threat finance organizations as well as the specific tactics used by those organizations.

f. (U) **Military Information Support Operations.** Personnel involved in the planning and conduct of MISO require training on TTPs to adapt established procedures for the conduct of MISO to support CTF. Their training will help to identify key targets inside the threat finance organizations, as well as the population as a whole, with the greatest influence to degrade an adversary's finance system and to develop and deliver messages to that end. Additionally, training for MISO personnel should increase their awareness of the structure, function, and behavior of threat finance organizations as well as the specific tactics used by those organizations as well as the relevant characteristics of the local populations.

g. (U) OJT provides the training audience experience in performing tasks in the actual work environment with all systems, technologies, and capabilities available. OJT can be particularly useful used to reinforce instructional training or to develop new skills and knowledge where instructional training is not available or practicable. OJT is most appropriate for jobs and tasks where sufficient time and oversight is available and risk mitigation can be appropriately employed. For CTF, intelligence analysts, planners, and finance personnel may benefit from OJT.

(1) (U) OJT is the least desirable technique for providing technical CTF training. CTF requires advanced application of basic intelligence and analytical methods. OJT programs should be properly structured and resourced to be effective.

(2) (U) The level and proficiency of the training will be heavily dependent upon the experience of the trainer, the skills the trainer has learned, the aptitude of the trainer, and the time allocated for training. OJT training is often performed in a fast paced, operational environment where the trainee is expected to perform; limiting the trainee's exposure to CTF. OJT may not be effective unless it is used in conjunction with prior technical skills training and supervision by a trained and experienced supervisor.

h. (U) Internships provide an unparalleled opportunity to experience culture, behaviors, and conditions which may not be adequately conveyed by other means. The downside is internships are most effective when they are of sufficient length to experience all the relevant culture and events. This means structuring a CTF capability, which allows for these extended periods outside of the supported command. Internships with interagency and international CTF mission partners build a shared understanding of the procedural and cultural differences between the US military and its mission partners, which are invaluable to planning and coordinating future CTF operations.

3. (U) Unit Training

a. (U) CTF unit training seeks to develop the skills and knowledge of the unit in order to better plan and execute CTF operations.

b. (U) In order to be most effective, CTF should be incorporated into existing unit training. This training can include exercises the unit participates in as well as pre-deployment training such as training center rotation for a deploying Army battalion or the Inter-Deployment Training Cycle for a Navy Carrier Battle Group.

c. (U) In order for such unit training to successfully build the skills and knowledge required to conduct CTF operations, the exercises and pre-deployment training must provide sufficient realism and sensitivity as it relates to CTF. For example, exercises need trainers/white cell who understand CTF and how it impacts the operational environment, an adversary or Red Cell who can accurately represent adversary responses to CTF actions, and realistic CTF data and injects for the training unit.

4. (U) International Training

Under the auspices of nation assistance or FID, the US military may provide CTF training to international mission partners. Additionally, where international mission partners have unique or well-developed capabilities, the US may receive training from those mission partners. International mission partners can be allied or coalition partner nations, they can be international organizations such as the UN or the Egmont Group of Financial Intelligence Units, or they may be international corporations such as banks or telecommunications companies. Training with international mission partners build capabilities. For those being trained, it builds skills and abilities in the training audience. New training can result in new capabilities or at the very least newly enhanced capabilities. For those training, it builds expertise and experience. In the same way as internships, multinational training can build a shared understanding of the procedural and cultural differences between the US military and its mission partners. This shared understanding can be the basis for developing trust and is invaluable in planning and conducting multinational CTF operations in the future. Training with international mission partners increases awareness of their capabilities, limitations, authorities, and information environment (what information they do and do not have access to) and theirs of ours. Increasing their awareness on both sides can lead to more coherent and integrated intelligence, planning, and execution for multinational CTF operations. It can help the US better understand what types of intelligence need to be shared, what missions are appropriate to be shared and which should be retained, and where mission partners can perform missions and tasks which the US is not able or allowed to perform.

5. (U) Courses

a. (U) **Joint Special Operations University (JSOU)** (<https://jsou.socom.mil/Pages/Default.aspx>) educates Special Operations Forces executive, senior, and intermediate leaders and selected other national and international security decision-makers, both military and civilian, through teaching, research, and outreach in the science and art of joint special operations. JSOU conducts a “Counter Threat Finance Educational Seminar” which addresses CTF fundamentals, and how to effectively use intelligence to combat enemy financial networks with strategic and tactical collection, analysis, and targeting processes. The seminar will cover an intermediate level of how to identify and map threat networks in order to disrupt and dismantle logistic and financial facilitation.

b. (U) **Northeast Counterdrug Training Center (NCTC)**. The mission of the NCTC (<http://www.counterdrug.org/NCTC/nctc.html>) is to provide drug law enforcement and demand reduction agencies within the geographic boundaries of the Northeastern United States with a no-cost training center. Applicable CTF courses include: Domestic Terrorism, Introduction to Narco-Terrorism, Money Laundering, Terrorism Intelligence Gathering, and Middle Eastern Intelligence.

c. (U) **Federal Law Enforcement Training Center (FLETC)**. The FLETC (<http://www.fletc.gov>) serves as a law enforcement training organization for over 80 USG agencies. The FLETC also provides services to state, local, tribal, and international law enforcement agencies. Applicable CTF courses include: International Banking and Money Laundering Training Program, Financial Forensics Techniques Training Program, Money Laundering and Asset Forfeiture Training Program, Intelligence Analyst Training Program, Black Market Peso Exchange Training Program, and Fundamentals of Terrorism Training Program.

d. (U) **The Threat Finance Course** is one of the electives for the Defense Intelligence Strategic Analysis Program II program. The Threat Finance Course is a 3-day course provided in Washington, DC; at CCMDs, and other sites, providing analysts with indicators and triggers needed to uncover money trails used to support terrorist activities, trafficking, trade finance, and other international crimes/schemes. The Threat Finance Course provides tools and techniques used to analyze financial networks and provide actionable intelligence. It focuses on how money moves through banks, money service businesses, informal value transfer systems (e.g., Hawala), and virtual economies. The course uses learning through student discovery, participation, and practical exercises (https://www.intelink.gov/wiki/Threat_Finance_Course).

6. (U) Education Programs

a. (U) Mercyhurst College, Department of Intelligence Studies (http://intel.mercyhurst.edu/content/applied_intelligence_graduate_certificate) offers a Graduate Certificate in Applied Intelligence.

b. (U) Henley – Putnam University (<http://www.henley-putnam.edu>) offers Certificate Programs in Intelligence Collection, Intelligence Analysis, and Intelligence and Terrorism Profiling.

Intentionally Blank

APPENDIX F
REFERENCES (U)

1. (U) United States Government Laws, Executive Orders, and Reports

a. (U) U.S. Congress. Duncan Hunter National Defense Authorization Act for Fiscal Year 2009. Public Law 110-417, 110th Cong., 2d sess., October 14, 2008. http://www.dod.gov/dodgc/olc/docs/2009NDAA_PL110-417.pdf.

b. (U) U.S. Congress. National Defense Authorization Act for Fiscal Year 2010. Public Law 111-84. 111th Cong., 1st sess., October 28, 2009. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_public_laws&docid=f:publ084.111.pdf.

c. (U) U.S. Congress. National Defense Authorization Act for Fiscal Year 2008. Public Law 110-181. 110th Cong., 2d sess., January 28, 2008. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ181.110.pdf.

d. (U) U.S. Congress. House. Subcommittee on National Security and Foreign Affairs of the Committee on Oversight and Government Reform. Warlord, Inc.: Extortions and Corruption Along the U.S. Supply Chain in Afghanistan. 111th Cong., 2nd sess., 2010. http://www.oversight.house.gov/images/stories/subcommittees/NS_Subcommittee/6.22.10_HNT_HEARING/Warlord_Inc_compress.pdf.

e. (U) U.S. Government Accountability Office (GAO). International Security: DOD and State Need to Improve Sustainment Planning and Monitoring and Evaluation for Section 1206 and 1207 Assistance Programs. GAO-10431, Washington DC: Government Printing Office, April 15, 2010. <http://www.gao.gov/new.items/d10431.pdf>.

f. (U) U.S. Government Accountability Office (GAO). Iraq and Afghanistan: Agencies Face Challenges in Tracking Contracts, Grants, Cooperative Agreements, and Associated Personnel. GAO-10-509T, Washington DC: Government Printing Office, March 23, 2010. <http://www.gao.gov/new.items/d10509t.pdf>.

g. (U) U.S. Government Accountability Office (GAO). Military Operations: Actions Needed to Improve Oversight and Interagency Coordination for the JFC's Emergency Response Program in Afghanistan. GAO-09-615, Washington DC: Government Printing Office, May 2009. <http://www.gao.gov/new.items/d09615.pdf>.

h. (U) Commission on Wartime Contracting. "Commission on Wartime Contracting in Iraq and Afghanistan." <http://www.wartimecontracting.gov>.

i. (U) Executive Order 13224, *Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism*

Appendix F

j. (U) Special Inspector General for Afghanistan Reconstruction. Quarterly Report to the United States Congress. Arlington, VA: SIGAR, October 30, 2009. <http://www.sigar.mil/Oct2009Report.asp>.

2. Department of Defense Issuances

a. (U) DODD 5205.14, *DOD Counter Threat Finance (CTF) Policy*.

b. (U) DOD 5105.38-M. *Security Assistance Management Manual*. www.dsca.mil/samm/.

c. (U) *Department of Defense Counter Threat Finance Roadmap: Combating 21st Century National Security Threats*. 01 November 2010.

3. (U) Chairman of the Joint Chiefs of Staff Issuances

Irregular Warfare: Countering Irregular Threats, Joint Operating Concept, Version 2.0, 17 May 2010, http://www.dtic.mil/futurejointwarfare/concepts/iw_joc2_0.pdf.

4. (U) Non-Department of Defense Agency Issuances

a. (U) US Institute of Peace. *Measuring Progress in Conflict Environments (MPICE): A Metrics Framework*, <http://www.usip.org/publications/measuring-progress-conflict-environments-mpice>

b. (U) United States Institute of Peace. *Guidelines for Relations between U.S. Armed Forces and Non-Governmental Humanitarian Organizations in Hostile or Potentially Hostile Environments*. Washington DC: United States Institute of Peace. http://www.usip.org/files/resources/guidelines_pamphlet.pdf.

5. (U) Joint Publications, Directives, and Papers

a. (U) JP 4-10. *Operational Contract Support*. Joint Chiefs of Staff, October 17, 2008. http://www.dtic.mil/doctrine/new_pubs/jp4_10.pdf.

b. (U) United States Joint Forces Command. *Handbook for Military Support to Economic Stabilization*. Unified Action Handbook Series, Book Four, February 27, 2010. http://www.dtic.mil/doctrine/doctrine/jwfc/econ_hbk.pdf.

c. (U) United States European Command. *Handbook of Theater Security Cooperation Resources*, February 2010.

6. (U) Army Publications and Lessons Learned

- a. (U) Center for Army Lessons Learned. *Assessment and Measures of Effectiveness in Stability Ops Handbook: Tactics, Techniques, and Procedures*. No. 10-41, Leavenworth, KS: Center for Army Lessons Learned, May 2010. <http://usacac.army.mil/cac2/call/docs/10-41/10-41.pdf>.
- b. (U) Center for Army Lessons Learned. *JFC's Guide to Money as a Weapons System: Tactics, Techniques, and Procedures*. No. 09-27, Ft. Leavenworth, KS: Center for Army Lessons Learned, 2009. <http://usacac.army.mil/cac2/call/docs/09-27/toc.asp>.
- c. (U) National Training Center Operations Group *Attack the Network Handbook*.
- d. (U) US Army Asymmetric Warfare Group's *Counter Threat Finance Handbook*.

7. (U) Academic Resources

- a. (U) AKSS- Ask a Professor. "Welcome to Ask a Professor!" Defense Acquisition University <https://akss.dau.mil/askaprof-akss/>.
- b. (U) Defense Acquisition University. "DAU Home page." Defense Acquisition University. <http://www.dau.mil/>.
- c. (U) Defense Institute of Security Assistance Management, *The Management of Security Assistance*. The Twenty-Ninth Edition, Wright-Patterson AFB, Ohio. January 2010. www.disam.dsca.mil/DR/29th%20Gbook.pdf.
- d. (U) Joint Special Operations University Report 08-3, *Disrupting Threat Finances Using Financial Information to Disrupt Terrorist Organizations* Wesley J.L. Anderson.
- e. (U) Malkasian, Carter and Gerald Meyerle. *Provincial Reconstruction Teams: How Do We Know They Work*. Carlisle, PA: Strategic Studies Institute, March 2009. <http://www.strategicstudiesinstitute.army.mil/pdf/files/PUB911.pdf>.
- f. (U) Peterson, Marilyn; *A Guide to Counter Threat Finance Intelligence*.

8. (U) Books and Articles

- a. (U) Bracken, Paul. "Financial Warfare." <http://www.fpri.org/enotes/200709.bracken.financialwarfare.html>.
- b. (U) Hunt, James P. "The 800-Pound Gorilla and Stability Operations." *Small Wars Journal* (June 30, 2010). <http://smallwarsjournal.com/blog/2010/06/print/the-800poundgorilla-and-stabi/>.

c. (U) Islamic Republic of Afghanistan. *Afghanistan National Development Strategy:*

1387 – 1391 (2008 – 2013); *A Strategy for Security, Governance, Economic Growth and Poverty Reduction*. Kabul, Afghanistan: Gul Khana Palace, 2008.

d. (U) Lee, Mark W. “The JFC’s Emergency Response Program: Synergistic Results Through Training.” *Army Sustainment* 42, no. 3 (May-June 2010). http://www.almc.army.mil/alog/synergy_thrutrain.html.

e. (U) Levitt, Matthew “Follow the Money: Leveraging Financial Intelligence to Combat Transnational Threats,” *Georgetown Journal of International Affairs*, Winter/Spring 2011.

f. (U) Levitt, Matthew and Michael Jacobson *The Money Trail Finding, Following, and Freezing Terrorist Finances*, Policy Focus #89, Washington Institute for Near East Policy.

g. (U) Long, William. “Joint Contingency Contracting: A Step Forward.” *Defense AT&L*, May-June 2010. http://www.dau.mil/pubscats/ATL%20Docs/May-Jun10/long_may-june10.pdf.

h. (U) Luck, Gary, and Mike Findlay. *Interagency, Intergovernmental, Nongovernmental, and Private Sector Coordination*, Focus Paper #3, 2nd ed. Joint Warfighting Center United States Joint Forces Command, February 2009. <https://jko.cmil.org/file/124/view>.

i. (U) NATO-News. “Provincial Reconstruction Teams Look at Way Forward in Afghanistan.” NATO, March 16-17, 2010. http://www.nato.int/cps/en/SID-2296AC14-289F6401/natolive/news_62256.htm.

j. (U) Non-Governmental Organization/DPI. “About NGO Association with the UN.” United Nations DPI-NGO. <http://www.un.org/dpi/ngosection/about-ngo-assoc.asp>.

k. (U) Wojciechowski, Mark. “CIDNE Empowers Theater-wide Communication.” *USASOC News Service*, February 14, 2006. <http://news.soc.mil/releases/News%20Archive/2006/06FEB/060214-02.html>.

9. (U) Online Resources

a. (U) Combined Information Data Network Exchange. <http://www.issinc.com/solutions/cidne.html>.

b. (U) Joint Knowledge Online (JKO). <http://jko.jfcom.mil/>, <http://jko.jwfc.jfcom.smil.mil>, <http://jko.cmil.org>.

APPENDIX G
ENDNOTES (U)

¹ (U) Jacobson, Michael and Matthew Levitt. “The Money Trail: Finding, Following, Freezing Terrorist Finances.” The Washington Institute for Near East Policy, November 2008. p. 1. <http://www.washingtoninstitute.org/pubPDFs/PolicyFocus89.pdf>.

² (U) Ibid.

³ (U) Ibid.

⁴ (U) International Criminal Police Organization. Anti-Money Laundering Unit. <http://www.interpol.int/Public/FinancialCrime/MoneyLaundering/Unit.asp>.

⁵ (U) Anne L. Clunan, “The Fight against Terrorist Financing,” Political Science Quarterly, Vol. 121, No. 4 (2006): 570.

⁶ (U) Ibid., p. 570.

⁷ Ibid., p. 570.

⁸ (U) World Council of Credit Unions. “What is a Credit Union?” <http://www.woccu.org/about/creditunion>.

⁹ (U) Financial Action Task Force. “Terrorist Financing.” 29 February 2008. <http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf>.

¹⁰ (U) Olson, Dean T. “Financing Terror.” FBI Law Enforcement Bulletin. FBI Academy. Feb 2007. p. 4.

¹¹ (U) Jost, Patrick M. and Harjit Singh Sandhu. “The hawala alternative remittance system and its role in money laundering.” Interpol. Jan 2009.ets.

Intentionally Blank

GLOSSARY

PART I — ABBREVIATIONS AND ACRONYMS (U)

AML	anti-money laundering
AOR	area of responsibility
ATF	(Bureau of) Alcohol Tobacco, and Firearms (and Explosives)
ATFC	Afghan Threat Finance Cell
BSA	Bank Secrecy Act
C2	command and control
CBP	US Customs and Border Protection
CCDR	combatant commander
CCMD	combatant command
CGIS	Coast Guard Investigative Service
CIA	Central Intelligence Agency
CMO	civil military operations
COA	course of action
COIN	counterinsurgency
COM	chief of mission
CONOPS	concept of operations
CSG	counterterrorism security group
CT	counterterrorism
CTF	counter threat finance
CTFI	counter threat finance intelligence
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DOD	Department of Defense
DODD	DOD Directive
DOJ	Department of Justice
DOS	Department of State
DOTMLPF	doctrine, organization, training, materiel, leadership and education, personnel, and facilities
EEB	(Bureau of) Economic Energy and Business Affairs
FATF	financial action task force
FBI	Federal Bureau of Investigation
FID	foreign internal defense
FinCEN	Financial Crimes Enforcement Network
FINOOB	Financial Order of Battle
FIU	financial intelligence unit

Glossary

FOUO	for official use only
FTF	fusion task force
GCC	geographic combatant command
GEOINT	geospatial intelligence
HN	host nation
HUMINT	human intelligence
ICE	Immigration and Customs Enforcement
IED	improvised explosive device
IGO	intergovernmental organization
IIFC	Islamic investment and finance cooperatives
INL	(Bureau of) International Narcotics and Law Enforcement Affairs
INTERPOL	International Criminal Police Organization
IRS	Internal Revenue Service
IRS-CI	Internal Revenue Service - Criminal Investigations
ITFC	Iraq Threat Finance Cell
JIACG	Joint Interagency Coordination Group
JFC	Joint Force Commander
JIPOE	Joint Intelligence Preparation of the Operational Environment
JOPP	Joint Operations Planning Process
JP	Joint Publication
JPME	joint professional military education
JTF	joint task force
JTTF	joint terrorism task force
MISO	Military Information Support Operations
MOE	measure of effectiveness
NCTC	National Counterterrorism Center
NDU	National Defense University
NGO	nongovernmental organization
NSC	National Security Council
NSS	National Security Staff
OCDETF	Organized Crime Drug Enforcement Task Forces
ODNI	Office of the Director of National Intelligence
OFAC	Office of Foreign Asset Control
OIA	Office of Intelligence Analysis
OJT	On-The-Job Training
PIR	priority intelligence requirement

ROE	rules of engagement
SAO	security assistance officer
S/CT	Department of State Office of the Coordinator for Counter Terrorism
SIGINT	signals intelligence
TBML	trade based money laundering
TFC	threat finance cell
TFFC	(Office of) Terrorist Financing and Financial Crimes
TFI	(Office of) Terrorism Financial Intelligence
TFEU	threat finance exploitation unit
TFOS	Terrorist Financing Operations Section
TF Sub-CSG	Terrorism Finance Sub-Counterterrorism Security Group
TFWG	Terrorist Finance Working Group
TTP	tactics, techniques, and procedures
UJTL	universal joint tasks list
UN	United Nations
UNSCR	United Nations Security Council Resolution
USC	US Code
USCG	US Coast Guard
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of defense for Policy
USG	US government
USCENTCOM	US Central Command
USSOCOM	US Special Operations Command
USSOUTHCOM	US Southern Command
WMD	weapon(s) of mass destruction

Intentionally Blank

PART II — TERMS AND DEFINITIONS (U)

adversary. A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged. (JP 1-02. SOURCE: JP 3-0)

assessment. 1. A continuous process that measures the overall effectiveness of employing joint force capabilities during military operations. 2. Determination of the progress toward accomplishing a task, creating an effect, or achieving an objective. 3. Analysis of the security, effectiveness, and potential of an existing or planned intelligence activity. 4. Judgment of the motives, qualifications, and characteristics of present or prospective employees or “agents.” (JP 1-02. SOURCE: JP 3-0)

beneficiary. The ultimate party to be credited or paid as a result of the funds transfer, or the receiver. (SOURCE: Financial Crimes Enforcement Network or FinCEN).

beneficiary’s financial institution. The financial institution that is to credit or pay the Beneficiary party. (SOURCE: FinCEN).

bulk cash smuggling. The movement of large amounts of currency usually across a border - currency may be carried or shipped in compartments or other means to avoid detection. (SOURCE: Army Asymmetric Warfare Group CTF Handbook)

civil affairs. Designated Active and Reserve component forces and units organized, trained, and equipped specifically to conduct civil affairs activities and to support civil-military operations. Also called CA. (JP 1-02. SOURCE: JP 3-57)

civil-military operations. The activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate military operations, to consolidate and achieve operational US objectives. Civil-military operations may include performance by military forces of activities and functions normally the responsibility of the local, regional, or national government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. Civil military operations may be performed by designated civil affairs, by other military forces, or by a combination of civil affairs and other forces. Also called CMO. (JP 1-02. SOURCE: JP 3-57)

civil-military operations center. An organization normally comprised of civil affairs, established to plan and facilitate coordination of activities of the Armed Forces of the United States with indigenous populations and institutions, the private sector, intergovernmental organizations, nongovernmental organizations, multinational forces, and other governmental agencies in support of the joint force commander. Also called CMOC. See also civil-military operations. (JP 1-02. SOURCE: JP 3-57)

Glossary

coalition. An ad hoc arrangement between two or more nations for common action. See also **multinational**. (JP 1-02. SOURCE: JP 5-0)

counterinsurgency. Comprehensive civilian and military efforts taken to defeat an insurgency and to address any core grievances. Also called COIN. (JP 1-02. SOURCE: JP 3-24)

counterterrorism. actions taken directly against terrorist networks and indirectly to influence and render global and regional environments inhospitable to terrorist networks. (JP 1-02. SOURCE: JP 3-26)

counter threat finance. “The means to detect, identify, deny, destroy, defeat, contain, disrupt, exploit, deter, or dismantle the collection, storage, transmission, distribution, and usage of currency, assets or resources, which support state and non-state threats to US national security.” (SOURCE: working definition)

country team. The senior, in-country, US coordinating and supervising body, headed by the chief of the US diplomatic mission, and composed of the senior member of each represented US department or agency, as desired by the chief of the US diplomatic mission. (JP 1-02. SOURCE: JP 3-07.4)

end state. The set of required conditions that defines achievement of the commander’s objectives. (JP 1-02. SOURCE: JP 3-0)

financial institution. Any person or entity who conducts a financial activity or operation on behalf of a customer as a business activities include acceptance of deposits, lending, financial leasing, transfer of money or value, money and currency changing, etc. (SOURCE: Army Asymmetric Warfare Group CTF Handbook)

financial management. Financial management encompasses the two core functions of resource management and finance support. Also called FM. (JP 1-02. SOURCE: JP 1-06)

generation. During the generation stage, activities or conduct are undertaken to acquire monetary proceeds or commodities/goods to support or profit from an illegal activity or, in some instances, move value acquired legally. In the instance of terrorism, licit sources of funds may include state sponsors, donations from individuals or businesses, or money from charities or NGOs. (SOURCE: Army Asymmetric Warfare Group CTF Handbook)

hawala(dar). Informal banking or alternative remittance system in South Asia and the Middle East areas that has existed for centuries. Hawala is dependent upon personal relationships between hawaladars and allows value to be moved upon request from one area or country to another. A hawaladar is the individual operating the hawala. (SOURCE: Army Asymmetric Warfare Group CTF Handbook)

host nation. A nation that receives the forces and/or supplies of allied nations, coalition partners, and/or NATO organizations to be located on, to operate in, or to transit through its territory. Also called HN. (JP 1-02. SOURCE: JP 3-57)

integrated financial operations (IFO). The integration, synchronization, prioritization and targeting of fiscal resources and capabilities across US agencies, multinational partners, and nongovernmental organizations against an enemy and in support of the population, combined with minimizing the possibility that such resources/capabilities will be diverted or inadvertently misused to support an enemy's financial networks. (SOURCE: *Integrated Financial Operations JFC's Handbook* a Joint Force Guide to Financial Operations.)

integration. The return of funds to the beneficiary in a form that appears to be legitimate after the placement and layering stages of traditional money laundering. The funds may be brought back as a loan, salary, commission, or proceeds of other legal activity. It is at this point that funds have been sufficiently separated from their probable illicit origins that they are considered laundered. (SOURCE: Army Asymmetric Warfare Group CTF Handbook)

interagency coordination. Within the context of Department of Defense involvement, the coordination that occurs between elements of Department of Defense, and engaged US Government agencies for the purpose of achieving an objective. (JP 1-02. SOURCE: JP 3-0)

intergovernmental organization. An organization created by a formal agreement (e.g. a treaty) between two or more governments. It may be established on a global, regional, or functional basis for wide-ranging or narrowly defined purposes. Formed to protect and promote national interests shared by member states. Examples include the United Nations, North Atlantic Treaty Organization, and the African Union. Also called IGO. (JP 1-02. SOURCE: JP 3-08)

irregular warfare. A violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). Irregular warfare favors indirect and asymmetric approaches, although it may employ the full range of military and other capacities, in order to erode an adversary's power, influence, and will. Also called IW. (JP 1-02. SOURCE: JP 1-0)

insurgency. The organized use of subversion and violence by a group or movement that seeks to overthrow or force the change of a governing authority. Insurgency can also refer to the group itself. (JP 1-02. SOURCE: JP 3-24)

joint force commander. A general term applied to a combatant commander, sub-unified commander, or joint task force commander authorized to exercise combatant command (command authority) or operational control over a joint force. Also called JFC. (JP 1-02.)

Glossary

joint task force. A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a sub-unified commander, or an existing joint task force commander. Also called JTF. (JP 1-02. SOURCE: JP 1)

lead agency. Designated among US Government agencies to coordinate the interagency oversight of the day-to-day conduct of an ongoing operation. The lead agency is to chair the interagency working group established to coordinate policy related to a particular operation. The lead agency determines the agenda, ensures cohesion among the agencies and is responsible for implementing decisions. (JP 1-02. SOURCE: JP 3-08)

measure of effectiveness. A criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect. Also called MOE. (JP1-02. SOURCE: JP 3-0).

measure of performance. A criterion to assess friendly actions that is tied to measuring task accomplishment. Also called MOP. (JP1-02. SOURCE: JP 3-0)

multinational. Between two or more forces or agencies of two or more nations or coalition partners. (JP 1-02. SOURCE: JP 5-0)

nongovernmental organization. A private, self-governing, not-for-profit organization dedicated to alleviating human suffering; and/or promoting education, health care, economic development, environmental protection, human rights, and conflict resolution; and/or encouraging the establishment of democratic institutions and civil society. Also called NGO. (JP 1-02. SOURCE: JP 3-08)

operational area. An overarching term encompassing more descriptive terms for geographic areas in which military operations are conducted. Operational areas include, but are not limited to, such descriptors as area of responsibility, theater of war, theater of operations, joint operations area, amphibious objective area, joint special operations area, and area of operations. Also called OA. (JP 1-02. SOURCE: JP 3-0)

order of battle. The identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force. (JP 1- 02. SOURCE: JP 2-01.3)

originator. The individual or organization that initiates the fund transfer, or the Sender. (SOURCE: FinCEN).

originator's financial institution. The financial institution receiving the transfer instructions from the Originator and transmitting the instructions to the next party in the funds transfer. (SOURCE: FinCEN).

placement. The physical movement of currency into the banking system, either in the country of origin or in another country's system. It is the first phase in traditional money laundering. (SOURCE: Army Asymmetric Warfare Group CTF Handbook)

remittance. Money sent by one person to another, either in specie, bill of exchange, check, or otherwise. (SOURCE: Black's Law Dictionary, 1990, St. Paul, MN: West Publishing Company)

stability operations. An overarching term encompassing various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. (JP 1-02. SOURCE: JP 3-0)

third party. Individual involved in a third party transaction which usually includes the writer of a monetary instrument, the payee on the monetary instrument and a third person to whom the instrument is endorsed. (SOURCE: Army Asymmetric Warfare Group CTF Handbook)

threat finance. The manner in which adversarial groups move and use funds to support their illegal activities or profit from them. (SOURCE: Army Asymmetric Warfare Group CTF Handbook)

trade-based money laundering. An alternative remittance system in which earned, moved and stored proceeds can be disguised as legitimate trade. Value can be moved through this process by false-invoicing, over-invoicing and under-invoicing commodities that are imported or exported around the world. (SOURCE: US Immigration and Customs Enforcement)

unified action. The synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort. (JP 1-02. SOURCE: JP 1)

wire transfer. Any transaction carried out on behalf of an originator person through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. (SOURCE: Financial Action Task Force, 2004, FATF Reference Document – Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations. Paris, France: Financial Action Task Force).

Intentionally Blank

Intentionally Blank



Developed by the
Joint Staff, J-7
Joint and Coalition Warfighting