

AU/ACSC/5611/SUMMER B AY10

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

**Disrupting Illicit Trafficking Networks:  
Defining the DoD's Role as Part of a Strategic Network Focused  
Strategy to Disrupt Illicit Trafficking Networks**

by

Malcolm N. Pharr, Major, USAF

Advisor: Fred P. Stone, Col, USAF

Maxwell Air Force Base, Alabama

August 2010

**APPROVED FOR PUBLIC RELEASE: DISTRIBUTION UNLIMITED**

### **Disclaimer**

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the U.S. Government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the U.S. Government.

# Table of Contents

<b>Abstract</b>	<b>iv</b>
<b>Introduction</b>	<b>1</b>
<i>Research Question</i>	5
<i>Research Framework</i>	6
<i>Outline</i>	6
<i>Scope</i>	7
<b>A Collaborative and Network Focused Approach</b>	<b>9</b>
<i>Why Focus on the Network?</i>	9
<i>A Strategic Network Focused Approach</i>	11
<i>Strategic Network Analysis</i>	12
<i>Strategic Network Attack</i>	15
<i>Department of Defense's Involvement in Combating Illicit Trafficking</i>	17
<b>Methodology and Evaluation Criteria</b>	<b>21</b>
<i>Appropriateness</i>	21
<i>Cost</i>	22
<i>Legality</i>	23
<i>Lethality</i>	24
<i>Risk</i>	24
<b>DoD Roles in Strategic Network Analysis and Attack:</b>	<b>26</b>
<i>DoD roles in Strategic Network Analysis</i>	27
<i>Network Intelligence Collection</i>	29
<i>Analytical Process</i>	33
<i>DoD roles in Strategic Network Attack</i>	36
<i>Strategic Network Attack Roles</i>	39
<b>Conclusion</b>	<b>44</b>
<b>Recommendations</b>	<b>51</b>

## List of Tables

<b>Table 1.</b> <i>Evaluation of DoD roles in Strategic Network Analysis</i>	29
<b>Table 2.</b> <i>Evaluation of DoD roles in Strategic Network Attack</i>	39

## **Abstract**

In the twenty-first century, globalization has linked transnational crime, illicit trafficking, and terrorists. These groups were once distinct in function and makeup, but have now become increasingly similar and connected by decentralized networks and financed by an ever-expanding global illicit economy. Collaboratively these illicit networks pose ever-increasing threats to the national security of countries across the globe. Efforts to counter the threats posed by the broad scope of illicit trafficking is being collaboratively developed by governments across the globe. This paper examined a strategic focused network approach at disrupting illicit trafficking networks and defined the U.S. Department of Defense's role within this strategy. The two phases of the strategy, strategic network analysis and strategic network attack, were examined and possible DoD roles evaluated utilizing the provisions for civilian cooperation set up in US Code Title 10, Ch 18 and DoD Directive 3025.15. The evaluation found that although the DoD primarily plays a supporting role in counter illicit trafficking it has unique capabilities and resources that are invaluable to the overall process. The conclusion and recommendations outline the similarities between current DoD counternarcotics trafficking and counterterrorism operations and suggest ways for the DoD to be integrated into the strategy as full and active partners with this interagency and international effort.

## Introduction

*“In recent years, the world has seen a convergence of transnational threats and networks, which are more dangerous and destabilizing than ever. These threats and networks are becoming more fluid and sophisticated; are able to cross borders; and involve elements of international organized crime, particularly illicit finance and trafficking in drugs, arms and persons. This can undermine stability and security, fuel violence and corruption, weaken the rule of law, and subvert legitimate economies. Addressing these 21<sup>st</sup> century transnational threats is an important priority of the United States.”*

President Barack Obama

Opening message at the Trans-Pacific Symposium, November 2009

At the onset of the twenty-first century, non-state actors grabbed the attention of nations across the world when Al-Qaeda carried out a set of coordinated and deadly attacks on the United States of America. The end of the twentieth century brought globalization, which connected the economies and peoples of the world. Unexpectedly, it also gave new tools and opportunities to criminals and terrorists to collaborate, communicate, and exchange resources.<sup>1</sup> Organizationally and operationally they lowered their profiles and migrated away from hierarchical organizations and towards decentralized network structures.<sup>2</sup> Illicit traffickers gained new and expanding ways to get trafficked goods to a wider global market. Criminal and terrorist groups found a rapidly expanding illicit economy to finance their operations that would not scrutinize their ideology or goals.<sup>3</sup>

Neither illicit trafficking nor terrorism are new phenomena. Dr. Moisés Naím, current editor-in-chief of *Foreign Policy* magazine, former university professor and dean, Venezuelan

Minister of Trade, and executive Director at the World Bank, has written extensively on the subject of illicit trafficking, explains this in his book, “Illicit: How smugglers, traffickers, and copycats are hijacking the global economy.” Black markets flourished in Europe and the United States during World Wars I and II and the great depression.<sup>4</sup> Likewise, terrorism has long been employed as a leveraging tool by the weak against the strong. Its use has not been exclusive to radical Islamic groups either, but also employed by anarchists, nationalists, anti-colonialists, political activists, and extremists of various religions.<sup>5</sup> What is unique about these activities in the twenty-first century is that they have become connected on a global scale. Historically, the primary threat of illicit trafficking derived from either the product itself, such as is the case with illicit drugs, arms, and human trafficking, or an economic concern, such as with counterfeit products. With decentralized transnational global illicit networks the principle concern derives from the collective network versus that of its individual actors.

Even as far back as the early 1990s, the US National Drug Control Strategy proclaimed that federal law enforcement had already begun to upgrade its capacity to better understand and attack trafficking networks.<sup>6</sup> However, even though the term “networks” was being utilized during the 1990s, the networks utilized by illicit traffickers and the threats that they posed were not very well understood. Up until recently, many academics and policy makers thought about these networks primarily as traditional hierarchically structured organizations; therefore, their focus was heavily weighted towards attacking critical leadership nodes and kingpins.<sup>7</sup> Additionally, the threats posed by illicit trafficking were assessed to primarily affect economic and local interests, as opposed to being a national security concern. Therefore, the strategies that were developed to combat these groups focused on local leaders of hierarchical organizations.<sup>8</sup> Although these strategies were successful, they forced illicit trafficking

organizations to adapt their business in order to avoid government disruption of their operations. As prominent top-notch leadership constructs were replaced by more co-dependent partnering relationships, illicit trafficking began to decentralize adapt a more network-like construct.

While globalization created many new opportunities for connection and commerce across the globe, it also created large numbers of people who became displaced from their local economies because their industry could not adapt to the changing business environment. In some regions of the world the globalization opened a whole new group of economically displaced individuals who were ideally positioned to enter an alternate illicit global economy. While in other regions, displaced people began to channel their frustrations into ideologies that sympathized with their loss and distanced themselves from the agents that brought about this changing economy. Meanwhile, law enforcement became unable to see the real nature of the growing problem they faced because their scope was limited by tribal, local, state, and national boundaries while their adversaries operations transcended these boundaries.<sup>9</sup> Illicit actors devised creative ways to blend their operations into the legal world of commerce, while at the same time seeking out a wider base of illicit actors whose illicit nature made them natural business partners with whom they could more openly negotiate the illicit side of their ventures.<sup>10</sup> These circumstances created an environment that fostered increased linkages between criminal and terrorist groups through illicit trafficking. Illicit trafficking financed their criminal, ideological, and opportunistic enterprises, while helping them to establish powerful political influence.<sup>11</sup>

After 11 September 2001, governments around the world began to understand that the same globalization that had created new opportunities for legal international trade and globally connected economies gave rise to an ever-increasing globalized illicit economy as well.<sup>12</sup> As the

nexus between criminal groups, the full spectrum of illicit trafficking, and terrorism became increasingly illuminated, this problem's wide reaching threats developed into real concerns for governments across the globe. The resources generated from these illicit activities created a global illicit economy that grew outside of the rule of national or international law. This illicit economy became the logical venue for illicit organizations to participate in a rapidly developing and lucrative global economy. By the nature of its operations, its net worth is impossible to measure, but conservative estimates appraise it at over \$300 billion per year, or the equivalent of the world's twentieth largest economy.<sup>13</sup>

When the world began to realize the scope of resources that these networks had developed and the threat that they posed to the global economy and security; it also realized that these well-financed, decentralized, and globally adaptive networks, formed by loose alliances, had a distinct advantage over the bureaucratic governments of the world.<sup>14</sup> The networks were able to exploit the limitations that governments had placed on themselves by creating borders and limited sharing of information. The borders did not affect the illicit traffickers who did not respect them, but they did affect the governments that could only contend with the part of the network that stayed within their boundaries.

The strategic network focused strategy tackles the problem of illicit trafficking by refocusing the full spectrum of government efforts to collaboratively identify and strategically attack the network itself.<sup>15</sup> The concept was introduced to the U.S. government in the 2008 National Drug Control Strategy.<sup>16</sup> It zeroes in on the illicit network itself as the strategic center of gravity and root source of the threats posed by illicit trafficking. The approach is comprised of two main efforts: network analysis and strategic network attack. Network analysis combines collaborative efforts across the full spectrum of government intelligence collection and analysts,



to understand, map out, and target illicit trafficking networks. Strategic network attack is the offensive portion of the approach, which looks to attack the vulnerabilities of the network and disrupt its ability to operate as a cohesive system.

## **Research Question**

Illicit trafficking networks threaten the national security and sovereignty of States across the globe.<sup>17</sup> While it is true that DoD forces have long been active participants in actions aimed at thwarting illicit trafficking, especially in the western hemisphere; these efforts have traditionally been largely focused on interdiction and key leadership figures, rather than focused on their networks.<sup>18</sup> After 11 September 2001, the DoD became more engaged in disrupting terrorist networks and targeting illicit financial networks,<sup>19</sup> as part of the Global War on Terror. However, unlike terrorism, illicit trafficking is traditionally more of a focus of law enforcement rather than military. As illicit trafficking networks become more decentralized and seek refuge by intermingling their operations with legal commerce, the task of dismantling them becomes an increasingly predominant function of law enforcement and less of military.

Illicit trafficking networks represent a wide spectrum of actors and challenges and combating them requires a strong balance of all national instruments of power.<sup>20</sup> Additionally, as these networks become increasingly connected to terrorist networks, this threat has begun to merge with the DoD's primary lane of responsibility.<sup>21</sup> Such is the case in Afghanistan, where certain illicit traffickers and their resources, who have been deemed to be instrumental in financing insurgent operations against Coalition forces are being officially designated as legitimate military targets.<sup>22</sup> As the U.S. government looks to answer this growing challenge it will look to the various resources to assist in answering this threat. While it is true that the preponderance of this effort is not a function of military; the United States Department of

Defense has unique capabilities, resources, and skills that, when combined with other government instruments, increases the effectiveness of the overall strategy. Therefore this research asks the question; with the United States government pushing to develop a more interagency and network focused strategy that zeroes in on disrupting illicit trade networks, what role should the Department of Defense play within this strategy?

## **Research Framework**

This research utilizes an evaluation methodology to determine the most appropriate role of the U.S. Department of Defense within an interagency and international strategy focused on disrupting illicit trafficking networks. The research compares the parts of this strategy and examines Defense Department resources, skills, and capabilities that fit within the overall strategy. It then evaluate DoD roles utilizing the provisions for civilian cooperation set up in US Code Title 10, Ch 18 and DoD Directive 3025.15 in order to develop recommendations for how DoD resources should be integrated into the strategy, and in what capacity.

## **Outline**

This paper begins by laying out the components of the interagency and international, network focused strategy aimed at disrupting them. It explains why this strategy is being developed, the merits of a networked focused solution and how it is different from previous approaches. It explains why illicit networks have evolved into the decentralized transnational networks that they have and the strengths that this gives them. It also discusses the DoD's current role in combating illicit trafficking.

The paper then compares the main components of this strategy to resources, skills, and capabilities represented in the DoD. The areas that are identified are evaluated utilizing the

guidelines set forth in both US Code Title 10, Ch 18 and DoD Directive 3025.15 in order to determine the scope and capacity of DoD resources most appropriate to the overall strategy. It then evaluates DoD resources' participation in strategic network analysis and strategic network attack.

Finally the paper determines the most appropriate utilization of DoD assets in this strategy, as per the previous evaluation, and gives recommendations for why DoD should be integrated into the two basic elements of this strategy and in what capacity they should be utilized.

## **Scope**

This research focuses on evaluating the DoD's role in a network focused strategy to disrupt illicit trafficking networks. It acknowledges that a network focused approach is not a miracle solution to combating illicit trafficking. Rather, it is one of the many facets of an overall strategy that answer the ever increasing and emergent threat posed by illicit trafficking networks.<sup>23</sup> This research acknowledges other facets of counter illicit trafficking strategies such as the strengthening of traditional law enforcement, regional security, interdiction, traditional military counterdrug roles, eradication, and demand reduction, as they lend to the discussion of the network focused solution, but these areas are not the focus of this research. This research also acknowledges that many non-network focused facets of counter illicit trafficking efforts will continue to be necessary even alongside this network focused solution. Traditional law enforcement, civil and military security operations, and interdiction will continue to be important aspects of the overall strategy as these lay the basic foundation under which the government agencies can pursue illicit trafficking. This a real paradigm shift in the way that the United States and international community address the problems of illicit trafficking. One that moves away

from a traditional focus on individual leaders, actors, and trafficked products, towards a broader scope which targets the networks that allow them to conceal their operations and move their products alongside legal trade. This research specifically focuses on those aspects of counter illicit trafficking that focus on disrupting illicit trafficking networks.

### **Notes:**

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

- 
- <sup>1</sup> Williams, *Strategy for a New World*, 192.
  - <sup>2</sup> Arquilla and Ronfeldt, *Networks and Netwars*, 61-64.
  - <sup>3</sup> Naim, *Illicit*, 6-8.
  - <sup>4</sup> Craddick-Adams, *The Home Front in World War One*.
  - <sup>5</sup> Williams, *Strategy for a New World*, 194.
  - <sup>6</sup> Bush, *1991 National Drug Control Strategy*, 107.
  - <sup>7</sup> Cheatham, *A Strategy to Destabilize Drug Trafficking Networks*, 1.
  - <sup>8</sup> Arquilla and Ronfeldt, *Networks and Netwars*, 62.
  - <sup>9</sup> Williams, *Strategy for a New World*, 194.
  - <sup>10</sup> Serena, *Dynamic Attenuation*, 345-365.
  - <sup>11</sup> Naim, *Illicit*, 13.
  - <sup>12</sup> *Ibid.*, 7.
  - <sup>13</sup> Geneva Centre for Security Policy, *A Comprehensive Approach to Combating Illicit Trafficking*, 2.
  - <sup>14</sup> Williams, *Strategy for a New World*, 192-193.
  - <sup>15</sup> Cheatham, *A Strategy to Destabilize Drug Trafficking Networks*, 1.
  - <sup>16</sup> Bush, *2008 National Drug Control Strategy*, 50.
  - <sup>17</sup> United Nations, *International Day Against Drug Abuse and Illicit Trafficking*.
  - <sup>18</sup> Naim, *Illicit*, 4-7.
  - <sup>19</sup> Frothingham, *Tracking and Disrupting Terrorist Financial Networks*, 7-8.
  - <sup>20</sup> Geneva Centre for Security Policy, *A Comprehensive Approach to Combating Illicit Trafficking*, 21.
  - <sup>21</sup> Rollins and Wyler, *International Terrorism and Transnational Crime*, 5.
  - <sup>22</sup> Senate Committee on Foreign Relations, *Afghanistan's Narco War*, 1-2.
  - <sup>23</sup> Bergin, *Social Network Analysis of 'Dark Networks'*, 18.

## **A Collaborative and Network Focused Approach**

*Illicit trafficking poses the most serious hemispheric security challenge we all face. By illicit trafficking, I mean not just trafficking in drugs, but also weapons smuggling, trafficking in persons, and associated crimes such as money laundering and document forgery.*

General Douglas Fraser, United States Air Force

Commander, U.S. Southern Command

### **Why Focus on the Network?**

The concerns over threats posed by illicit groups such as criminals, traffickers, and terrorist were real concerns even before the twenty-first century or globalization. President Ronald Reagan officially declared illicit drug trafficking as a threat to national security when he issued National Security Directive 221 in 1986.<sup>24</sup> Today, the principle concern has shifted from the illicit activities of these groups and more towards the collaborative threats that they pose as they network together.<sup>25</sup> In addition to the increasingly inextricable linkages between narcotics trafficking and terrorism, transnational gangs, criminal groups, and terrorist have continually grown in size and strength. Funded by illicit trafficking, they have amassed the financial and political capital to threaten security and challenge the sovereignty of governments.<sup>26</sup> From the Eastern Pacific, to Afghanistan, to Africa, to South America, to the Caribbean, to Central America these groups intimidate government officials, compromise law enforcement, and weaken governments' ability to govern and provide basic security for its people.<sup>27</sup>

Although the term network has been utilized by social scientists for the past forty years to describe both formally and informally developed social structures, it was not until recently that

political scientist have utilized the term to describe both localized and transnational non-state actors.<sup>28</sup> The term network is utilized to describe social organizational structures that have migrated away from traditional hierarchical structures where communication and direction flow from the top down throughout the organization, towards a more horizontal and decentralized structure, where individual actors are given a high degree of autonomy for decision making.<sup>29</sup> During the process of globalization many businesses found that formulating formal and informal networks with sub-contractors, competitors and research institutions helped them maintain their competitive edge. Similarly, illicit actors utilized the technology and connections available in the globally connected market to transform their operations and structure. They found new ways to conduct and finance their operations by developing loose associations with other illicit actors and forming decentralized networks both locally and across the globe.<sup>30</sup>

This is not to say that hierarchies do not exist. In fact, al-Qaeda carried out its most successful attack when it was structured much more hierarchically than it is today.<sup>31</sup> Today hierarchies exist at the tactical and even operational levels of illicit networks. Nevertheless, at the strategic level, illicit trafficking organizations operate more as loose networks than they do as hierarchies. Additionally, just as al-Qaeda was forced to adapt their structure and become more dispersed and decentralized in order to survive in response to their own security challenges, illicit trafficking networks are having to do the same as they find themselves increasingly challenged by governments around the world.<sup>32</sup>

The existing literature on illicit networks explains that their agile and adaptable network structure allows them to exploit a wide array of resources and connections both globally and locally. Their ability to swiftly formulate and dissolve relationships in response to security and market changes makes them ideally structured to thrive in a dynamic global market.<sup>33</sup> On the

other hand, some authors such as, Eilstrup-Sangiovanni and Jones, who wrote “Assessing the Dangers of Illicit Networks: Why al-Qaida May Be Less Threatening Than Many Think,” feel that too much has been made of the threats that are posed by these illicit networks. Their view is that much of the existing literature readily declares these networks as insurmountable threats that cannot be overcome by bureaucratic governments; however, even they do not truly diminish the threats posed by these networks, but rather argue that the threats posed by them are readily surmountable if governments exploit the weaknesses of illicit clandestine network structure.<sup>34</sup> Thus, the common ground between scholars, authors, policy makers, and DoD leadership is that if governments are to defeat these illicit networks, the approach needs to be one that is tailored to the specific threats and vulnerabilities represented by these illicit networks.

### **A Strategic Network Focused Approach**

This approach addresses the problem of disrupting illicit networks by focusing on the strategic level centers of gravity of the networks.<sup>35</sup> It calls for a collaborative approach that utilizes the full spectrum of government. The concept of this strategic approach was first introduced to the U.S. government in the 2008 National Drug Control Strategy.<sup>36</sup> It focuses its efforts on the network itself as opposed to the individual leaders or products that are trafficked. It first looks to analyze the network and determine its scope, organization, structure, connections, nodes, strengths, and vulnerabilities. It then strategically targets the vulnerabilities of the illicit networks in a way that will cause long-term disruption of the networks’ ability to operate and function as a cohesive system. This approach is comprised of two main efforts, network analysis and strategic network attack. Network analysis stems from Sun Tzu’s assertion that it is imperative to know the enemy. Strategic network attack is the offensive portion of the approach,

which utilizes analytical strategic targeting to deliver an attack specifically tailored to the threats and vulnerabilities of the illicit network.

The concept of targeting and attacking an adversary at the strategic level is a concept that is well developed in DoD doctrine. According to U.S. military doctrine, a strategic approach concentrates its focus on the strategic center of gravity of the adversary system<sup>37</sup> and examines the adversary's entire system to develop the most effective method of targeting, disrupting, or influencing that system.<sup>38</sup> With transnational illicit trafficking networks, the most important strategic level center of gravity is the network that connects individual nodes together.<sup>39</sup> This strategy neither ignores nor denies the importance that key individuals, leadership and hierarchies play within illicit trafficking organizations. Its focus lies at the strategic level where the networks that connects decentralized networks, grants them greater freedom of action, allows them to avoid detection by state authorities, and gives them the cumulative ability to threaten national security.<sup>40</sup>

## **Strategic Network Analysis**

The Strategic Network Focused Strategy is not an intelligence process. It is, however, a process driven by intelligence. Strategic Network Analysis is the intelligence gathering and analytical process of this strategy. Information is gathered in order to visualize network structure and connectedness. That information is compiled and analyzed in order to understand the networks connections, functions, capabilities, strengths and weaknesses. Also important to the overall success of the process is analyst collaboration across the broad spectrum of intelligence and law enforcement. The final goal of the analyst is to create products that help develop targets for strategic attacks as well as identify key intelligence gaps in order to keep the process going and constantly update the analytical and targeting picture.



Intelligence is a key ingredient to combating illicit networks. Armed with a thorough understanding of the adversary network, analysts can assess the network's depth, capabilities, functions, linkages, strengths and weaknesses. Illicit networks understand this and constantly conduct their operations in order to keep its networks hidden from authorities. Government and law enforcement officials are already collecting some of the types of information needed for this process.<sup>41</sup> However, without focused analytical collaboration and assessment, this information is not often developed into products that are capable of being utilized to assess and target these illusive networks.<sup>42</sup> One effective way for this to occur is to have network focused analysts, compile the available information and determine intelligence gaps so that it can be tasked to government resources able to collect targeted information, which strengthens the utility of analytical products and hones target development.

Network analysis produces various products that enable effective targeting and strategic attack of the network. Many of these products are derived through social network visualization software tools that compile and analyze information about the network. These tools can produce network visualization illustrations that graphically depict the connections between network nodes. These visualization assist analysts in determining key nodes, connecting organizational relationships, and determining functional qualities of nodes. They can also be utilized to identify key characteristics such as their degree connectedness and functional importance to overall network functions.<sup>43</sup> These tools help break large quantities of information into manageable products and assist in overall network assessment and target development. In this way they help analysts produce tangible products that can be shared with leadership and policy makers. They also facilitate the conversion of information into a simplified form that is more easily shared with

partnering organizations, while minimizing the risk of compromising intelligence collection sources and methods.

Adaptive illicit transnational networks have an advantage over bureaucratically rigid governmental agencies that are limited by their own boundaries, borders, and jurisdictions.<sup>44</sup> Analytical collaboration across these barriers is the key to counter this advantage and allow separate government agencies to visualize the entire network. Without this key ingredient governments will be unable to successfully visualize the full scope of the network and illicit networks will continue to exploit these governmental blind spots in order to continue to elude detection and disruption. Increasing analytical collaboration and utilization of network visualization tools helps government agencies work to develop a common frame of reference and further facilitate information sharing across multiple platforms.<sup>45</sup>

Strategic Network Analysis is an intelligence operation and the U.S. government has various mechanisms in place to collect, analyze and utilize intelligence information. Across the United States intelligence operations are run locally by state and municipal law enforcement organizations and on a national and international scale through the U.S. Intelligence Community (IC), directed by the Director of National Intelligence (DNI). With the exception of the CIA, which is an independent agency of the U.S. government, IC members are offices or bureaus representing six different federal executive departments. Eight of the total sixteen IC members fall under the Department of Defense: the Air Force Intelligence, Surveillance and Reconnaissance Agency (AFISRA), Army Military Intelligence (MI), the Defense Intelligence Agency (DIA), Marine Corps Intelligence Activity (MCIA), the National Geospatial-Intelligence Agency (NGA), the National Reconnaissance Office (NRO), the National Security Agency (NSA), and the Office of Naval Intelligence (ONI).<sup>46</sup> Although the Central Intelligence Agency

(CIA) is the most well-known intelligence organization in the United States, the bulk of US government intelligence funding and personnel belong to the Department of Defense.<sup>47</sup>

## **Strategic Network Attack**

Strategic Network Attack is the operational offensive arm of the strategy. Armed with analytical intelligence products and a comprehensive understanding of the illicit network, offensive attacks are specifically designed to induce long-term system wide crippling effects on the illicit networks.<sup>48</sup> The U.S. National Military Strategic Plan for the War on Terrorism describes network resources, functions, and processes as the key elements that adversary networks need in order to remain cohesive, operate, and survive.<sup>49</sup> Network resources are critical requirements of network systems. These can be physical or non-physical entities consisting of people, key leadership, organizations, or locations. These are commonly referred to as network nodes. Functions are critical capabilities of the networked systems representing the roles, utilization, or specific purpose of individual players, nodes or resources of the network. Network processes are the actions or operations that serve as the basis for the connections that form between network resources. These processes serve as the critical linkages that form the decentralized structure of the overall network system.<sup>50</sup>

Traditional counter illicit trafficking strategies focused primarily on key resources of illicit organizations, with the hopes that neutralization or removal of these key resources would render the organization unable to continue operations. Strategic Network Attack focuses on these same key resources but centers its focus on efforts that will cause the most long lasting system wide disruption of the network. With decentralized networks, removing key nodes and resources is not often the best course of action for long-term disruption. These key nodes can become known entities that can be monitored in order to advance visualization of the overall

network. Decentralized networks may also have hierarchies at the operational and tactical level. Therefore network-targeting analysts evaluate the overall network and design network attacks in order to maximize disruption in the best and most lasting method available. This is also where network function comes into the picture. Armed with an understanding of the functionality of individual resources within the network attack can seek to remove or neutralize key nodes of similar function in order to cause system wide shock to the overall network by removing critical capabilities across the network. In much the same way network processes and connections can be evaluated for vulnerabilities and systematically attacked across the network.

Key elements are targeted for monitoring, degradation, or removal from the system depending on which action is assessed to cause the most long-term disruption of the overall network system. Strategic attacks are designed to incapacitate, or sufficiently degrade the network's key elements. These attack are conducted in such a way to induce stress on the entire network system.<sup>51</sup> It is extremely difficult to design attacks that will entirely cripple a network with a single blow. Therefore attacks are designed to strike with just enough intensity and frequency to systematically cause sufficient stress to the system that it causes a shock like incapacitation of targeted nodes and capabilities in order to induce long-term system wide network disruption.<sup>52</sup>

One key advantage of a decentralized networked system is its agility in flexing its operation and structure in response to emergent and dynamic threats to the networks operations. Strategic attacks must assess the networks adaptability if it is to counteract this advantage. Therefore attacks are not always intended to simply destroy or even cause long-term disruption of the network. Attacks are sometimes needed as part of the network analysis process in order to effectively map the networks structure and gauge its adaptability to stress. In this way some

attacks are specifically designed to induce just enough applied stress in order to induce a reaction that causes the targeted entity to reveal its processes, organization, functions, and adaptability.<sup>53</sup>

## **Department of Defense's Involvement in Combating Illicit Trafficking**

Since 1989, when U.S. law designated the DoD as the lead agency for the detection and monitoring of illegal drugs into the United States by air and sea, the department has been an active partner with law enforcement in combating illicit trafficking.<sup>54</sup> The DoD has numerous air and space based intelligence and reconnaissance collection platforms that currently operate around the world; some of which are already being utilized to collect intelligence on illicit trafficking.<sup>55</sup> Currently, these platforms are primarily utilized to monitor and detect in transit product movement.<sup>56</sup> The intelligence that they collect contributes to the overall picture but is more useful in detecting the outer layers of the network and interdiction. The focus of strategic network analysis is to uncover the nodes, functions, and connections of the network. In order to analyze the networks and develop strategic level attack, analysts need to combine information on product movement with a full spectrum of network information. Network intelligence can vary and may include: information gleaned through human contacts at various levels of the networks, interception of communication between key nodes, and government and law enforcement information covering import and export activities, financial sector, criminal activity, and local level illicit trafficking.<sup>57</sup> The DoD is not and cannot be expected to provide all or even the majority of this information; however with the unique capabilities and resources that the department maintains it has much to offer in support of this effort.<sup>58</sup>

Over the past twenty years illicit trafficking has gradually evolved and adapted to the changing world in which it operates. Today illicit trafficking involves much more than drugs, it include a whole myriad of illicit trafficking activities. In order to avoid government disruption,

illicit traffickers have found many creative methods of blurring the lines between legal trade and illicit trafficking. As illicit trafficking changes and the U.S. military is already in very high demand around the world, some have expressed concern about reevaluating the military's role in illicit trafficking.<sup>59</sup> In March of 2010, U.S. Senators Robert Menendez (D-NJ), a member of the Foreign Relations Committee, and Committee Chairman John Kerry (D-MA), introduced legislation called "Counternarcotics and Citizen Security for the Americas Act of 2010" (S.3172), which among many other recommendations, called for a reduction in the role of the military.<sup>60</sup> Amongst the reports published by various international agencies and forums on the subject of illicit trafficking, the preponderance of the focus is placed on civil law enforcement.<sup>61</sup> This is also true of the 2010 US National Security Strategy (NSS). Although the 2010 NSS calls for a multidisciplinary solution to disrupting illicit networks, it pairs illicit trafficking networks with law enforcement yet does not mention this topic specifically in conjunction with the military.

Although the DoD has not been the overall lead agency in counter illicit trafficking it has been a valuable contributor and an active partner in combating drugs and disrupting terrorist networks. Since 11 September 2001, it has become increasingly clear that drug trafficking organizations and terrorist have integrated themselves into vast global illicit networks. Although their motivations (from criminal, to opportunistic, to ideological), and the various trafficked products vary; they have joined a vast global economy with substantial political and economic capital around the world.

As the threat posed by illicit trafficking networks are becoming better understood, it is challenging governments around the world to revise their approach at combating them. Therefore the US government is revising its approach at leveraging joint, combined, and multinational

efforts to combat and dismantle these networks;<sup>62</sup> this is also the proper juncture in which to evaluate the most appropriate roles for the DoD to contribute to the overall effort.

## Notes:

---

<sup>24</sup> CJCS, *Joint Publication 3-07.4*, I-2.

<sup>25</sup> Luna, *Narco-Trafficking*.

<sup>26</sup> *Ibid.*

<sup>27</sup> Center for Strategic and International Studies, *PONI 2010 Spring Conferense*; Llorente and Arnson, *Fundación Ideas para la Paz*, 5; Luna, *Narco-Trafficking*; Pham, *Emerging West African Terror-Drug Nexus*; UNESCO Kabul, *Country Planning Document Afghanistan*, 5; Williams, *Drug Trafficking, Violence, and the State in Mexico*, 1-4;

<sup>28</sup> Eilstrup-Sangiovanni and Jones, *Assessing the Dangers of Illicit Networks*, 9-10.

<sup>29</sup> Arquilla and Ronfeldt, *Networks and Netwars*, 62-67; Eilstrup-Sangiovanni and Jones, *Assessing the Dangers of Illicit Networks*, 9; and Williams, *Strategy for a New World*, 199.

<sup>30</sup> Eilstrup-Sangiovanni and Jones, *Assessing the Dangers of Illicit Networks*, 10.

<sup>31</sup> Eilstrup-Sangiovanni and Jones, *Assessing the Dangers of Illicit Networks*, 34.

<sup>32</sup> Luna, *Dynamic Threat Mitigation*.

<sup>33</sup> Arquilla and Ronfeldt, *Networks and Netwars*, 7; Department of State, *Trans-Pacific Symposium*; Geneva Centre for Security Policy, *A Comprehensive Approach to Combating Illicit Trafficking*, 2; Luna, *Dynamic Threat Mitigation*; Naim, *Illicit*, 35; Weschler, *Senate Testimony May 2010*, 1-3; and Williams, *Strategy for a New World*, 199.

<sup>34</sup> Eilstrup-Sangiovanni and Jones, *Assessing the Dangers of Illicit Networks*, 9-10.

<sup>35</sup> Cheatham, *A Strategy to Destabilize Drug Trafficking Networks*, 1.

<sup>36</sup> Bush, *2008 National Drug Control Strategy*, 50.

<sup>37</sup> Chairman of the Joint Chiefs of Staff, *Joint Operation Publication 3-0, III-22*

<sup>38</sup> USAF, *Air Force Doctrine Document 2-1.2.*, 2.

<sup>39</sup> Luna, *Narco-Trafficking*.

<sup>40</sup> Williams, *Strategy for a New World*, 199.

<sup>41</sup> *Ibid.*, 194-207.

<sup>42</sup> Cheatham, *A Strategy to Destabilize Drug Trafficking Networks*, 1.

<sup>43</sup> Memon and Larsen, *Investigative Data Mining Toolkit*.

<sup>44</sup> Williams, *Strategy for a New World*, 207.

<sup>45</sup> Interagency OPSEC Support Staff, *Intelligence Collection Activities and Disciplines*.

<sup>46</sup> Director of National Intelligence, *Overview of the US Intelligence Community*.

<sup>47</sup> Best, *Intelligence Community Reorganization*.

<sup>48</sup> Bush, *National Drug Control Strategy*, 50.

<sup>49</sup> CJCS, *National Military Strategic Plan for the War on Terrorism*.

<sup>50</sup> *Ibid.*

<sup>51</sup> USAF, *Air Force Doctrine Document 2-1.2.*, 14.

<sup>52</sup> *Ibid.*, 14.

<sup>53</sup> Williams, *Strategy for a New World*, 194-207.

<sup>54</sup> CJCS, *Joint Publication 3-07.4*, I-2.

<sup>55</sup> Fraser, *2010 SOUETHCOM Posture Statement*, 17.

<sup>56</sup> Gates, *Remarks at the Halifax International Security Forum*.

<sup>57</sup> Geneva Centre for Security Policy, *A Comprehensive Approach to Combating Illicit Trafficking*, 23-27.

---

<sup>58</sup> Weschler, *Senate Testimony May 2010*, 1-3.

<sup>59</sup> Arquilla and Ronfeldt, *Networks and Netwars*, 62-67; Menendez and Kerry, *Counternarcotics and Citizen Security*; Santos, *Five false assumptions about the "war on drugs" in Latin America*.

<sup>60</sup> Menendez and Kerry, *Counternarcotics and Citizen Security*.

<sup>61</sup> Pham, *Criminal Networks in West Africa*; Geneva Centre for Security Policy, *A Comprehensive Approach to Combating Illicit Trafficking*; Royal United Services Institute, *Cross-Border Security Symposium*, 2-6; United Nations Office on Drugs and Crime, *World Drug Report 2010*.

<sup>62</sup> Cheatham, *A Strategy to Destabilize Drug Trafficking Networks*, 1.



## **Methodology and Evaluation Criteria**

This research develops recommendations for using DoD assets within a network focused strategy to disrupt illicit trafficking networks. It accomplishes this by comparing the two principle facets of the network focused strategy: Strategic Network Analysis and Strategic Network Attack, to DoD resources and capabilities. It then evaluates the appropriateness of utilization of these assets in support of civil authorities according to criteria established by DoD Directive 3025.15<sup>63</sup> and guided by DoD Directive 5525.5<sup>64</sup> and Title 10 U.S.C. Chapter 18.<sup>65</sup>

Illicit trafficking is increasingly conducted by decentralized networks, camouflaging its operations amongst legal trade. The effort to combat them is primarily focused on local and state law enforcement, the Department of Justice, and the Department of Homeland vice the Department of Defense. The DoD plays a supporting role to civil law enforcement. Therefore this research utilizes the criteria of legality, lethality, risk, cost, and appropriateness, in order to evaluate the utilization of DoD assets in support of civil authorities.<sup>66</sup>

### **Appropriateness**

DoD Directive 3025.15 describes appropriateness as it relates to whether the desired mission is in the interest of the DoD to conduct it.<sup>67</sup> The mission must be assessed to determine that DoD assets, as opposed to other U.S. government assets, are the best fit for the given mission. Additionally, while it is true that the DoD possesses many of the capabilities necessary to perform strategic network analysis, and illicit trafficking networks pose threats to national security, the DoD is neither the sole entity with capabilities that fit nor the sole protector of national security. The DoD must evaluate not just whether the proposed mission is appropriate

for DoD assets but whether other U.S. government assets are more appropriate to fulfill the mission.

The DoD plays a supporting role in counter illicit trafficking operations. According to the Foreign Assistance Act of 1961, responsibility for coordinating U.S. assistance for counter illicit trafficking is the Secretary of State.<sup>68</sup> DoD counter illicit trafficking roles in the United States are normally performed by National Guard forces. Many U.S. Government agencies have assets and capabilities that contribute to the overall mission. Therefore, when considering new roles for DoD forces to augment this effort it is important to evaluate whether the proposed role would be in the best interest of the department, whether DoD specific assets are the most suited to perform the given mission, and the possibility of training civil forces to perform that mission when it is best suited or more feasible for other entities to perform that function.<sup>69</sup>

While evaluating appropriateness, this research examines the mission and functions that are performed in each role. Considering that the DoD plays an overall supporting role in this strategy, appropriateness is one of the most discriminating factors in determining the utilization of DoD assets. Determining a role is appropriate does not automatically justify a particular role; on the other hand, if the role's appropriateness is in question, it is very difficult to justify that role as a valid utilization of DoD assets.

## **Cost**

Considering the resource constrained environment that DoD operates in, cost is also an important discriminating factor in the overall evaluation. DoD Directive 3025.15 describes cost as it relates to the impact that evaluated role has on the overall DoD budget.<sup>70</sup> The cost of any allocation of resources could have detrimental effects on other key capabilities as they all pull from the same finite financial resources available to the entire DoD. These costs include various

factors such as, training, specialized equipment, deployment, and sustainment. Costs are evaluated based on any cost incurred to DoD units and forces that are above and beyond those cost that are already budgeted for and incurred during normal previously existing DoD operations.<sup>71</sup> This research did not perform an exhaustive cost analysis on the roles. The purpose of the cost evaluation contained here is to determine the types of cost related to implementation and sustainment, which go above and beyond that which is currently being spent on these assets, and compare these costs in relation to other alternative roles.

## **Legality**

DoD Directive 3025.15 describes legality as compliance with laws.<sup>72</sup> While legality is always a consideration for planning any military involvement or operation, the issue becomes even more complicated for the DoD when it comes to operations that occur within the United States. Outside of the United States, DoD assets have much more freedom to operate and utilize their full capabilities. Aside from the Uniform Code of Military Justice, the Posse Comitatus Act of 1878 limits operations in the United States. The Posse Comitatus Act<sup>73</sup> prohibits the utilization of federally controlled military forces in civil law enforcement to “execute the laws,”<sup>74</sup> except when authorized by the Constitution or by Congress.

The Posse Comitatus Act restrictions poses the most significant barrier to US military performing law enforcement in the United States. Congress has passed other legislation that has facilitated U.S. military cooperation with civil law enforcement, such as: 10 U.S.C., sections 331–334, which applies in civil disturbances when requested by state government<sup>75</sup>, 10 U.S.C., sections 371–381, which applies to counter narcotics trafficking operations,<sup>76</sup> and various sections of U.S.C.<sup>77</sup> and the PATRIOT Acts I<sup>78</sup> and II,<sup>79</sup> which apply to counterterrorism operations. Additionally, U.S. National Guard forces are not specifically bound by Posse

Comitatus restrictions when operating under the control of State government under Title 32 U.S.C. authority.

This research examines the total spectrum of application of DoD assets against illicit networks; however, it is outside of the scope of this research to complete a thorough legal review of possible military operations. Therefore this research will not seek to create new missions or roles for the DoD, but rather seek to compare existing legal military capabilities and roles in order to apply them to meet the unique challenges posed by this specific strategy and will not evaluate roles in terms of legality.

## **Lethality**

DoD Directive 3025.15 describes lethality as the potential use of lethal force by or against DoD Forces.<sup>80</sup> While lethal force is neither a qualifier nor disqualifier, the case for utilizing offensive military kinetic capabilities against illicit trafficking must be substantially compelling in order to for it to outweigh the risk of political and public affairs consequences that could be associated the taking of life while operating in a non-combat environment in support of primarily civil effort. This research assesses the possibility of utilization of lethal force while accomplishing missions that support the strategy by examining roles to determine if application of lethal force is necessary to accomplish the examined offensive roles. It also assesses the likelihood of DoD forces needed to utilize lethal force in a force protection, or defensive manner, during operations.

## **Risk**

DoD Directive 3025.15 describes risk as it relates to the safety of DoD Forces.<sup>81</sup> While the DoD is accustomed to accepting a certain level of risk while conducting operations it is

important to evaluate the risks involved before committing valuable DoD personnel, and resources, towards a given objective. Roles that present a low risk to the safety of DoD forces will be considered as positively contributing to supporting utilization of DoD forces. Risk can come in the form of the possibility of physical damage to DoD assets during operations or standard force protection concern for a given area of operations. The risk of the DoD encountering possible political or governmental friction or conflict is also considered.

## Notes:

---

<sup>63</sup> Department of Defense , *Military Assistance to Civil Authorities*.

<sup>64</sup> Department of Defense, *Cooperation with Civilian Law Enforcement Officials*.

<sup>65</sup> United States Congress, *USC Title 10- Armed Forces*.

<sup>66</sup> Department of Defense , *Military Assistance to Civil Authorities*, 2-3.

<sup>67</sup> *Idid.*, 3.

<sup>68</sup> Seelke, Liana and Beittel, *Latin America and the Caribbean*, 18.

<sup>69</sup> Department of Defense , *Military Assistance to Civil Authorities*, 3.

<sup>70</sup> *Idid.*, 3.

<sup>71</sup> *Idid.*, 3.

<sup>72</sup> *Idid.*, 3.

<sup>73</sup> United States Congress, *18 USC Chapter 67*.

<sup>74</sup> *Ibid.*

<sup>75</sup> *Ibid.*

<sup>76</sup> United States Congress, *USC Title 10*.

<sup>77</sup> Doyle and Elsea, *Terrorism*, 2-4.

<sup>78</sup> United States Congress, *Public Law 107-56*.

<sup>79</sup> United States Congress, *Justice Enhancement and Domestic Security Act of 2003*.

<sup>80</sup> Department of Defense , *Military Assistance to Civil Authorities*, 3.

<sup>81</sup> *Idid.*, 3.

## **DoD Roles in Strategic Network Analysis and Attack:**

The biggest difficulty in evaluating DoD roles in Strategic Network Analysis and Attack is that currently, this strategy is not fully a reality, but more of a concept developed and being implemented at various levels across the U.S. government. In evaluating DoD roles this research examined preexisting roles performed by DoD assets through counter illicit narcotics trafficking as well as roles that DoD has already been involved in through its efforts to disrupt IED networks, terrorist networks, and counterthreat finance operations. However, at the time that the research was performed the DoD was not involved in the type of network approach described by the Strategic Network Focused Strategy. DoD roles were evaluated utilizing the criteria of appropriateness, cost, lethality, and risk. The legality of proposed roles is examined below but was not utilized as a discriminating evaluation factor as all of the roles are preexisting DoD roles and assumed to be legal.

The tables included in this section are a subjective graphical representation of the evaluation of DoD roles. The tables utilize three symbols. The check mark “√” is utilized to denote that the evaluation under the selected criterion positively supports utilization of DoD assets in that role. The x-mark “X” is utilized to denote that the evaluation under the selected criterion negatively detracts from utilization of DoD assets in that role. The dash “-” is utilized to denote that the evaluation under the selected criterion neither clearly supports, nor detracts from, utilization of DoD assets in that role. Along with the tables, this section contains a detailed description of the evaluated roles and analysis.

## **DoD roles in Strategic Network Analysis**

Strategic Network Analysis is the intelligence gathering and analytical process of this strategy. It follows the normal intelligence cycle utilized by the U.S. Intelligence Community, which flows through the steps of planning, direction, collection, analysis, production and dissemination, where dissemination flows back to guide planning and direction.<sup>82</sup> This section focuses on the collection and analytical parts of the overall cycle as the bulk of intelligence activity is represented by the two larger categories of intelligence collection and the analytical process.

Intelligence collection can be broken down into two broad categories of human intelligence collection and technical intelligence collection. Human Intelligence collection is also referred to as HUMINT and involves human interaction with sources. In the intelligence community technical intelligence collection goes by names such as SIGINT, IMINT, ELINT, COMINT, or MASINT,<sup>83</sup> that describe the various transmission sources and collection technologies utilized to collect these various types of information. For the sake of simplicity, this research will refer to all of these technical and technological collection methods as technical intelligence.

Illicit networks are social networks that rely heavily on their connections and relationships with others. As the intelligence community has honed its focus on terrorist networks it has found HUMINT information to be very important in piecing together the puzzles of illicit and clandestine networks.<sup>84</sup> HUMINT sources come in many different varieties. These sources may be witting or unwitting, tasked and compensated for their participation, or simply volunteer information. HUMINT information can be obtained by a number of different methods to include interrogation, debriefing, or elicitation.

Technical intelligence collection depends on the targeted network and the environment that it operates in. DoD capabilities range from airborne and space based platforms that perform reconnaissance, to communications interception, to computer network monitoring. Technical intelligence is a non-intrusive method of gaining information and monitoring the network.<sup>85</sup>

Once raw intelligence has been collected it must then be processed, analyzed and compiled into products that can be utilized by planners, policy makers and shared amongst other analytical partners.<sup>86</sup> The analytical process takes raw and unevaluated intelligence data, processes it, and integrates this data into the greater field of knowledge on the given subject. With illicit networks one of the primary challenges and goals of this process is visualization of these hidden networks. Analysts can also compile data and facilitate interagency intelligence sharing in order to collaboratively build a more complete picture of these hidden networks. Armed with a comprehensive understanding of the covert network's composition, connections, operations, and functions, the network can then be targeted for strategic disruption.

Legality is a valid concern for intelligence activity especially when there is a possibility that intelligence operations may occur in the United States. Collection of intelligence by DoD personnel within the United States is legally problematic and would require a thorough legal review before even considering such action. The majority of the legal restrictions that apply to collection on U.S. persons or on operations conducted in the United States, do not apply outside of the country when collecting on foreign entities and persons. Additionally, these restrictions do not discriminate between collection against different target groups such as: terrorists, narcotics traffickers, weapons trafficker, human traffickers, or nuclear proliferators.<sup>87</sup> For intelligence collection, this research focused solely on roles conducted outside of the United States. Due to the sensitivities and legal ramifications of DoD intelligence collection on US



persons or within the United States, a discussion of that type of collection would be more appropriate in a classified forum. The legality of the proposed DoD intelligence collection and analytical roles was not evaluated as a discriminating factor because this research focused on preexisting DoD intelligence collection and analytical operations, previously directed towards counternarcotics and counterterrorism efforts.

Analysis Roles	Appropriateness	Cost	Lethality	Risk
<i>Intelligence Collection:</i>				
Technical Collection	✓	✓	-	✓
Overt HUMINT	-	-	-	✓
Clandestine HUMINT	-	X	-	X
<i>Analytical Process:</i>				
Analysis	✓	-	-	✓
Collaboration	✓	-	-	✓

*Table 1. Evaluation of DoD roles in Strategic Network Analysis*

## Network Intelligence Collection

**Appropriateness:** Intelligence collection was evaluated according to the two subcategories of HUMINT and technical collection. In relation to intelligence collection on illicit trafficking, the DoD’s current role is a limited role to detect and monitor illicit trafficking.<sup>88</sup> With respect to technical collection, DoD assets are currently being utilized in counter illicit trafficking operations, however the mission here would mean expanding their focus from primarily centered around the illicit actors and products to the actual network. Although mission, focus, and even the assets utilized may have to be adjusted, the overall mission and

goal is very similar to that of current DoD technical intelligence collection operations. The DoD has specialized technical intelligence collection equipment and capabilities that other organizations do not have access to. Some of these technical collection assets and capabilities are highly specialized. Capabilities and resources represented by the NSA, NRO, and military air and space based platforms, are being optimized through DoD employment in support of both military and civilian authorities, vice duplicating these specialized equipment and capabilities in the civilian sector. This is due to the substantial financial investment required for acquisition and sustainment, their limited diversity in functional utility, and because their overall employment most closely aligns with the DoD's operational mission responsibility.<sup>89</sup> Additionally, because of the DoD's unique operational global reach, these assets can more readily be utilized in conjunction with partner nations and assist in building their security and law enforcement situational awareness.<sup>90</sup>

The appropriateness of HUMINT is situationally dependent on the collection environment and collection targets.<sup>91</sup> HUMINT collectors are a scarce resource and extremely valuable to the DoD. The appropriateness of their utilization is directly correlated to the risk incurred by collectors through proposed collection operations. HUMINT operations often operate away from the normal security and protections that normal DoD operations operate in. Risks to HUMINT collectors may come from normal force protection risks and collection operations risks.<sup>92</sup> They include physical harm, and in more sensitive collection, there is a risk of detection or reprisal for collection activity. While DoD HUMINT collectors may have the requisite skills and ability to collect intelligence on any number of target organizations, they should be utilized in a way that adds to the overall mission of the Department. HUMINT collection in unsecure or ungoverned areas, combat

zones, or running sources from terrorist networks are all logical arenas for DoD HUMINT collectors. On the other side of the scale, collection on suspected front companies, financial institutions and political sector nodes of the illicit networks are likely more appropriate for collectors from other members of the intelligence community.

**Cost:** One of the current government challenges that these illicit networks exploit is that they specifically design their operations to avoid government detection by operating in the intelligence gaps of compartmentalized information, collected and maintained within separate government agencies, borders, and jurisdictions.<sup>93</sup> Therefore, the focus of this strategy is not primarily on increasing collection activity across the spectrum of intelligence collection. This strategy primarily looks to focus the full spectrum of government intelligence collection operations to provide information vital to visualizing and targeting the full scope of these networks.<sup>94</sup> Deploying and sustaining DoD assets around the world in order to specifically task them for this type of collection requirement could be a costly endeavor; however, there are already DoD intelligence assets continually deployed all across the globe that could be utilized for collection on illicit trafficking networks. With the DoD already focused on counternarcotics trafficking and terrorist network disruption, many established DoD intelligence operations could be sensitized to illicit trafficking network collection requirements. Doing this would require minimal additional missions, assets, or cost. Sensitizing current collection operations, so that they can capitalize on capturing information that would be useful to illicit trafficking network analysts as they come across in the course of their normal collection operation, would come at little to no financial cost to the DoD. In this way, these collection activities can positively contribute to the overall

development of this information with minimal impact on current intelligence operations' cost and collection asset workload.

**Lethality:** The potential for DoD personnel utilizing lethal force during intelligence collection is very small. Force is generally counterproductive to intelligence collection. The biggest risk is that lethal force would be applied as a force protection measure, however even this risk is very small as intelligence operations are specifically designed to minimize the risk of detection and confrontation during collection.

**Risk:** Technical intelligence incurs minimal risk to DoD forces. However, the risk to HUMINT collectors is highly dependent on the type of collection environment in which they operate.<sup>95</sup> Overt HUMINT collectors under diplomatic status generally provide very minimal risk. However, their ability to gather information that reaches deep into illicit networks may be limited. HUMINT collection that penetrates illicit networks and runs source operations incurs significantly more risk to individual collectors but also may have a better chance of collecting valuable information that is otherwise unattainable. The level of risk involved with HUMINT collection generally directly correlates with the collection activity's ability to penetrate deeper into the organization.<sup>96</sup> There is not a "one size fits all" risk assessment for this, as every collection operation has to be individually assessed. The specific collection operation and intelligence requirements must be assessed in order to determine the appropriate risk level to accept for the given collection requirements.<sup>97</sup> With the exception of the more clandestine HUMINT operations, the risk to DoD assets posed by technical collection and overt HUMINT operations is relatively low. By the nature of

clandestine HUMINT, there are risks that are inherent to its operations. These operations are only performed when the risks can be mitigated and are outweighed by the gain of the targeted intelligence being collected.<sup>98</sup>

## **Analytical Process**

***Appropriateness:*** Due to the link between counternarcotics trafficking, terrorist networks, the broad scope of illicit trafficking networks, and direction from DoD intelligence leadership, it is appropriate for the DoD to play an active role in the analytical process supporting the strategic network focused approach. The DoD currently provides analytical support dedicated to counternarcotics trafficking and terrorist network disruption, but not specifically to the more encompassing threat posed by the illicit trafficking of a variety of items to include narcotics. The threats posed by these decentralized networks trafficking various illicit items are well documented across the globe.<sup>99</sup> Additionally, there is an abundance of intelligence reporting that links Islamic radical terrorist groups with the illicit trafficking of narcotics, weapons, people, narcotics, and materials utilized in the production of weapons of mass destruction.<sup>100</sup> Finally, according to the Defense Intelligence Strategy, DoD participation in intelligence collection and analytical support of efforts to disrupt various illicit networks is not only a focus but also a priority for the Defense Intelligence Community.<sup>101</sup>

Collaboration of classified information across government agencies is a key concept that is an essential ingredient of the analytical process. The collaboration and sharing of information is the only way for separate government agencies, all holding key pieces of the illicit network intelligence puzzle, to put all of the pieces together and visualize the entire network.<sup>102</sup>

One method to accomplish this would be to establish a separate counter illicit trafficking network joint organization, such as the Joint Improvised Explosive Device Defeat Organization (JIEDDO) that focuses on attacking IED networks as one of its three central efforts.<sup>103</sup> JEIDDO is a prime example of effective interagency and international collaboration. On the other hand, one of the differences with IED network disruption and illicit trafficking network disruption is that, IEDs represent a threat that clearly falls in the military's area of primary responsibility. This is not the case with illicit trafficking networks. Although the DoD plays an important role in countering illicit trafficking, its role is clearly a support role.<sup>104</sup>

The Joint Interagency Task Force (JIATF) construct is another possibility for implementation of this role. For example, JIATF-South covers the United States Southern Command's Area Of Responsibility (AOR). It serves as "a model for regional engagement and international and interagency coordination"<sup>105</sup> to manage the DoD's contribution to counterdrug operations in the AOR. JIATF South already oversees collection, analysis, and distribution of counter illicit trafficking intelligence. The current focus of the JIATF is primarily to assist with interdiction efforts, although it has recently begun to expand this scope to also include to a broader spectrum of illicit trafficking and network disruption.<sup>106</sup> Implementing analytical teams at JIATF-South and West, specifically focused on analyzing illicit trafficking network intelligence, bringing DoD intelligence and expertise to this interagency forum, and collaboratively developing strategic network attack targeting solutions, would be an appropriate utilization of DoD assets. This could also be employed at JIATF-West and even deployed as part of contingency JIATF constructs, such as the JIATF-Iraq and the CJIATF-Afghanistan as these needs arise.

The JIATF construct is not the only implementation area where DoD analytical expertise would help U.S. and international efforts against illicit trafficking networks. DoD analyst collaboration at Civil-Military operations centers, such as in Somalia, creates opportunities for civilian and military information collaborations while maintaining Operational Security (OPSEC).<sup>107</sup> Fusion Centers such as those in Afghanistan, Mexico, and Colombia also provide international and interagency also provide appropriate forums to implement this type of analytical collaboration, as these locations are already active in similar activities.<sup>108</sup>

**Cost:** The cost associated with the DoD establishing an active role in the analytical intelligence process of compiling information, visualization, and targeting illicit trafficking networks is largely dependent on the level at which the department allocates assets toward this mission. More than any other factor, the success of government efforts to defeat decentralized illicit networks relies on wide spread analytical intelligence collaboration across the full spectrum of government intelligence assets at the local, tribal, state, national, and international levels.<sup>109</sup>

Many of the most appropriate entities for this function could perform this analysis at some level with existing personnel; however, adding this would likely impact their ability to perform the high demand functions that they are already performing. Costs associated with the analytical process are primarily associated with adding analytical personnel to already existing analytical entities. The DoD could also capitalize on virtual collaboration through efforts such as the Law-enforcement Information Exchange (LInX),<sup>110</sup> which provides

worldwide law enforcement collaboration tools, and the Maritime Safety and Security Information System, which was developed to help track sea vessels.<sup>111</sup>

Implementation across currently existing counternarcotics and counterterrorism intelligence efforts would be very cost effective, due to the increasingly overlapping spheres of operations of terrorist, narcotics trafficking, and various other illicit trafficking networks. Additionally, even if DoD collection assets continued to collect the same intelligence that they are currently collecting, an increase in collaboration from the analytical intelligence community would considerably contribute to this overall effort. If analysts utilize the network visualization tools to process network intelligence, it will facilitate production and utilization of analytical products that serve as the basis for strategic attacks against the illicit networks of both terrorists and illicit traffickers.

***Lethality:*** There are no concerns of possible utilization of lethal force during the intelligence centered analytical process.

***Risk:*** DoD members are not placed in harm's way during the analytical process. Analysts generally perform their work at secure locations inside a Sensitive Compartmented Information Facility (SCIF) to protect the integrity of the information.

## **DoD roles in Strategic Network Attack**

Strategic Network Attack is the operational offensive portion of the Strategic Network Focused Strategy. This evaluation focuses on attacks that target the three critical elements of network organizations: resources, functions, and processes. Network resources are critical requirements of networked systems, commonly referred to as network nodes. Functions are



critical capabilities of the networked systems, representing the roles and specific purposes of individual network nodes or resources.<sup>112</sup> Individual nodes may be very valuable to the network and individually targeted. On the other hand, when considering long-term destabilization of the network, it is often more disruptive to target attacks on multiple nodes with similar function. Simultaneous attacks that effectively disable critical network functions may be more disruptive than removing single key nodes.<sup>113</sup> Network processes are the actions that serve as the basis for network connections and critical linkages that form the decentralized structure of the overall network system.<sup>114</sup> Attacks that target the nodes and functions of the network may utilize the same resources and strategic approach as those that target the connections of the network. There are two principle differences between the two types of attacks. The first focuses on attacks that induce network wide disruption of the parts and functions of the network. The second specifically focuses attacks on the cohesiveness of the networks themselves, their ability to connect the individual parts, and move operations across the network.

Network resources are the nodes of the network consisting of people, key leadership, organizations, or locations. Network resource attack activities can take various forms. Some attacks target individual nodes to induce them to react in order to further assess the nodes function and adaptability. Other actions direct conduct electronic attacks on financial or communications nodes. Others target specific nodes for removal from the network. Although individual nodes may be singularly targeted, it is often more strategically effective to attack multiple nodes in parallel across the network and induce long term disruption of the network by depriving it of the targeted functions or critical capabilities.

Network processes are the actions or operations that serve as the basis for the connections that form between network resources. These processes serve as the critical linkages that form the

decentralized structure of the overall network system.<sup>115</sup> Network connections are attacked with the goal of degrading the integrity of the bonds of the network, causing wide spread isolation of nodes across the network and disrupting its ability to function as a cohesive network. Linkages between illicit trafficking nodes are primarily formed according to the operational function of network nodes. However, even operational linkages are often formed and strengthened by shared ideology, relationship, communication, and the transfer of illicit products and finances. All of these factors must be understood by targeting analysts in order to pick the most critical linkages for the targeted network and design attacks that disrupt those network connections. This type of attack may be accomplished by strategically targeting communication, transportation, and movement of products, across network lines. It may also be accomplished by attacking the relationships that connect the nodes by using psychological operations (PSYOPs), information warfare, and social network virus attacks. Targeting financial resources, such as with counterthreat finance operations, is another way to accomplish the same objective. Operations that target finances have the potential to affect the network's connections by removing or freezing financial resources. These connections may also be impaired by manipulating them in such a way that causes a mistrust or discord across the network. Another type of network linkage attack is accomplished by strategically targeting the communication, transportation, and movement of products, across specifically targeted network lines in order to isolate the targeted portion of the network.

Attack Roles	Appropriateness	Cost	Lethality	Risk
Information Warfare	✓	-	-	-
PSYOPs	✓	-	-	-
Viral Network Attack	✓	-	-	-
Kinetic Operation	✗	-	✗	✗
Arrest/Removal	✗	-	✗	✗
Electronic Attack	✓	✓	-	-
Counterthreat Finance	✓	✓	-	-

*Table 2. Evaluation of DoD roles in Strategic Network Attack*

## Strategic Network Attack Roles

**Appropriateness:** Although illicit trafficking networks clearly pose economic, political, and security threats the effort to attack illicit trafficking network nodes is primarily a function of law enforcement vice military, especially when the attacks are directed towards physical entities. Military capabilities provide critical communications and situational awareness to law enforcement officials carrying out physical attacks. Depending on the scope of electronic attacks, these may require specialized equipment and expertise that is most appropriate for the military to perform. Direct utilization of military assets to perform attack should be evaluated on a case-by-case basis. As the targets of networks attack reach closer into terrorist or combative networks, as well as in areas where the physical combat or security environment dictates greater military cooperation, it becomes more appropriate for military forces to play a more prominent part in this role. The overall lead for this role rests in the law enforcement arena.

Of the network attacks evaluated, kinetic operations and node removal or arrest raise the biggest issue for appropriateness of utilizing military forces, as they require physical force application. Narcotics trafficking networks are one of the many types of illicit networks involved in illicit trafficking across the globe. Evaluating this role using current military use of force guidelines for operations targeting illicit narcotics trafficking; the appropriateness of kinetic military force application by DoD to capture, arrest, and possibly use of deadly force all is not generally supported.<sup>116</sup> The most notable exception is in areas where the DoD already has an established military force due to another already existing DoD mission, such as Afghanistan. Due to current military operations and a challenging security situations, the military is appropriate in such areas. In fact, in August of 2009 there were 50 illicit drug traffickers, linked to financing terrorists, officially being targeted by military forces in Afghanistan.<sup>117</sup>

**Cost:** The vast majority of network resource attacks do not require military force application. Even when kinetic offensive assets are required for network resource attack, host-nation military forces and law enforcement are the primary assets. Thus, the cost of physical offensive DoD assets would be minimized by their limited utilization in the strategy. DoD ISR and command and control resources may be utilized and, depending on the assets utilized, this would be the biggest possible cost to the DoD. Electronics attacks could be carried out or coordinated remotely and thus, the primary cost would be measured in man hours dedicated to this task vice additional dollars spent on it. Other costs would depend on how PSYOPs, information warfare, and communications attacks are conducted. Depending on the specifics of the targeted network, local and host-nations capabilities, and

operational design, these operations could be directed remotely, or with teams deployed to assist these operations. Operations such as counterthreat finance, could be accomplished by DoD specialists already performing that function with little additional cost.

***Lethality:*** The possibility of DoD members utilizing lethal force while contributing to these attacks is very low. In areas where DoD forces are already performing security or combat operations, military force may likely be the most appropriate means to remove critical resources from a network, especially if the node of the targeted network was also part of a combatant or terrorist group. However, the majority of illicit trafficking network resources do not fall into this category. When it comes to illicit trafficking networks, the DoD plays a supporting role.<sup>118</sup> In that context, forceful network removal or arrest would primarily be a function of local law enforcement or security forces. Additionally, targeted resources are valuable to network analysis after networks attacks are complete. These resources may serve as future sources of intelligence on the network's operations. Although resources are the critical requirements of the networks, the overall strategy focuses on attacks that affect the network itself and the cumulative threat posed by it, rather than on the individual resources and nodes that comprise it. Network connection attacks are the least likely to apply force to physical objects. Furthermore, during actions that do apply physical force, DoD members are more likely to assist local and host-nation law enforcement or military forces, provide planning support, and utilize assets that increase situational awareness instead of applying direct force. The exception, as described above, would be an attack against network entities operating inside a military designated combat area where DoD forces are

present as part of a larger operation. In this case use of force would be evaluated in the context of the larger operation.

**Risk:** This role does not significantly increase the risk incurred by DoD assets. Even for DoD assets that are utilized in this role in a combat area, or as part of a security operation, the risks associated with performing this type of action should not significantly increase the risks incurred as part of the larger operation. Outside of combat operation environments, any physical force operation is more appropriate for law enforcement and therefore the risk to DoD assets is not significantly greater than standard force protection risks for their normal operations basing areas.

## Notes

- 
- <sup>82</sup> Interagency OPSEC Support Staff, *Intelligence Threat Handbook*, 67.
- <sup>83</sup> Interagency OPSEC Support Staff, *Intelligence Collection Activities and Disciplines*.
- <sup>84</sup> Innocenti et al., *Direct Support HUMINT in Operation Iraqi Freedom*, 48.
- <sup>85</sup> Interagency OPSEC Support Staff, *Intelligence Threat Handbook*, 67.
- <sup>86</sup> Interagency OPSEC Support Staff, *Intelligence Collection Activities and Disciplines*.
- <sup>87</sup> United States Congress, *18 USC Chapter 67*.
- <sup>88</sup> Gates, *Remarks at the Halifax International Security Forum*.
- <sup>89</sup> Weschler, *Senate Testimony May 2010*, 1-3.
- <sup>90</sup> Fraser, *2010 SOUETHCOM Posture Statement*, 8-16.
- <sup>91</sup> U.S. Army, *FM 2-22.3 Ch. 3*.
- <sup>92</sup> *Ibid.*
- <sup>93</sup> Williams, *Strategy for a New World*, 206.
- <sup>94</sup> Cheatham, *A Strategy to Destabilize Drug Trafficking Networks*, 1.
- <sup>95</sup> U.S. Army, *FM 2-22.3 Ch. 3*.
- <sup>96</sup> *Ibid.*
- <sup>97</sup> *Ibid.*
- <sup>98</sup> Nitze, *Navy clandestine intelligence collection program*, 1-5.
- <sup>99</sup> Geneva Centre for Security Policy, *A Comprehensive Approach to Combating Illicit Trafficking*, ix-xx.
- <sup>100</sup> Weschler, *Senate Testimony May 2010*, 1-3.
- <sup>101</sup> Department of Defense 2008, *Defense Intelligence Strategy*, 10.
- <sup>102</sup> Geneva Centre for Security Policy, *A Comprehensive Approach to Combating Illicit Trafficking*, 49.
- <sup>103</sup> JIEDDO, *The Joint IED Defeat Organization*.
- <sup>104</sup> Frothingham, *Tracking and Disrupting Terrorist Financial Networks*, 2.
- <sup>105</sup> Fraser, *2010 SOUETHCOM Posture Statement*, 16.

- 
- <sup>106</sup> Weschler, *Senate Testimony May 2010*, 6.
- <sup>107</sup> Joint Irregular Warfare Center, *Joint Irregular Warfare 2010 Analyst Review*, 23.
- <sup>108</sup> Leonhart, *House Testimony March 2009*, 2-8.
- <sup>109</sup> Geneva Centre for Security Policy, *A Comprehensive Approach to Combating Illicit Trafficking*, 49.
- <sup>110</sup> Haines, *LInX - Law Enforcement Information Exchange*.
- <sup>111</sup> Geneva Centre for Security Policy, *A Comprehensive Approach to Combating Illicit Trafficking*, 39.
- <sup>112</sup> Chairman of the Joint Chiefs of Staff, *National Military Strategic Plan for the War on Terrorism*, 14.
- <sup>113</sup> USAF, *Air Force Doctrine Document 2-1.2.*, 9.
- <sup>114</sup> Chairman of the Joint Chiefs of Staff, *National Military Strategic Plan for the War on Terrorism*, 14.
- <sup>115</sup> *Ibid.*, 14.
- <sup>116</sup> Chairman of the Joint Chiefs of Staff, DoD Counterdrug Support; Chairman of the Joint Chiefs of Staff, DoD Rule on Use of Force in Support of law Enforcement.
- <sup>117</sup> Senate Committee on Foreign Relations, *Afghanistan's Narco War*, 2-8.
- <sup>118</sup> Frothingham, *Tracking and Disrupting Terrorist Financial Networks*, 2.

## Conclusion

Today some of the DoD's biggest threats are not conventional military threats but are posed by various non-state actors. The more that these non-state actors can collaborate, combine and coordinate their actions, the more potential they have to be a threat to the national security and sovereignty of nation states across the globe.<sup>119</sup> These threats often surface far away from combat zones and sometime preclude the utilization of traditional military force.<sup>120</sup> The adaptability and dispersion of these threats amongst law abiding citizens demands that a whole of government approach be applied in order to address them.<sup>121</sup> Illicit trafficking has become one of these emergent national security threats and should be addressed by the Department of Defense. The Joint Combatant Commander of United States Southern Command, General Fraser has repeatedly characterized illicit trafficking as the biggest security challenge in the Western Hemisphere.<sup>122</sup> The Deputy Secretary of Defense for Counternarcotics and Global Threats, William Weschler, testified to Congress in May of 2010 that illicit trafficking had clear connections to Islamic radical terrorist groups and represents "a present and growing danger to the security of the United States, our forces abroad, and our allies." In his 2010 National Security Strategy, President Barack Obama called for a multidisciplinary approach that "enlists all of our intelligence, law enforcement, and homeland security capabilities."<sup>123</sup> All of the United States instruments of power must be brought to bear on this ever-increasing threat to national security. Ten years ago, many in the DoD thought of illicit trafficking as well outside of the scope of the U.S. military's area of responsibility.<sup>124</sup> Today, illicit trafficking networks have been recognized by the department's leadership as a national security threat and that the DoD should be included as an integral part in defeating this threat.



The strategic network focused strategy considered here is a long-term approach aimed at disrupting illicit trafficking networks. Although it is not an intelligence process, it is driven by intelligence in order to conduct network analysis, with the goal of targeting networks of illicit actors. The goal of the strategy is to disrupt the operations and unity of illicit trafficking networks. Illicit trafficking networks pose serious threats to national security in the United States and across the globe. The goal of disrupting the networks aims to neutralize this threat by attacking the unity of the network by isolating it to its separate parts, or by weakening the operational cohesiveness of the network. The desired end state is to separate illicit actors so that their collective threat is neutralized. This allows them to be contained as local threats manageable to law enforcement.

This research evaluated the overall strategy in three parts. It evaluated intelligence collection, analytical process and networks attacks utilizing the criteria of appropriateness, cost, legality, lethality, and risk. The overall appropriateness of the Department of Defense taking an active role in disrupting illicit trafficking networks is one of the most important discriminating factors of this evaluation. As the DoD plays an overall support role in counter illicit trafficking, the appropriateness of utilizing DoD assets must be determined before the DoD spends time and money investing in utilization. There is currently a high level of interest from within DoD towards disrupting illicit trafficking networks; however, most of the focus of this interest is on utilizing existing DoD efforts in counternarcotics and counterterrorism as the basis for developing DoD response to the interconnected problem of these two areas within illicit trafficking networks.<sup>125</sup> There was a time when these were thought of as separate disciplines and in many respects they still are. Today, networks that are formed between terrorist and narcotics traffickers have become intertwined with one another and with other illicit trafficking as well.

FARC insurgents in Colombia smuggle cocaine to terrorist groups in Africa utilizing human traffickers and receive payment in small arms smuggled back into Colombia.<sup>126</sup> Terrorist groups from the Middle East exploit illicit trafficking nodes in Central America in order to use them to funnel personnel and materials north for attacks on the United States.<sup>127</sup> Drug traffickers in Afghanistan harbor terrorists, finance their operations, and link with traffickers that move vacuum parts utilized in illicit nuclear proliferation trafficking.<sup>128</sup> In fact, in Afghanistan illicit traffickers are so intertwined with terrorists that some have officially been declared military targets alongside terrorists and insurgents and are pursued by military forces operating there.<sup>129</sup>

There were three roles that raised issues with appropriateness: human intelligence collection, kinetic operations, and node removal or arrest. The appropriateness of HUMINT is difficult to thoroughly evaluate in an open source forum. In general terms, the appropriateness of HUMINT collection is situationally dependent on the collection environment and collection targets.<sup>130</sup> In areas where the DoD already has an established military force due to another already existing DoD mission, the full spectrum of DoD HUMINT collection may be the most appropriate asset to utilize. In other environments, and when collection is more geared toward civilian or business sectors, DoD HUMINT is much less appropriate. Although illicit trafficking networks are not currently a focus for the defense intelligence community, it overlaps current focus areas and is mentioned as such in the Defense Intelligence Strategy alongside narcotics trafficking and terrorist networks.<sup>131</sup> If the DoD intelligence community is to dedicate HUMINT resources to specifically target this threat, it needs to develop the parameters for determining the most appropriate targets, along with the acceptable level of risk for collection operations. The appropriateness of kinetic military force application and DoD assets involved in physically removing nodes from their network through capture, arrest, and possible use of deadly force is

only appropriate in a limited context, such as in Afghanistan.<sup>132</sup> In other operational environments, local law enforcement and security forces are the most appropriate means to apply force. This does not rule out DoD involvement in these operations. DoD assets can apply their unique skills and experience to targeting, planning, communications, and contribute to situational awareness during operations.

In a resource constrained environment cost is a significant factor for the department, possibly limiting the scale of implementation. Across the board of possibilities, the cost of DoD implementation would be highly dependent on the level at which the DoD decides to directly allocate assets towards this endeavor. In order to maximize the effect of the network disruption, there needs to be a concerted effort to maintain a focus that goes beyond interdiction and targets these networks at the strategic level. While the DoD is primarily a supporting entity in the overall strategy, the department could implement changes to collection and analysis utilizing assets currently deployed around the world, with little to no additional cost. These assets could continue to pursue counternarcotics and counterterrorism operations with minimal changes to current operational missions.<sup>133</sup> Collection efforts can be sensitized to illicit trafficking intelligence gaps. Counterterrorism analysts can develop visualizations that further the understanding on these networks and the linkages they share with terrorist networks, while also assessing their strengths and vulnerabilities. They could collaborate across the intelligence and law enforcement communities to help all involved government parties build better pictures on all forms of illicit trafficking networks, to include narcotics and terrorist networks. As terrorist and trafficking are inextricably linked,<sup>134</sup> DoD targeting analysts, currently working on attacking the terrorist networks, can help target and provide direction on attacks on illicit trafficking networks.<sup>135</sup> Informally this has already begun to happen in Afghanistan, where DoD

intelligence process is identifying illicit trafficking targets linked to terrorism and targeting them; military forces work with local security forces to neutralize these illicit trafficking targets.<sup>136</sup> Although the financial cost of formally implementing this across DoD would represent minimal additional costs to the DoD, the workload increase would be minimal. These operations run parallel, intersect and even contribute to current operations. The other end of this scale would be to add additional personnel to specifically perform this task. The cost of this would be determined by the amount of assets that DoD dedicates to this. Aside from the normal DoD budget, there is congressional money set aside to assist the DoD with both counternarcotics and counterterrorism requirements, such as the DoD Counternarcotics Central Transfer Account established by the FY 1988 National Defense Authorization Act.<sup>137</sup> These funds are provided in order to allow the DoD the flexibility to support emergent and contingency requirements in these areas. To the extent that illicit trafficking connects with illicit narcotics and terrorism it may be possible to utilize counternarcotics and counterterrorism funding to pursue these requirements; however, in order to succeed this needs to be programmed into the DoD long-term budget. The problem of illicit trafficking has grown to global proportions and governments will have to invest both unilaterally and collaboratively in resolving this problem in order to disrupt the unity of these networks and counter the threats that they pose.<sup>138</sup>

This research recognizes the importance of legal restrictions on DoD operations against illicit trafficking. The majority of these restrictions arise when DoD operations are conducted in the United States and against U.S. persons. There are many legal provisions for DoD assets to successfully navigate these challenges. In order to limit the scope this research only examined implementation that fell into previously established operational DoD roles in counterterrorism and counternarcotics. There is no difference in the legal protection offered to illicit actors of

terrorism, narcotics trafficking, or other illicit trafficking operations, which in the case of counternarcotics is no difference at all.<sup>139</sup> Therefore, the only fundamental legal difference between the DoD roles described in this research and previously established legal counternarcotics and counterterrorism roles is the type of illicit activity that the targeted individuals are involved in.

Lethality and risk were not found to be particularly discriminating in evaluating the various roles. They were primarily a factor in the evaluated roles conducted in the context of a larger combat or security operation. In those cases, the lethality and risk of the missions supporting this strategy would be determined in the larger frame of reference of the combat operation, such as the case currently in Afghanistan.<sup>140</sup> As the DoD primarily plays a supporting role in counter illicit trafficking, local law enforcement and security personnel are the most appropriate entities to apply physical force and apart from the noted exception lethality and risk were not factors.

In light of the this evaluation, having the DoD as a full partner in both network analysis and strategic attack would positively advance the effectiveness of the U.S. government's overall effort at strategically disrupting illicit trafficking networks. Even though the DoD plays a support role to the overall effort of illicit trafficking, due to the increasingly inextricable relationship between current DoD efforts in counternarcotics trafficking and counterterrorism this also has vast potential to be conducted in a way that advances primary DoD missions. Involving the DoD intelligence community in network analysis advances the overall picture of all participants in the full spectrum of illicit trafficking and terrorist networks, but also follows the direction of DoD Intelligence Community guidance which sets this type of collaboration across the entire intelligence community and law enforcement as a priority and focus.<sup>141</sup> With

regard to strategic network attack the DoD is able to offer a wealth of experience in planning and assisting others to plan offensive strategic operations. However, this part of the overall strategy is still developing and is currently much more of an academic concept than an operational reality. As this develops the DoD should be an active partner in contributing its unique perspective and experience conducting similar operations against illicit trafficking in Afghanistan.<sup>142</sup>

## Note

---

<sup>119</sup> Naim, *Illicit*, 6-8.

<sup>120</sup> Fraser, *2010 SOUETHCOM Posture Statement*, 6-14.

<sup>121</sup> Fridovich, *Tracking and Disrupting Terrorist Financial Networks*, 2.

<sup>122</sup> Appin, *Statement by General Fraser April 2010*.

<sup>123</sup> Obama, *Natinal Security Strategy*, 20,49.

<sup>124</sup> Fridovich, *Tracking and Disrupting Terrorist Financial Networks*, 2.

<sup>125</sup> Weschler, *Senate Testimony May 2010*, 1-3.

<sup>126</sup> Pham, *Emerging West African Terror-Drug Nexus*.

<sup>127</sup> Department of State, *Country Reports on Terrorism 2009*.

<sup>128</sup> Shelly, *Growing Together*, 1-2.

<sup>129</sup> Senate Committee on Foreign Relations, *Afghanistan's Narco War*, 1.

<sup>130</sup> U.S. Army, *FM 2-22.3 Ch. 3*.

<sup>131</sup> Department of Defense 2008, *Defense Intelligence Strategy*, 10.

<sup>132</sup> Chairman of the Joint Chiefs of Staff, *DoD Counterdrug Support*.

<sup>133</sup> Frothingham, *Tracking and Disrupting Terrorist Financial Networks*, 4.

<sup>134</sup> Williams, *Strategy for a New World*, 206.

<sup>135</sup> JIEDDO, *The Joint IED Defeat Organization*

<sup>136</sup> Senate Committee on Foreign Relations, *Afghanistan's Narco War*, 1.

<sup>137</sup> Weschler, *Senate Testimony May 2010*, 4.

<sup>138</sup> Geneva Centre for Security Policy, *A Comprehensive Approach to Combating Illicit Trafficking*, 75.

<sup>139</sup> United States Congress, *18 USC Chapter 67*.

<sup>140</sup> Fridovich, *Tracking and Disrupting Terrorist Financial Networks*, 1.

<sup>141</sup> Department of Defense 2008, *Defense Intelligence Strategy*, 10.

<sup>142</sup> Senate Committee on Foreign Relations, *Afghanistan's Narco War*, 13.

## Recommendations

One of the challenges faced in defining DoD roles in this strategy is that much of it is not yet fully a reality but more of a concept developed and being implemented at various levels across the U.S. government. It has only been in the past few years that the threats posed by illicit trafficking networks have gone from an academic concept to one that is acknowledged by nations across the globe, and even more recently that DoD leaders have publicly acknowledged this as a threat that pertains to DoD.<sup>143</sup> Therefore the U.S. Strategy for defeating illicit trafficking networks will continue to change and evolve as the government organizes its efforts and continually adapts to the dynamically changing tactics that these networks employ to counteract government intervention. Based on a thorough examination of the problem of illicit trafficking and the strategic network focused approach, this research makes the following recommendations:

### **DoD needs to be a full and active partner in this strategy.**

In order effectively answer the threats posed by these networks the DoD should continue to be a full and active partner in this strategy. In order to defeat this threat it will take a cooperative effort on the part of the intelligence community, law enforcement, military, policy makers, US interagency, coalition partners, and other nations across the globe.<sup>144</sup> This pertains as much to congressional and national policy makers as it does to the Department of Defense. The DoD needs funding from congress and strategic direction from policy makers and from lead agencies from the Departments of Homeland Security, State, and Justice. The DoD has various capabilities and assets that are unique to the department that are extremely valuable in the overall effort of disrupting illicit trafficking networks.<sup>145</sup> Although the department plays a supporting

role in this effort their niche role is indispensable to its success. Additionally with the connectedness that these networks have with terrorism, this effort also positively contributes to the DoD's ability to accomplish missions that are its primary responsibility.<sup>146</sup>

### **Integrate strategic network analysis into current DoD intelligence community.**

The DoD is focused on the emerging threat of illicit trafficking networks and committed to increasing its collaboration with the interagency effort to answer this threat.<sup>147</sup> With its connections to both terrorism and illicit narcotics trafficking, integrating this strategic focus into the current DoD intelligence community could positively contribute to the departments stated goals of increasing collaboration along this front, while also furthering its own primary intelligence mission.<sup>148</sup> Currently, established DoD intelligence operations could be sensitized to illicit trafficking network collection requirements. This will allow them to capitalize on capturing information that would be useful to illicit trafficking network analysts as they come across this type of intelligence in the course of their normal collection operations. Analysts can collaborate across the interagency to both share information that would help other intelligence community members build network visualization as well as seek out information from interagency partners to facilitate visualization of terrorist and narcotics trafficking networks.<sup>149</sup>

### **Investigate the integration of strategic network analysis into JIATF structure.**

Narcotics trafficking is one portion of the overall spectrum of illicit trafficking. With the successes that the JIATF structures have had in its counternarcotics trafficking efforts this is a good place to begin developing the analytical process of strategic network analysis. JIATFs already have the J2 structure in place to accommodate the kind of strategic intelligence that is



needed to develop network visualizations. The DoD should investigate the possibility of integrating illicit trafficking analysts who could utilize much of the information that the JIATFs already process and also help focus illicit trafficking collection requirements to fill network gaps in their areas of responsibility.

### **Work with interagency community to develop Strategic Network Attack.**

While the whole strategy is still developing, at the unclassified level, Strategic attack is much more of an academic concept than an operational reality. The Joint Improvised Explosive Device Defeat Organization is one organization within the DoD that is specifically attacking illicit networks for disruption.<sup>150</sup> Additionally, the DoD is currently pursuing illicit traffickers connected with terrorist networks in Afghanistan.<sup>151</sup> The DoD can utilize this developing expertise and collaboration with the interagency community that is developing this strategy in order to study these networks, design and execute attacks, and evaluate the effects on them to build operational understanding of how to further the overall strategy.<sup>152</sup>

### **Notes:**

---

<sup>143</sup> Luna, *Dynamic Threat Mitigation*.

<sup>144</sup> Fridovich, *Tracking and Disrupting Terrorist Financial Networks*, 1.

<sup>145</sup> Weschler, *Senate Testimony May 2010*, 4.

<sup>146</sup> *Ibid.*, 1.

<sup>147</sup> Pendleton, *House testimony July 2008*, 1.

<sup>148</sup> *Ibid.*, 10.

<sup>149</sup> Cheatham, *A Strategy to Destabilize Drug Trafficking Networks*, 1.

<sup>150</sup> JIEDDO, *The Joint IED Defeat Organization*.

<sup>151</sup> Senate Committee on Foreign Relations, *Afghanistan's Narco War*, 13.

<sup>152</sup> Williams, *Strategy for a New World*, 202-206.

## Bibliography

- Appin, Robert. *United States Southern Command*. 15 April 2010.  
<http://www.southcom.mil/appssc/news.php?storyId=2296> (accessed 10 July 2010).
- Arquilla, John, and David Ronfeldt. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, Ca: RAND Corporation, 2001.
- Bergin, Sean. "Social Network Analysis of 'Dark Networks': Where are we now?" *University of Wollongong, Melbourne Australia*. Dec 2009.  
<http://ctcp.uow.edu.au/content/groups/public/@web/@law/@ctcp/documents/doc/uow072215.pdf> (accessed 16 July 2010).
- Best, Richard A., Jr. *Intelligence Community Reorganization: Potential Effects on DOD Intelligence Agencies*. CRS Report for Congress. 21 December 2004.  
<http://www.fas.org/irp/crs/RL32515.pdf> (accessed 30 July 2010).
- Bush, George H.W. "National Drug Control Strategy 1991." *National Criminal Justice Reference Service (NCJRS)*. February 1991.  
<http://www.ncjrs.gov/pdffiles1/ondcp/128897.pdf> (accessed 10 July 2010).
- Bush, George W. "National Drug Control Strategy 2008 Annual Report." *The White House Office of National Drug Control Policy (ONDCP)*. 2008.  
<http://www.ncjrs.gov/pdffiles1/ondcp/221371.pdf> (accessed 20 July 2010).
- Center for Strategic and International Studies. *PONI 2010 Spring Conference*. 2 April 2010.  
[http://csis.org/files/attachments/100402\\_Abstracts.PDF](http://csis.org/files/attachments/100402_Abstracts.PDF) (accessed 8 July 2010).
- Chairman of the Joint Chiefs of Staff. "DoD Counterdrug Support." *Defense Technical Information Center*. 28 January 2008.  
[http://www.dtic.mil/cjcs\\_directives/cdata/unlimit/3710\\_01.pdf](http://www.dtic.mil/cjcs_directives/cdata/unlimit/3710_01.pdf) (accessed 10 August 2010).
- Chairman of the Joint Chiefs of Staff. "Joint Operation Publication 3-0." *The Defense Technical Information Center (DTIC)*. 22 March 2010.  
[http://www.dtic.mil/doctrine/new\\_pubs/jp3\\_0.pdf](http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf) (accessed 20 July 2010).
- Chairman of the Joint Chiefs of Staff. "Joint Publication 3-07.4 Joint Counterdrug Operations." *Federation of American Scientists*. 13 June 2007. <http://www.fas.org/irp/doddir/dod/jp3-07-4.pdf> (accessed 20 August 2010).
- Chairman of the Joint Chiefs of Staff. "National Military Strategic Plan for the War on Terrorism." *US Army Strategic Studies Institute*. 1 February 2006.  
<http://www.strategicstudiesinstitute.army.mil/pdffiles/gwot.pdf> (accessed 24 July 2010).

- Chairman of the Joint Chiefs of Staff. "RULES ON THE USE OF FORCE BY DOD PERSONNEL PROVIDING SUPPORT TO LAW ENFORCEMENT AGENCIES CONDUCTING COUNTERDRUG OPERATIONS IN THE UNITED STATES." *Defense Technical Information Center*. 31 May 2000. [http://www.dtic.mil/doctrine/jel/cjcsd/cjcsi/3121\\_02.pdf](http://www.dtic.mil/doctrine/jel/cjcsd/cjcsi/3121_02.pdf) (accessed 10 August 2010).
- Cheatham, David. *A Strategy to Destabilize Drug Trafficking Networks*. working Paper, Washington DC: White House Office of Drug Control Policy, 2008.
- Congress, United States. "10 USC CHAPTER 15 - INSURRECTION." *U.S. Code*. 1 February 2010. <http://uscode.house.gov/download/pls/10C15.txt> (accessed 20 July 2010).
- Craddick-Adams, Peter. *The Home Front in World War One*. 14 March 2005. [http://www.bbc.co.uk/history/trail/wars\\_conflict/home\\_front/the\\_home\\_front\\_12.shtml](http://www.bbc.co.uk/history/trail/wars_conflict/home_front/the_home_front_12.shtml) (accessed 10 August 2010).
- Department of Defense. "Defense Intelligence Strategy." *Air War College Gateway to the Internet*. 2008. [http://www.au.af.mil/au/awc/awcgate/dod/def\\_intell\\_strat\\_080501.pdf](http://www.au.af.mil/au/awc/awcgate/dod/def_intell_strat_080501.pdf) (accessed 30 July 2010).
- Department of Defense. "DOD Directive 5525.5 DoD Cooperation with Civilian Law Enforcement Officials." *OSD Policy*. 20 December 1989. [http://policy.defense.gov/sections/policy\\_offices/hd/references/directives\\_instructions/index.html](http://policy.defense.gov/sections/policy_offices/hd/references/directives_instructions/index.html) (accessed 22 July 2010).
- Department of Defense. "Military Assistance to Civil Authorities." *The Defense Technical Information Center (DTIC)*. 18 February 1997. <http://www.dtic.mil/whs/directives/corres/pdf/302515p.pdf> (accessed 10 July 2010).
- Department of Defense. "Strategy for Homeland Defense and Civil Support and Civil Support." *U.S. Department of Defense*. 30 June 2005. <http://www.defense.gov/news/Jun2005/d20050630homeland.pdf> (accessed 1 August 2010).
- Department of State. "Country Reports on Terrorism 2009." *U.S. Department of State*. 5 August 2010. <http://www.state.gov/s/ct/rls/crt/2009/index.htm> (accessed 9 August 2010).
- Department of State. *Current List of Designated Foreign Terrorist Organizations*. 19 January 2010. <http://www.state.gov/s/ct/rls/other/des/123085.htm> (accessed 8 July 2010).
- Department of State. "Trans-Pacific Symposium on Dismantling Transnational Illicit Networks." *U.S. Department of State*. February 2010. <http://www.state.gov/documents/organization/137524.pdf> (accessed 9 July 2010).
- Doyle, Charles, and Jennifer Elsea. "Terrorism: Some Legal Restrictions on Military Assistance to Domestic Authorities Following a Terrorist Attack." *CRS Report for Congress*. 27 May 2005. <http://www.fas.org/sgp/crs/natsec/RS21012.pdf> (accessed 20 July 2010).

- Eilstrup-Sangiovanni, Mette, and Calvert Jones. "Assessing the Dangers of Illicit Networks: Why al-Qaida May Be Less Threatening Than Many Think." *International Security* 33, no. 2 (Fall 2008): 7-44.
- Fraser, Douglas M, General. "2010 POSTURE STATEMENT OF GENERAL DOUGLAS M. FRASER." *UNITED STATES SOUTHERN COMMAND*. 11 March 2010. <http://www.southcom.mil/AppsSC/files/634038960550937500.pdf> (accessed 17 July 2010).
- Fridovich, David P. *Tracking and Disrupting Terrorist Financial Networks: A potential model for Inter-agency success?* 11 March 2009. [http://armedservices.house.gov/pdfs/TUTC031109/Fridovich\\_Testimony031109.pdf](http://armedservices.house.gov/pdfs/TUTC031109/Fridovich_Testimony031109.pdf) (accessed 10 July 2010).
- Friedkin, Noah E. "Social influence network theory: Toward a science of strategic modification of interpersonal influence systems." *The National Academic Press*. 2003. <http://www.nap.edu/openbook.php?isbn=0309089522&page=89> (accessed 17 July 2010).
- Frothingham, Edward III. *Tracking and Disrupting Terrorist Financial Networks: A potential model for Inter-agency success?* 11 March 2009. [http://armedservices.house.gov/pdfs/TUTC031109/Frothingham\\_Testimony031109.pdf](http://armedservices.house.gov/pdfs/TUTC031109/Frothingham_Testimony031109.pdf) (accessed 10 July 2010).
- Gates, Robert M. "Secretary Gates Remarks at the Halifax International Security Forum, Halifax, Nova Scotia." *U.S. Department of Defense*. 20 November 2009. <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4518> (accessed 7 Aug 2010).
- Geneva Centre for Security Policy (GCSP). "A Comprehensive Approach to Combating Illicit Trafficking." *Institute for Foreign Policy Analysis*. June 2010. <http://www.ifpa.org/pdf/IFPA-GCSPTraffickingReport.pdf> (accessed 10 July 2010).
- Greenhil, Jim. "National Guard troops to deploy to U.S.-Mexico Border." *U.S. Army*. 19 July 2010. <http://www.army.mil/-news/2010/07/19/42515-national-guard-troops-to-deploy-to-us-mexico-border/> (accessed 16 August 2010).
- Haines, Keith. *LInX - Law Enforcement Information Exchange*. 2007. <http://www.najis.org/Presentations/NAJIS%20Presentations%202006/20%20LInX%20-%20Keith%20Hannes.ppt> (accessed 11 August 2010).
- Innocenti, Charles W., Ted L. Martens, and Daniel E. Soller. "Direct Support HUMINT in Operation Iraqi Freedom." *MILITARY REVIEW*. June 2009. [http://www.oss.net/dynamaster/file\\_archive/100118/8e758ff9625cada83204dd01b3bf810b/2010-01-18%20HUMINT%20in%20Iraq.pdf](http://www.oss.net/dynamaster/file_archive/100118/8e758ff9625cada83204dd01b3bf810b/2010-01-18%20HUMINT%20in%20Iraq.pdf) (accessed 30 July 2010).
- Interagency OPSEC Support Staff. "Intelligence Collection Activities and Disciplines." *Intelligence Threat Handbook*. 1996. <http://www.fas.org/irp/nsa/iOSS/threat96/part02.htm> (accessed 30 July 2010).

- Interagency OPSEC Support Staff. "Intelligence Threat Handbook ." *Intelligence Threat Handbook* . June 2004. <http://fas.org/irp/threat/handbook/> (accessed 31 July 2010).
- International Atomic Energy Agency. "IAEA's "Essential Role" in Building a Global Response to a Global Threat ." *International Atomic Energy Agency*. 14 April 2010. <http://www.iaea.org/NewsCenter/News/2010/nucsec.html> (accessed 16 August 2010).
- Joint IED Defeat Organization. *The Joint Improvised Explosive Device Defeat Organization (JIEDDO)*. 21 June 2010. <https://www.jieddo.dod.mil/about.aspx> (accessed 2 Aug 2010).
- Joint Irregular Warfare Center, USJFCOM. "JOINT IRREGULAR WARFARE 2010 ANALYST REVIEW." *All Partners Access Network*. 4 March 2010. [https://community.apan.org/.../ALL-Collated-RQs-\\_2800\\_PDF\\_2900\\_.pdf](https://community.apan.org/.../ALL-Collated-RQs-_2800_PDF_2900_.pdf) (accessed 11 August 2010).
- Kraul, Chris. *Jamaica violence: Former prime minister fears indefinite martial law*. 29 May 2010. <http://articles.latimes.com/2010/may/29/world/la-fg-0530-jamaica-seaga-20100529> (accessed 8 July 2010).
- Leonhart, Michele. "House Testimony of the Honorable Michele Leonhart, Acting Administrator for the Drug Enforcement Agency, March 2009." *US Department of Justice*. 26 March 2009. <http://www.justice.gov/dea/pubs/cngrtest/ct032609.pdf> (accessed 11 August 2010).
- Llorente, María Victoria, and Cynthia J. Arnson. "Fundación Ideas para la Paz." *Cuadernos Del Conflicto: Initiatives and Colombia's Armed Conflict*. December 2009. [http://www.ideaspaz.org/secciones/publicaciones/download\\_publicaciones/Washington\\_WEB\\_en.pdf](http://www.ideaspaz.org/secciones/publicaciones/download_publicaciones/Washington_WEB_en.pdf) (accessed 9 July 2010).
- Lumpe, Lura. *Small Arms Trade*. 1 May 1998. [http://www.fpif.org/reports/small\\_arms\\_trade](http://www.fpif.org/reports/small_arms_trade) (accessed 10 July 2010).
- Luna, David. "Dynamic Threat Mitigation: Combating Transnational Threats and Dismantling Illicit Networks--The Role of Corruption Nodes ." *U.S. Department of State*. 26 February 2009. <http://www.state.gov/p/inl/rls/rm/119840.htm> (accessed 16 August 2010).
- Luna, David. "Narco-Trafficking: What Is the Nexus With the War on Terror?" *U.S. Department of State*. 8 October 2008. <http://www.state.gov/p/inl/rls/rm/c25212.htm> (accessed 10 July 2010).
- Malm, Aili, Gisela Bichler, and Stephanie Van De Walle. "Comparing the ties that bind criminal networks: Is blood thicker than water." *Security Journal* (Palgrave Macmillan) 23, no. 1 (Feb 2010): 52-57.
- Memon, N., and H.L. Larsen. "Investigative Data Mining Toolkit: A Software Prototype for Visualizing, Analyzing and Destabilizing Terrorist Networks ." *NATO Research and Technology Organization*. 2006. <http://www.rto.nato.int/abstracts.asp> (accessed 31 July 2010).

- Mendel, William W. "Counterdrug Strategy - Illusive Victory: From Blast Furnace to Green Sweep." *Military Review*. 1992 December.  
<http://fmso.leavenworth.army.mil/documents/ilusive.htm> (accessed 13 July 2010).
- Menendez, Robert, and John Kerry. "Counternarcotics and Citizen Security for the Americas Act of 2010." *Robert Menendez United States Senator for New Jersey*. 26 March 2010.  
<http://menendez.senate.gov/imo/media/doc/20100326CounternarcoticsBill.pdf> (accessed 17 July 2010).
- Morton, John. *Statement of John Morton, Assistant Secretary, U.S. Immigration and Customs Enforcement, Regarding a Hearing on "Update on Southwest Border; The Challenges that DHS Continues to Face," Before the U.S. House of Representatives Committee on Appropriations, Subcommittee on Homeland Security*. 14 April 2010.  
[http://www.dhs.gov/ynews/testimony/testimony\\_1274112299629.shtm](http://www.dhs.gov/ynews/testimony/testimony_1274112299629.shtm) (accessed 17 July 2010).
- Naím, Moisés. *Illicit: How smugglers, traffickers, and copycats are hijacking the global economy*. New York, NY: Anchor Books, Random House, 2005.
- National Drug Intelligence Center. "National Drug Threat Assessment 2010." *U.S. Department of Justice*. February 2010. <http://www.justice.gov/ndic/pubs38/38661/index.htm> (accessed 16 August 2010).
- Nitze, Paul H. "Instructions for the coordination and control of the Navy's clandestine intelligence collection program." *A National Security Archive Electronic Briefing Book*. 7 December 1965. <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB46/document1.pdf> (accessed 6 August 2010).
- Obama, Barack. "2010 National Drug Control Strategy." *The White House Office of National Drug Control Policy (ONDCP)*. 2010.  
<http://www.whitehousedrugpolicy.gov/publications/policy/ndcs10/ndcs2010.pdf> (accessed 10-July 2010).
- Obama, Barack. "National Security Strategy." *The White House*. 2010 May.  
[http://www.whitehouse.gov/sites/default/files/rss\\_viewer/national\\_security\\_strategy.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf) (accessed 1 July 2010).
- Office of the Director of National Intelligence. "An Overview of the United States Intelligence Community for the th 111 Congress." *Office of the Director of National Intelligence*. 2009. <http://www.dni.gov/overview.pdf> (accessed 30 July 2010).
- Pendleton, John H. *Testimony before the Subcommittee on National Security and Foreign Affairs, Committee on Oversight and Government Reform, House of Representatives*. 2010 йил 28-July. <http://www.gao.gov/new.items/d10962t.pdf> (accessed 2010 йил 16-August).
- Pham, Peter J., Ph.D. *Criminal Networks in West Africa: An Emerging Security Challenge*. 29 May 2008. <http://worlddefensereview.com/pham052908.shtml> (accessed 8 July 2010).

- Pham, Peter J., Ph.D. *Emerging West African Terror-Drug Nexus Poses Major Security Threat*. 28 January 2010. <http://worlddefensereview.com/pham012810.shtml> (accessed 8 July 2010).
- Rollins, John, and Liana Sun Wyler. "International Terrorism and Transnational Crime: Security Threats, U.S. Policy, and Considerations for Congress." *Congressional Research Service*. 2010 йил 18-March. [http://assets.opencrs.com/rpts/R41004\\_20100318.pdf](http://assets.opencrs.com/rpts/R41004_20100318.pdf) (accessed 10 July 2010).
- Royal United Services Institute. "AFGHANISTAN/IRAN/PAKISTAN CROSS-BORDER SECURITY SYMPOSIUM." *Royal United Services Institute*. 2009 йил 25-March. [http://www.rusi.org/downloads/assets/Cross-Border\\_Security\\_Symposium\\_FINAL.pdf](http://www.rusi.org/downloads/assets/Cross-Border_Security_Symposium_FINAL.pdf) (accessed 14 July 2010).
- Santos, Lucila. *Five false assumptions about the "war on drugs" in Latin America*. 7 July 2010. <http://justf.org/blog/2010/07/07/five-false-assumptions-about-lqwar-drugsrdquo-latin-america> (accessed 17 July 2010).
- Seelke, Clare Ribando, Sun Wyler Liana, and June S. Beittel. *Latin America and the Caribbean: Illicit Drug Trafficking and U.S. Counterdrug Programs*. Congressional Reserch Service. 30 April 2010. [http://assets.opencrs.com/rpts/R41215\\_20100430.pdf](http://assets.opencrs.com/rpts/R41215_20100430.pdf) (accessed 20 July 2010).
- Serena, Chad. "Dynamic Attenuation: Terrorism, Transnational Crime and the Role of the US Army Special Forces." *Global Crime* (Routledge) 8, no. 4 (November 2007): 345-365.
- Shelley, Louise. "Growing Together: Ideological and Operational Linkages Between Terrorist and Criminal Networks." *Fund For Peace*. 14 August 2006. <http://www.fundforpeace.org/web/images/pdf/shelley.pdf> (accessed 7 August 2010).
- Suddath, Claire. *The War on Drugs*. 25 March 2009. <http://www.time.com/time/world/article/0,8599,1887488,00.html> (accessed 12 July 2010).
- Swanson, Scott. "VIRAL TARGETING OF THE IED SOCIAL NETWORK SYSTEM." *Small Wars Journal*. 2007 йил May. <http://smallwarsjournal.com/documents/swjmag/v8/swanson-swjvol8-excerpt.pdf> (accessed 17 July 2010).
- Trebilcock, Craig T. *The Myth of Posse Comitatus*. 2000 October. <http://www.homelandsecurity.org/journal/articles/Trebilcock.htm> (accessed 20 July 2010).
- U.S. Army. "FM 2-22.3 Chapter 3 - HUMINT in Support of Army Operations." *US Army Soldier Portal*. 6 September 2006. <https://rdl.train.army.mil/soldierPortal/atia/adlsc/view/public/23167-1/FM/2-22.3/chap3.htm> (accessed 31 July 2010).

- U.S. Senate Committee on Foreign Relations. "AFGHANISTAN'S NARCO WAR: BREAKING THE LINK BETWEEN DRUG TRAFFICKERS AND INSURGENTS." *US Government Printing Office*. 10 August 2009. <http://www.gpo.gov/fdsys/pkg/CPRT-111SPRT51521/pdf/CPRT-111SPRT51521.pdf> (accessed 10 August 2010).
- UNESCO Kabul. "UNESCO COUNTRY PROGRAMMING DOCUMENT (UCPD) AFGHANISTAN 2010 - 2011." *United Nation Educational, Scientific and Cultural Organization*. 2010. <http://unesdoc.unesco.org/images/0018/001875/187584e.pdf> (accessed 8 July 2010).
- United Nations. *International Day Against Drug Abuse and Illicit Trafficking*. June 26, 2010. <http://www.un.org/en/events/drugabuseday/index.shtml> (accessed 20 August 2010).
- United Nations Office on Drugs and Crime. "World Drug Report 2010." *1.3 The global cocaine market*. 2010. [http://www.unodc.org/documents/wdr/WDR\\_2010/1.3\\_The\\_global\\_cocaine\\_market.pdf](http://www.unodc.org/documents/wdr/WDR_2010/1.3_The_global_cocaine_market.pdf) (accessed 9 July 2010).
- United States Air Force. "Air Force Doctrine Document 2-1.2." *The Defense Technical Information Center (DTIC)*. 12 June 2007. [http://www.dtic.mil/doctrine/jel/service\\_pubs/afdd2\\_1\\_2.pdf](http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_1_2.pdf) (accessed 20 July 2010).
- United States Congress. *10 USC CHAPTER 15 - INSURRECTION*. 1 February 2010. <http://uscode.house.gov/download/pls/10C15.txt> (accessed 21 July 2010).
- United States Congress. "10 USC TITLE 10 - ARMED FORCES." *U.S. Code*. 1 February 2010. [http://uscode.house.gov/download/pls/Title\\_10.txt](http://uscode.house.gov/download/pls/Title_10.txt) (accessed 20 July 2010).
- United States Congress. "18 USC CHAPTER 67 - MILITARY AND NAVY." *U.S. Code*. 1 February 2010. <http://uscode.house.gov/download/pls/18C67.txt> (accessed 20 July 2010).
- United States Congress. "Justice Enhancement and Domestic Security Act of 2003." *U.S. Government Printing Office*. 7 January 2003. <http://www.gpo.gov:80/fdsys/pkg/BILLS-108s22is/pdf/BILLS-108s22is.pdf> (accessed 20 July 2010).
- United States Congress. "PUBLIC LAW 107 - 56 - UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT ACT) ACT OF 2001." *U.S. Government Printing Office*. 2001. (accessed 20 July 2010).
- Viña, Stephen R. "Border Security and Military Support: Legal Authorizations and Restrictions." *Air University selected Congressional Research Service (CRS) reports*. 23 May 2006. <http://www.au.af.mil/au/awc/awcgate/crs/rs22443.pdf> (accessed 10 July 2010).



- Weschler, William F. *TESTIMONY WILLIAM F. WESCHLER DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR COUNTERNARCOTICS AND GLOBAL THREATS BEFORE THE SUBCOMMITTEE ON CONTRACTING OVERSIGHT SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS Counternarcotics Contracts in Central and South America FY 1999 – FY 2009*. 20 May 2010. <http://justf.org/files/primarydocs/100520wech.pdf> (accessed 31 July 2010).
- Wilbanks, Larry W. “THE USE OF NATIONAL GUARD ASSETS FOR COUNTERDRUG OPERATIONS IN THE WAR ON DRUGS.” *The Defense Technical Information Center (DTIC)*. 2002. <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA415946> (accessed 13 July 2010).
- Williams, Dr. Phil. “Drug Trafficking, Violence, and the State in Mexico.” *Strategic Studies Institute Newsletter* (US Army War College), April 2009: 1-4.
- Williams, Phil. “Strategy for a New World: Combating Terrorism and Transnational Organized Crime.” In *Strategy in the contemporary world: an introduction to strategic studies*, by John Baylis, James J. Wirtz, Eliot A. Cohen and Colin S. Gray, 192-208. New York, NY: Pxford University Press, 2007.