

Combing the Underworld: Identification of South East Asian Non-State Actor Proliferation Networks, Nodes, and Chokeyoints

A Monograph

by

**Major Adrian A. Donahoe
United States Army**



**School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas**

AY 05-06

REPORT DOCUMENTATION PAGE			Form Approved OMS No. 0704-0188		
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE (DD-MM-YYYY) 25-05-2006		2. REPORT TYPE MONOGRAPH		3. DATES COVERED (From - To) SEPT 2005-MAR 2006	
4. TITLE AND SUBTITLE COMBING THE UNDERWORLD: IDENTIFICATION OF SOUTH EAST ASIAN NON-STATE ACTOR PROLIFERATION NETWORKS, NODES, AND CHOKEPOINTS			5a. CONTRACT NUMBER		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S) MAJOR Adrian A. Donahoe			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) School of Advanced Military Studies 250 Gibbon Ave Ft. Leavenworth, KS 66027			8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Command and General Staff College 1 Reynolds Ave Ft. Leavenworth, KS 66027			10. SPONSOR/MONITOR'S ACRONYM(S) CGSC, SAMS		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION/AVAILABILITY STATEMENT APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT The US military, as with all US government agencies, shares the responsibility for countering proliferation efforts. Although we have identified the types of threat we face, the systems through which it operates are more difficult to identify. Each region of the world, and indeed, each country have its own peculiarities. This paper asks the question, "How can we be prepared to identify potential proliferation networks and chokepoints in South East Asia?" This paper proposes that a potential solution is the development of a common template that we can use as a starting point for identification of networks, chokepoints, and nodes. This template begins by looking at the interactions within a single country and expands to a geographical region, then ties in other regions to encompass the globe. This paper focuses on South East Asia, and will use examples from a single country for the sample template. The US needs a holistic template that includes networks for other illicit trades identified by not only the Department of Defense but also other agencies. These templates, once completed, may not reveal existing networks, but they could identify the potential for network formation, and assist us in analyzing nodes to monitor, influence, or disrupt.					
15. SUBJECT TERMS Proliferation, Counterproliferation, Nonproliferation, Networks, Chokepoints, Nodes, South East Asia, Organized Crime, Black Markets, Piracy, Drug Smuggling, Arms Smuggling, CBRN, Money Laundering, Human Trafficking, Corruption, Non-State Actors, Terrorism					
16. SECURITY CLASSIFICATION OF:		17 LIMITATION OF ABSTRACT (U)	18. NUMBER OF PAGES 61	19a. NAME OF RESPONSIBLE PERSON	
REPORT (U)	b. ABSTRACT (U)			c. THIS PAGE (U)	19b. TELEPHONE NUMBER (Include area code) (913) 758-3300 Standard Form 298 (Rev. 8/98)

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major Adrian Andrew Donahoe

Title of Monograph: Combing the Underworld: Identification of South East Asian Non-State Actor Proliferation Networks, Nodes, and Chokepoints

Approved by:

David Burbach, Ph.D.

Monograph Director

Kevin C.M. Benson, COL, AR

Director,
School of Advanced
Military Studies

Robert F. Baumann, Ph.D.

Director,
Graduate Degree
Programs

Abstract

Combing the Underworld: Identification of South East Asian Non-State Actor Proliferation Networks, Nodes, and Chokepoints by Major Adrian A. Donahoe, US Army, 57 pages.

The US military, as with all US government agencies, shares the responsibility for countering proliferation efforts. Although we have identified the types of threat we face, the systems through which it operates are somewhat more difficult to identify. Each region of the world, and indeed, each country have its own peculiarities. This paper asks the question, “How can we be prepared to identify potential proliferation networks and chokepoints in South East Asia?” This paper proposes that a potential solution may be the development of a common template that we can use as a starting point for identification of networks, chokepoints, and nodes. This template begins by looking at the interactions within a single country and expands to a geographical region, then ties in other regions to encompass the globe. This paper focuses on South East Asia, and will use examples from a single country for the sample template. Why should we use South East Asia for the development of our template? South East Asia has long been a hub for illicit commerce, smuggling, piracy, and corruption. Many of the networks for drug, money, arms, and human trafficking intersect and often overlay one another within this region. Although many analysts believe that a connection between criminal elements and proliferators does not currently exist, this does not negate the necessity for identification of potential networking. The lack of hard evidence or the belief that criminal elements currently do not see the relative value in assisting proliferators or terrorists attempting to gain access to WMD may be an indicator that we have not looked closely enough at their possible linkages. As organizations and individuals attempt to market available WMD, it is likely that they will attempt to operate networks within countries and regions with pre-existing markets and routes for other illicit trade. Rather than create an entirely new system that counter proliferators would easily identify, it would be simpler to use pre-existing systems. The United States views nonproliferation of WMD through illicit networks and routes as a vital interest for the National Security Strategy. Because of the openness of these markets and trafficking routes, South East Asia poses a major threat to all nations seeking to counter the proliferation of WMD to non-state actors. The US military lacks commonality and interagency integration in its approach to tracking illicit networks and chokepoints. Military analysts or planning groups establish different templates for tracking various illicit networks, or proceed with no template at all. Consequently, it is difficult to maintain consistency in tracking the identified networks, let alone the connections between the proliferators. Current methods of identifying possible networks for trafficking WMD seldom involve an analysis of historic routes, or the possible multiple use by other illicit trades. Different agencies base their templates for identifying networks on individual efforts that they seldom share with others. The US needs a holistic template that includes networks for other illicit trades identified by not only the Department of Defense but also other agencies. These templates, once completed, may not actually reveal existing networks, but they could identify the potential for network formation, and assist us in analyzing nodes to monitor, influence, or disrupt.

Combing the Underworld: Identification of South East Asian Non-State Actor Proliferation Networks, Nodes, and Chokepoints	i
A Monograph	i
by	i
Major Adrian A. Donahoe.....	i
United States Army	i
School of Advanced Military Studies.....	i
United States Army Command and General Staff College	i
Fort Leavenworth, Kansas.....	i
AY 05-06.....	i
Abstract	iii
INTRODUCTION.....	1
CHAPTER ONE: REVIEW OF NATIONAL AND PACOM SYSTEMS AND COMPARISON TO THEORY	4
National Security Strategy Review.....	4
PACOM Review.....	6
Explanation of theory	7
Complexity Theory.....	7
Trust, Influence, and Network Theory	9
CHAPTER TWO: INTERACTION AND IDENTIFICATION STRUCTURES/ FRAMEWORKS	10
IPB vs. ONA.....	11
Sources of Data.....	13
Law Enforcement Models	13
Known Proliferation Network Models	17
Department of State for Arms Control and Monitoring	20
Recommended Model.....	22
CHAPTER THREE: APPLICATION OF THEORY THROUGH FRAMEWORK TO AN INDIVIDUAL COUNTRY	23
Sources of Proliferation.....	23
Identification of Historical Patterns.....	29
Available Means of Transport	32
Identification of Past, Current, and Projected Routes.....	34
Identification of nodes/ chokepoints.....	36
Figure 4.....	40
CHAPTER FOUR: APPLICATION TO REGION AND WORLD	45
Enlargement and Refinement of Recommended Model to Region	45
Enlargement and Refinement of Recommended Model to World	48
CONCLUSION	49
OPTIONS FOR DEALING WITH THE IDENTIFIED NODES	49
Interagency Requirements and Challenges.....	49
Multinational cooperation requirements.....	52
Individual agent requirements	53
Summary	54
BIBLIOGRAPHY	56

Figure 1.....	18
Figure 2.....	20
Figure 3.....	20
Figure 4.....	40
Figure 4.....	40
Figure 5.....	42
Figure 6.....	43
Figure 7.....	44
Finally, we add in the possible network interactions. (See Figure 8).....	44
Figure 8.....	45
Figure 9.....	46
Figure 10.....	47
Figure 11.....	52

INTRODUCTION

If all the nuclear powers of the world are reviewed from the start, all of them established themselves through the underworld. We have also acquired it [nuclear capability] through the underworld.

Pervez Musharaff, President General of Pakistan during proliferation news conference
February 2004

The US military, as with all US government agencies, shares the responsibility for countering proliferation efforts. Although we have identified the types of threat we face, the systems through which it operates are somewhat more difficult to identify. Each region of the world, and indeed, each country have its own peculiarities. This paper asks the question, “How can we be prepared to identify potential proliferation networks and chokepoints in South East Asia?” This paper proposes that a potential solution may be the development of a common template that we can use as a starting point for identification of networks, chokepoints, and nodes. This template begins by looking at the interactions within a single country and expands to a geographical region, then ties in other regions to encompass the globe. This paper focuses on South East Asia, and will use examples from a single country for the sample template. Why should we use South East Asia for the development of our template? South East Asia has long been a hub for illicit commerce, smuggling, piracy, and corruption. Many of the networks for drug, money, arms, and human trafficking intersect and often overlay one another within this region. Although many analysts believe that a connection between criminal elements and proliferators does not currently exist, this does not negate the necessity for identification of potential networking. The lack of hard evidence or the belief that criminal elements currently do not see the relative value in assisting proliferators or terrorists attempting to gain access to WMD may be an indicator that we have not looked closely enough at their possible linkages. As organizations and individuals attempt to market available WMD, it is likely that they will attempt

to operate networks within countries and regions with pre-existing markets and routes for other illicit trade. Rather than create an entirely new system that counter proliferators would easily identify, it would be simpler to use pre-existing systems. The United States views nonproliferation of WMD through illicit networks and routes as a vital interest for the National Security Strategy. Because of the openness of these markets and trafficking routes, South East Asia poses a major threat to all nations seeking to counter the proliferation of WMD to non-state actors. The US military lacks commonality and interagency integration in its approach to tracking illicit networks and chokepoints. Military analysts or planning groups establish different templates for tracking various illicit networks, or proceed with no template at all. Consequently, it is difficult to maintain consistency in tracking the identified networks, let alone the connections between the proliferators. Current methods of identifying possible networks for trafficking WMD seldom involve an analysis of historic routes, or the possible multiple use by other illicit trades. Different agencies base their templates for identifying networks on individual efforts that they seldom share with others. The US needs a holistic template that includes networks for other illicit trades identified by not only the Department of Defense but also other agencies. These templates, once completed, may not actually reveal existing networks, but they could identify the potential for network formation, and assist us in analyzing nodes to monitor, influence, or disrupt. The US military relies on guidance from a national strategy, which the Regional Combatant Commanders (RCCs) then translate into campaign plans germane to their specific Area of Responsibility (AOR). The design of the template gives the RCC Joint Intelligence Operations Center (JIOC) and Theater Special Operations Command (TSOC) planners a start point for the allocation of their intelligence resources dedicated to counterproliferation of WMD.

Many other authors and studies have addressed the nature of the threat posed by the possible connections between illicit trades, organized crime, proliferation networks, and terrorists. Issue papers from the Australian Centre for Peace and Conflict Studies, UNISCI, the Center for Nonproliferation Studies at the Monterey Institute of International Studies, and others address the

concerns of possible collaboration between non-state actors, illicit criminal enterprises, and proliferation networks. None of them encapsulates the full requirements needed to synchronize the efforts and capabilities of the US government and then operationalize the information presented by applying it to preventing, detecting, monitoring, disrupting, interdicting and destroying these networks. This paper attempts to address these requirements. The first chapter identifies the national strategy for combating proliferation of WMD, addresses initiatives that support this strategy, and reviews the military responsibilities of the Pacific Command (PACOM) in developing a campaign to support the strategy. It then looks at the underlying theories required for understanding network interactions. The second chapter examines analytical processes and models from the military, other agencies, and academia to determine available templates and data sources. The information gathered from this chapter provides the foundation for the proposed template. The third chapter provides a sample template using open-source information based on an individual example country, which expands to the region, and the world. The fourth chapter concludes the paper by discussing the difficulties associated with operationalizing the information the template provides, and suggests possible solutions for the difficulties, as well as applications of the template.

CHAPTER ONE: REVIEW OF NATIONAL AND PACOM SYSTEMS AND COMPARISON TO THEORY

The gravest danger our Nation faces lies at the crossroads of radicalism and technology. Our enemies have openly declared that they are seeking weapons of mass destruction, and evidence indicates that they are doing so with determination. The United States will not allow these efforts to succeed. ...History will judge harshly those who saw this coming danger but failed to act. In the new world we have entered, the only path to peace and security is the path of action.
George W. Bush from NSS and NDS on WMD

The purpose of this chapter is to provide an overview of both the national Counterproliferation Strategy and its roots, the structure for implementation of the strategy, and then identify the regional application of the strategy for the PACOM AOR, as well as identify the shortfalls PACOM is attempting to address. The final portion of the chapter introduces the theories of interaction that will assist in understanding nature of systems in place within PACOM.

National Security Strategy Review

The National Strategy to Combat Weapons of Mass Destruction recognizes that nonproliferation among nations is a difficult, if not impossible task, and instead focuses on preventing WMD from falling into the hands of non-state actors. “We know from experience that we cannot always be successful in preventing and containing the proliferation of WMD to hostile states and terrorists.”¹ The National Strategy for Combating Weapons of Mass Destruction outlines the three pillars for combating WMD as being counterproliferation, nonproliferation, and consequence management. It further identifies several “critical enabling functions”² supporting these pillars to include improved intelligence collection and analysis, and strengthened

¹National Strategy to Combat Weapons of Mass Destruction, p.2

² National Strategy to Combat Weapons of Mass Destruction, p.5

international cooperation. This paper addresses elements of these two critical functions in an attempt to help craft supporting strategic and regional campaign plans. The Department of Defense defines nonproliferation as, “Those actions (e.g., diplomacy, arms control, multilateral agreements, threat reduction assistance, and export controls) taken to prevent the proliferation of weapons of mass destruction by dissuading or impeding access to, or distribution of, sensitive technologies, material, and expertise (NP).”³ DOD further defines counterproliferation as, “Those actions (e.g., detect and monitor, prepare to conduct counterproliferation operations, offensive operations, weapons of mass destruction, active defense, and passive defense) taken to defeat the threat and/or use of weapons of mass destruction against the United States, our military forces, friends, and allies (CP).”⁴ The primary distinction between these two definitions lies in the timing of actions taken. Counterproliferation assumes that the weapons or materials are available and accessible and takes action to prevent the use or threat of use, whereas nonproliferation focuses on more preventative measures. The President strengthened US policy on both NP and CP with the introduction of the Proliferation Security Initiative (PSI). The purpose of the PSI “is a global initiative aimed at stopping shipments of weapons of mass destruction (WMD), their delivery systems, and related materials worldwide, announced by President Bush, May 31, 2003. It stems from the National Strategy to Combat Weapons of Mass Destruction issued in December 2002. That strategy recognizes the need for more robust tools to defeat the proliferation of WMD around the world, and specifically identifies interdiction as an area where greater focus will be placed.”⁵ The PSI is an activity that supports the efforts of other organizations in their attempts to counter proliferation of WMD materials. It does not replace any existing organizations, programs, or activities. In fact, the government intends the PSI to complement and bolster programs such as the Containerized Security Initiative (CSI). The PSI’s

³Joint Electronic Library, DOD Dictionary of Military Terms, www.dtic.mil/doctrine/jel/doddict/acronym_index.html nonproliferation

⁴ IBID, counterproliferation

⁵ US Department of State Information Pamphlet on the PSI, p.1

greatest strength is the invitation for other national governments to join and work with the US and UN in counterproliferation efforts. However, the PSI relies heavily on the diplomatic efforts of the Department of State, and lacks and real enforcement capability. The Department of States' Bureau of International Security and Nonproliferation seeks to address comprehensively the issues of both state and non-state proliferation of WMD. They consider combating WMD terrorism as an issue that bridges both nonproliferation and counterproliferation. They have identified the diverse nature of the networks available to terrorists and the threats they pose. "In some cases, they take advantage of safe havens in territories or locations that lack a robust legal or regulatory infrastructure or law enforcement and security capabilities, or worse, have governments that are witting collaborators in terrorist activities. Terrorists also rely on elaborate transportation, logistics, and travel capabilities to move personnel, material, and related capabilities necessary to plan for and carry out attacks. In still other cases, terrorists intrude into "virtual spaces" such as modern financial or communications networks to incite or carry out the preparations for ever more lethal attacks, including those involving weapons of mass destruction." ⁶ Unfortunately, the US government does not staff or sufficiently fund the Department of State to fulfill these intelligence requirements. Instead, we must rely on the capabilities of other government intelligence and operational agencies. In this paper, we will focus on the efforts of the Department of Defense, and specifically orient on the Pacific Command Area of Operations (PACOM AO).

PACOM Review

Currently the United States Pacific Command (PACOM) has identified non-proliferation and counterproliferation of WMD as a priority in their theater security cooperation plans. Additionally, PACOM is attempting to integrate the Effects Based Approach into their planning

⁶DOS Bureau of International Security and Nonproliferation Website, Terrorist Threat <http://www.state.gov/t/isn/wmd/c16583.htm>

methodology. However, development of an integrated campaign plan for dealing with these issues requires the use of Systems of Systems Analysis (SoSA), IPB, and other available systems to obtain a holistic Knowledge Base (KB). The planners apply the KB as part of a maintainable Operational Net Assessment (ONA).⁷ ONA is an attempt to describe the environment in holistic terms using all available information sources and requires constant updating. We will discuss these methods in further detail in the following chapter. PACOM has formed Effects cells within its planning staff elements to address the need for a background knowledge base, but the staff also tasks the effects cells to develop potential negative and positive effects generated by analyzing the KB. The eventual goal is to achieve an overall understanding of the dynamics of the complex systems existing within the PACOM area of operations, and be able to influence the systems to enhance US security while maintaining stability within the region.⁸ The effects cells face the daunting challenge of trying to develop a holistic knowledge base that can cover all areas of operations. They currently do not have a template to address non-state actor proliferation networks, and instead focus on the specifics of individual operations or campaigns. One of the key problems identified particularly by the SOCPAC staff is the lack of direction and prepared products to assist the process.⁹

Explanation of theory

Complexity Theory

Complexity theory looks at the world as a myriad of systems that interact, oppose, and support one another. The exact nature of these systems is particularly dynamic, complex, and adaptive. It requires us to identify not only the major systems and subsystems at play within the region, but also the agents and strategies employed attempting to influence and the artifacts

⁷ For a greater expansion on the Effects Based Approach, see JFCOM *JWFC PAM4*

⁸ Telephone Conversation with SOCPAC J05 GWOT Planner, 14 November 05

⁹ Telephone Conversation with SOCPAC J05 GWOT Planner, 14 November 05

within the systems. In simplified terms, it is a system of systems approach to understanding the world. This system of systems approach is not only valuable in its ability to analyze the region, but also because it can assist us in identifying key nodes or vulnerabilities for intervention in the system that can then produce greater change. This paper defines an agent as something “with the ability to interact with its environment, including other agents. An agent can respond to what happens around it and can do things more or less purposely.”¹⁰ Several aspects of the agent will remain consistent when we analyze their actions, these properties are “location- where the agent operates; capabilities- how the agent can affect the world; and memory- what impressions the agent can carry forward from its past.”¹¹ Furthermore, we can view the concerted actions of agents in terms of populations of agents. “If you are seeking to harness complexity, populations are important in three ways: as a source of possibilities to learn from, as recipients for a newfound improvement, and as a part of your environment.”¹² Complexity theory defines strategies as “the way an agent responds to his surroundings and pursues his goals.”¹³ Finally, we will define artifacts as, “objects that are used by agents.”¹⁴ Of distinct value in complexity theory is the importance of interaction. “Interaction is essential to our framework because the events of interest within a system arise from the interactions of its agents with each other and with artifacts.”¹⁵ By studying these interactions, we discern patterns that can be monitored, modified, or disrupted. These interaction patterns function through both internal and external mechanisms, and will affect the likelihood of continued development of the networks. Our ability to affect these mechanisms determines the selection criteria that attract the adversary for the expansion of his networks. The adversary bases the criteria on the reliability and availability of trusted agents and strategies with the greatest potential for success. Therefore if we place barriers to his

¹⁰ *Harnessing Complexity*, Axelrod & Cohen, p.4

¹¹ *IBID*, p.4

¹² *IBID*, p.5

¹³ *IBID*, p.4

¹⁴ *IBID*, p.6

¹⁵ *Harnessing Complexity*, Axelrod & Cohen, p.62

acquisition in developed nations, then he will likely turn to nations with greater tolerance for illicit activity. This understanding is key to developing a template for identifying proliferation network chokepoints and nodes.

Trust, Influence, and Network Theory

Trust, influence, and network theory (TIN) is very similar to complexity theory in its system of systems approach. It most closely resembles computer-networking theory. However, TIN focuses down much closer on the actual nature of the relationships existing within the systems. TIN works best as a tool of identification within complexity theory. The major advantage gained in using TIN is the identification of the primary nodes and gatekeepers to information and resources within the proliferation networks. Additionally, TIN allows us to identify the best methods of influencing those nodes and gatekeepers.

TIN relies heavily on Social Networking Analysis. Social Network Analysis is “an important academic specialty pursued by a relatively small number of anthropologists, sociologists, and organization theorist...[it] holds that all social relationships, including all social organizations, can and should be analyzed as networks: that is, as sets of actors (nodes) and ties (links) whose relationships have a patterned structure.”¹⁶ When we look at the aspect of trust in sociological settings, we see three broad categories. These categories are anticipatory, responsive, and evocative trust. We can demonstrate anticipatory trust as the act of trust given “because someone believes that the actions carried out anyway by someone else are favorable to the population’s interests, needs, and expectations.”¹⁷ We can liken responsive trust to “the act of entrusting a valuable object into someone else’s hands with their consent expecting responsible care.”¹⁸ Finally, evocative trust resembles “the act of trusting someone else on the belief that the

¹⁶ *Networks and Netwars*, Arquilla & Ronfeldt, p.316

¹⁷ *Trust, A Sociological Theory*, Sztompka, p. 27

¹⁸ *IBID*, p.27

other party will reciprocate with trust towards the first party.”¹⁹ There are a number of trust relationships at work within illicit networks. By identifying the categories of these relationships, we may then begin to determine the strengths and vulnerabilities inherent within them. This is central to the idea of influencing the networks by monitoring, coercing, or attacking the critical nodes and linkages. In this manner, TIN is a valuable analytical tool for the identification of proliferation nodes and chokepoints.

The theories presented here provide a baseline for understanding the nature of possible proliferation networks. They will also aid in determining which model or portions of the models presented are best suited for the development of a template of use at the theater level. Complexity theory demonstrates the ability to take a large, complex, adaptive system, break it down into several smaller systems that we will analyze on a micro scale, and then identify the critical actors, artifacts, networks, and interactions essential to the overall system. TIN allows us to identify and analyze the strength of the relationships within the interactions and aids in determining the likelihood of continued interactions. These theories are critical in determining the validity of current methods of performing analysis. As we examine the models we currently use for identifying illicit networks and past proliferation networks, a baseline understanding of the complexity of the systems is critical.

CHAPTER TWO: INTERACTION AND IDENTIFICATION STRUCTURES/ FRAMEWORKS

The purpose of this chapter is to identify and describe, analyze, and compare different models or processes used by various agencies involved in counterproliferation or other efforts that may assist in the development of a proliferation network template.

¹⁹*Trust, A Sociological Theory*, Sztompka, p.28

IPB vs. ONA

The military developed Intelligence Preparation of the Battlefield (IPB) to provide an easily understood system of quickly identifying enemy resources, capabilities, and vulnerabilities. It was based on pre-determined templates of former USSR modeled militaries, formations, and equipment. IPB, designed for this purpose, was an excellent process for dealing with enemies that used these models. Additionally, it allowed the US military to assess the capabilities we needed to defeat these enemies in an efficient manner. However, the threat we face following the collapse of the Soviet Union is much more complex, dynamic, and less set piece. Additionally, because of familiarity with and reliance on the templates, we discount the many years, if not decades, of analysis that went into the development of those templates. We can consider today's threats as adversarial as opposed to traditional enemies, particularly in South East Asia. The Effects Based Approach addresses many of these shortcomings by looking at the effects achieved by the adversary, and those we hope to achieve against the adversary and within the general populace. However, there is still resistance to completely adopting the Effects Based Approach. Instead, the Army has chosen to take portions of Effects Based Planning to augment the IPB process. US Army doctrine has attempted to adapt to this changed understanding of the enemy by developing an active or running-estimate style template that incorporates the critical challenges we will face until the year 2020. Doctrine developers call this template the Opposing Forces (OPFOR) Contemporary Operating Environment (COE).²⁰ The purpose of the COE is to describe the battlespace that we are likely to find ourselves operating in up through the year 2020. The COE attempts to be somewhat predictive, but not necessarily clairvoyant. Additionally, the Army Futures Center discusses the need for going beyond traditional IPB and including elements of ONA in the description of the COE.²¹ These elements specifically address

²⁰For a greater expansion on the COE, see US Army *FM 7-100*

²¹TRADOC Futures Center Memo: "Effects Based Concepts and Doctrine in Army Education"

political, military, economic, social, information, and infrastructure (PMESII) considerations.²²

At the interservice level, planners integrate the COE into a joint understanding or Joint Operating Environment (JOE).²³ JP 2-01.3 pointedly notes that the primary focus of JIPB is “on providing predictive intelligence designed to help the JFC discern the adversary’s probable intent and most likely future COA.”²⁴

JP 2-01.3 and JWFC Pam 4 describe the primary distinctions between IPB, JIPB, and ONA. The focus of IPB, as understood in joint doctrine, “concentrates on the capabilities and vulnerabilities of the adversary’s individual force components of interest to the component commands.”²⁵ Both JIPB and IPB analyze the effects of the battlespace environment, adversary doctrine if any exists, and hypothesize what courses of action the adversary may attempt.

The function of ONA is “the integration of people, processes, and tools that use multiple information sources and collaborative analysis to build shared knowledge of the adversary, the environment, and ourselves.”²⁶ ONA produces pre-analyzed actions and leverage points in a comprehensive database. The concept behind this database is that it will be available for combatant commanders and their staffs to react rapidly to crises through well-informed planning, leading to the best possible options for the commander to make a decision. ONA is not a substitute for IPB or JIPB, but complements the knowledge produced by these processes. ONA accomplishes this by “proposing options expressed in terms of effect-node-action-resource links. This deepens the SJFHQ’s knowledge of friendly forces and the adversary. The concept calls for persistent and habitual collaboration among subject matter experts from a wide variety of organizations, such as those from the interagency community (IAC) and centers of excellence, as

²² US Army Draft update *FMI5-0.1*

²³ *JP 2-01.3*

²⁴ *IBID*, p.I-1

²⁵ *JP 2-01.3*, p.I-3

²⁶ *JWFC PAM 4*, p.8

well as traditional military organizations.”²⁷ ONA capitalizes on the results of the systems of systems analysis, combined with all other knowledge-producing products. The harshest critique of ONA is the reality of the impossibility of generating an all-encompassing knowledge base prepared for any contingency. However, Joint Doctrine addresses this difficulty with the understanding that, “ONA products could be produced with current capabilities to a lower level of resolution if the joint community commits to the process and products.”²⁸

Sources of Data

The sources of data needed for the ONA approach requires input largely from outside the US military. Currently, analysts place emphasis largely on other government agencies, but as they expand their knowledge base, they are drawing greater amounts of data from other nations, international agencies, NGOs, local and regional law enforcement agencies, and local and multi-national corporations. The template and model for identification of proliferation networks uses the SoSA from ONA as a base to address the complex adaptive system present within potential non-state actor proliferation networks. Our SoSA includes the actors, existing and possible networks, strategies, and the artifacts (sources of material), and both the current and possible interactions. The next section looks at models from law enforcement, DOD, academia, DOS, and the UN. We determine the usefulness of these models in terms of their completeness for identification of current networks and their potential for determining future networks.

Law Enforcement Models

Most law-enforcement agencies design their models to gather evidence against individuals or groups in an attempt to bring the perpetrators before a court. These models are descriptive and designed to gather evidence after the fact. The models identify illegal acts

²⁷IBID, p.8

²⁸JWFC PAM 4, p.23

(problem identification), review available evidence, and then begin a cycle of gathering additional evidence while determining actual jurisdiction. Their general design is not preventative in nature. Their belief is that greater prosecution has its own deterrent effect.²⁹ The frameworks for these processes, therefore, are substantially more detailed, and require a greater depth of background information.³⁰ Additionally, these models tend to look exclusively at one particular illicit trade. This presents both advantages and disadvantages for use by PACOM. The disadvantages are the lack of holistic application, and the additional requirement of sifting through the overall information to find the relevant portions needed for identification. This section will look at models used by the DEA for narcotics trafficking, the FBI for organized crime, media piracy, human trafficking, and grey economics, and US Customs for smuggling, and piracy.

The DEA looks at the sources of drug production, the networks established to transfer the products, and attempts to work with partner nations to intercept and combat these systems as close to the point of production as possible. In this manner, the DEA is more actively preventative than most law-enforcement agencies. They identify the nature of the system, the major areas of activity, and the overall coordination mechanisms for the system. In the following example, the DEA outlines their conceptualization of the Southeast Asian heroin trade.

“Southeast Asian (SEA) heroin traffickers have been operating and conducting drug activity in Southeast Asia for centuries. Typically, these organizations control the cultivation and production levels. They regulate prices, materials, and procedures, allowing for only a small degree of flexibility. At the wholesale level, however, the trafficking process becomes fluid and diversified, and can involve any number of smuggling groups and brokers. Brokers will often have close connections with a particular producer while also arranging transactions with rival

²⁹ Discussions in the criminal justice community vary on the actual effectiveness of the deterrent effect of increased prosecution. Most experts agree that prosecution must be balanced with severity and celerity of punishment in order for deterrence to occur.

³⁰ For a greater expansion on the requirements of forensic investigation, see *Cracking Cases*, Dr. Henry C. Lee

producers. Instead of maintaining continuing relationships with the same group every time, SEA heroin traffickers form limited partnerships with different individuals or groups for the purpose of executing specific drug transactions. These procedures ensure business flexibility as well as protection.”³¹ As was noted earlier, the DEA works with Host Nation agencies in a collaborative effort to reduce the amount of drugs entering, produced by, and transported out of individual countries. Their focus is of course on one particular system within that country. In terms of complexity theory, the DEA model provides an excellent method of identifying actors, strategies, and possible interactions involving drug networks. However, it is not complete enough to provide a model for proliferation networks. But, we can integrate the systems they identify into the overall proposed model.

The FBI looks at individual systems as well, but also links the interconnected nodes of these systems where applicable. Additionally, the FBI works more closely with a variety of local and international law enforcement agencies that assists in expanding their understanding of the linkages of the networks with which they are concerned. An example of this cooperation is in their Asian Criminal Enterprises Working Groups. The assessment produced by these groups provides general background knowledge for the interconnected illicit trades in Asia. “Asian Criminal Enterprises impacting the United States are groups organized by criminals predominantly from East and Southeast Asia... Asian Criminal Enterprises can be categorized as traditional and non-traditional. Traditional criminal enterprises include the Chinese triads based in Hong Kong, Taiwan, and Macau as well as the Japanese Yakuza or Boryokudan. Non-traditional criminal enterprises include groups such as Chinese criminally influenced tongs, triad affiliates, and other ethnic Asian street gangs that are situated in several continents with sizeable Asian communities. The criminal conduct engaged in by Asian Criminal Enterprises include not only traditional racketeering activities normally associated with organized crime such as extortion,

³¹ DEA Intel Brief “SE Asian Heroin Smuggling Methods: Containerized Cargo,” September 2001

murder, kidnaping, illegal gambling, prostitution, and loansharking, but also international organized crime problems like alien smuggling, heroin and methamphetamine drug trafficking, financial frauds such as illegal credit cards, theft of automobiles and computer chips, counterfeiting of computer and clothing products, and money laundering. Several obvious trends have emerged regarding Asian Criminal Enterprises. First, it has become common to see the cooperation of criminal groups that cross ethnic and racial heritage lines. Also, the maturing Asian gangs and some other Asian Criminal Enterprises have begun to structure their groups in a hierarchical fashion to be more competitive, and the criminal activities they engage in have become globalized.”³² The FBI calls their model the “Investigative Process.”³³ The basis of the model is identification of requirements, planning and direction, collection, processing and exploitation, analysis and production, and finally dissemination. The FBI uses this method for tracking human trafficking, copyright infringement/ information piracy, organized crime, and proliferation. The FBI model uses aspects of TIN to identify the complexity of the social network interactions at play within illicit trades. They do not have a set template for proactive identification of potential networks, and in the past have been more concerned with domestic networks. As the FBI continues to field more agents and offices overseas, they enlarge and refine the scope of the identified illicit networks. The level of analysis conducted by the FBI is more exhaustive and aided greatly by extensive forensic capabilities. In this way, their method is more suited as a complementary process for the development of a proliferation network template. Therefore, we will use portions of their intelligence process to verify the known interactions, and the potential methods of trafficking in the proposed model.

³²FBI Asian organized crime web page, <http://www.fbi.gov/hq/cid/orgcrime/aace/asiancrim.htm>

³³FBI Intelligence web page, <http://www.fbi.gov/intelligence/process.htm>

Known Proliferation Network Models

The DIA conducts extensive analysis on the nature of proliferation networks, and portrays these networks using a system of systems approach. The DIA's template for Proliferation Networks shows a complex system involving recipients, front companies, brokers, exporters & producers, transportation & insurance companies, recipient banks, intermediary banks, and exporter & producer banks. (See Figure 1) Applying this model against governments attempting to gain WMD works fine, but falls short when applied to individuals or non-state actors attempting to gain WMD. It also discounts the use of non-western banking systems or grey market economic systems. Islamic banking systems and the Chinese Underground Banking System do not draw the attention of the international banking community, and are difficult to gauge.³⁴ Additionally, a large number of transactions, messaging, and brokering takes place both through underground middlemen, and increasingly in the cyber world. Internet traffickers increasingly pose a greater threat due to their relative anonymity, security, and connections to computer hackers/ crackers.³⁵

However, the model provides an excellent sample of traditional state sponsored proliferation networks. It provides a framework for developing a recommended template based on the resources required, the suppliers available, the required financing, means of transport, and the end-user capabilities. We can address further gaps in the model when we look at the nature of the types of social networks possible and plausible within the overall system. The question arises, "How and why would criminal organizations, terrorist organizations, and WMD subject matter experts interact?" We will address this question in a later section.

³⁴ Drug Intelligence Brief "Anatomy of a Southeast Asian Heroin Conspiracy," August 2002

³⁵ For a greater expansion on the linkages between transnational criminal networks and cyber criminal activities, see *Networks and Netwars*, Arquilla & Ronfeldt.

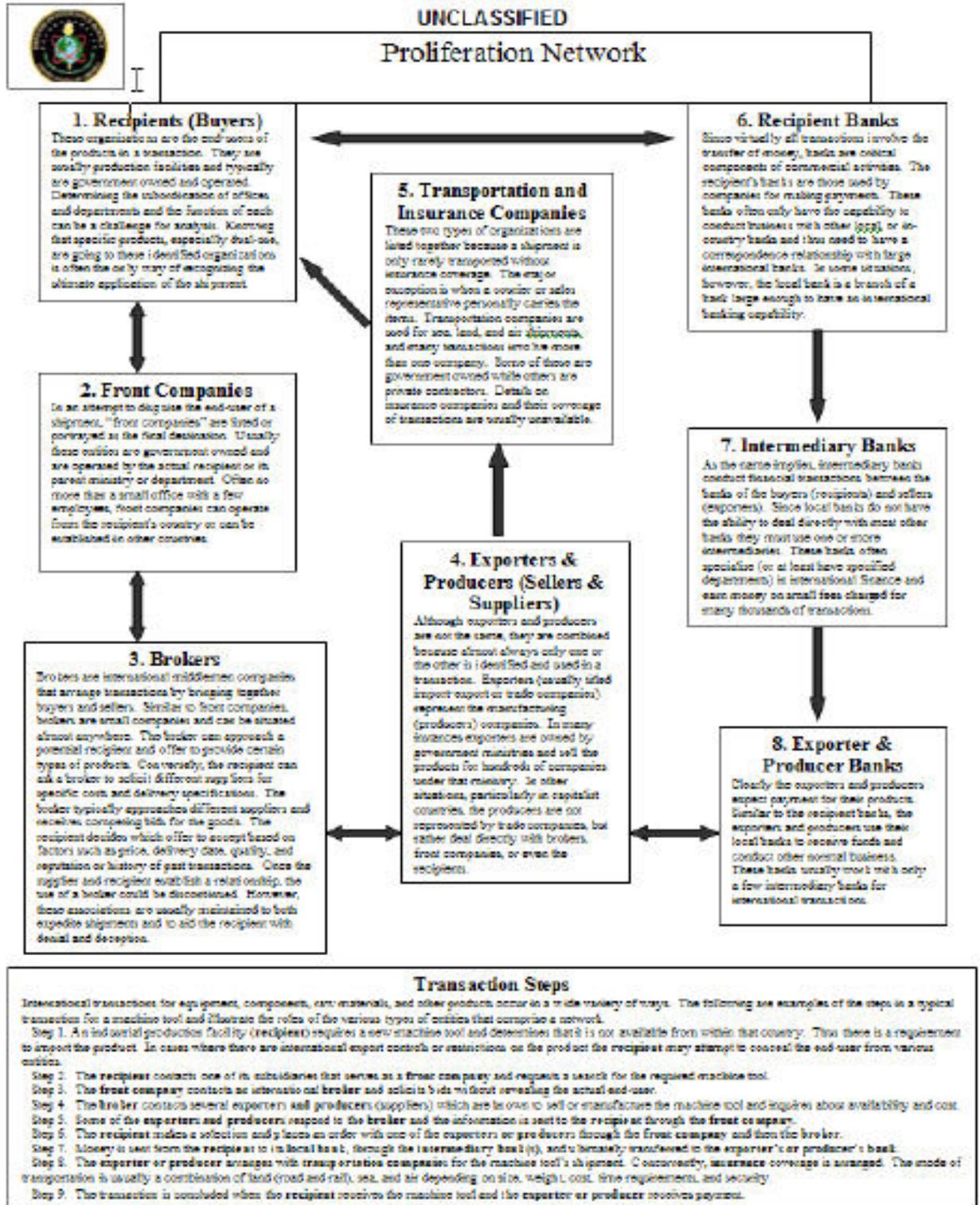


Figure 1

Some academic institutions have modeled proliferation networks as a supply chain. A study produced by Stanford University for a Social Sciences Seminar used the AQ Khan Network as a systems model for analysis and application. The intent of the study was to “determine how future nuclear proliferation networks might be structured and best defeated.”³⁶ They based their model on a risk analysis method, and attempts to understand the uncertainties and interdependent relationships required for the network. The study further attempts to use their understanding of the system of systems required for a proliferation network in order to determine what nodes or relationships must fail in order for the network to fail. In the example of the Khan Network, the study identified core competencies required for the creation and operation of a proliferation network. These core competencies included background knowledge and expertise, marketing and sales, procurement and manufacturing, outbound transport and logistics, service, and payment (See Figure 2). The study further refined their analysis by describing the individual core competencies according to levels of operational abilities and then tactical abilities. It is interesting to note that in the military we consider this a reduction down to lower levels, while this study perceived it as an expansion of levels. In the example provided, the study chose the core competency of payment. The second (operational) level of expansion for payment was money laundering and transfer of sought-after technology to seller. The third (tactical) level of expansion was trusted couriers (for cash transactions), one or more “loose” banks for losing track of cash flow, sought-after hardware, hardware transfer ability, sought-after information, and information transfer ability (See Figure 3). Using this model, the study identified three major factors that contributed to the success of the A.Q. Khan network. The factors are: ties to another successful nuclear program, government complicity through either active or passive participation, and the presence of a motivated “Father” figure with access to all or nearly all aspects of the program.

³⁶“A Systems Analysis of the A.Q. Khan Network”, Barrows, Kucik, Skimmyhorn, & Straigis

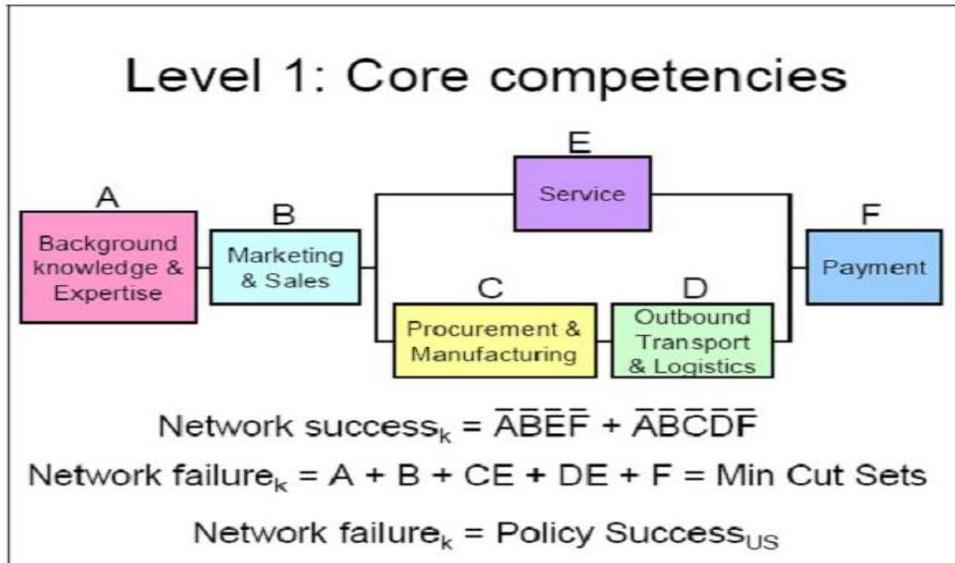


Figure 2

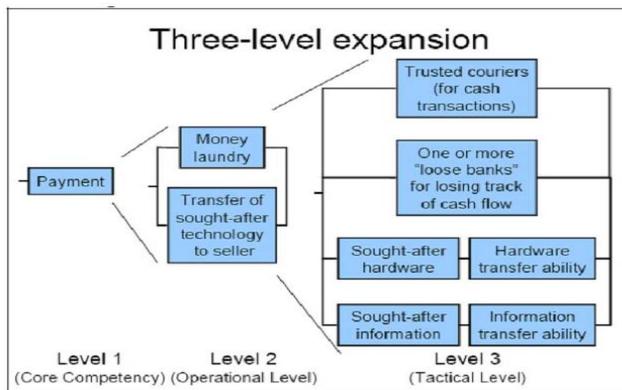


Figure 3

Department of State for Arms Control and Monitoring

The Department of State has authority for arms control and monitoring and is the coordinating agency for all international agreements dealing with these issues. They craft agreements that fall within the scope of USG policies and attempt to align them with international policies as created by the UN, G-8, and other international bodies. The DOS looks largely at nonproliferation efforts conducted through other agencies. Their model identifies source materials, source nations, transportation methods, the expertise needed for WMD development, and the regulatory agencies responsible for monitoring these resources. The DOS then conducts

coordination necessary for preventing proliferation. In this regard, the DOS model also provides an excellent reference base. They provide a database of materials for use in WMD production, as well as identification of dual-use technologies, resources, and expertise. The primary sources for this data come from the Nuclear Suppliers Group (NSG), the Wassenaar Arrangement, the Missile Technology Control Regime (MTCR), the Zangger Committee, and the Australia Group (AG). The NSG is an export-control arrangement, which contributes to the nonproliferation of nuclear weapons through implementation of guidelines for control of nuclear and nuclear-related exports. The NSG is comprised of 40 member nations who pursue the aims of the NSG through voluntary adherence to the guidelines adopted by consensus and through exchanges of information on developments of nuclear proliferation. The Wassenaar Arrangement is the first multilateral institution covering both conventional weapons and sensitive dual-use goods and technologies. The design of the WA is to prevent destabilizing accumulations of arms and dual-use goods and technologies. The Arrangement encourages transparency, consultation and, where appropriate, national policies of restraint. The Zangger Committee harmonizes implementation of the Non-Proliferation Treaty's requirement to apply International Atomic Energy Agency (IAEA) safeguards to nuclear exports. The Committee maintains and updates a list of equipment that countries may only export if the recipient facility applies safeguards, called the "Trigger List" because such exports trigger the requirement for safeguards. The MTCR applies a common export policy (MTCR Guidelines) to a common list (MTCR Annex) of controlled items, including virtually all key equipment and technology needed for missile development, production, and operation. The AG's purpose is "to ensure that the industries of the participating countries did not assist, either purposefully or inadvertently, states seeking to acquire a CBW (chemical and biological weapons) capability."³⁷ The AG provides an excellent example of categories available for data mining. The list of items over which all Australia Group participants

³⁷ US DOS Bureau of Nonproliferation Australia Group Fact Sheet

exercise national export control includes: 54 dual-use chemical precursors; dual-use CW-related production equipment (such as corrosion-resistant reactor vessels); 111 pathogens and toxins that affect humans, livestock animals, and/or food plants; and dual-use production equipment (such as containment facilities and fermenters). In this regard, the DOS provides an excellent background source for sources, uses, and nonproliferation regimes. They have extensive knowledge potential and contacts for identification, but their strategic planning is loosely based.

Recommended Model

The recommended model for identifying routes, nodes, and chokepoints of proliferation networks uses the resultant products from each of the other systems identified above and combines them in a system of systems approach to create a holistic template for allocation of resources. This method uses the background understanding generated from complexity theory to identify artifacts, networks, agents, interactions in a complex adaptive system. It further refines these interactions by examining the strength of existing and potential trust relationships using TIN theory. Furthermore, it uses a step-by-step methodology similar to IPB, but with the holistic effects in ONA. It gathers information from outside agencies such as the FBI, DEA, and combines them with models drawn from past and existing networks. If we understand that we are concerned with the proliferation of materials, knowledge, and expertise able to apply the knowledge to the materials, then we have initially identified what the networks will be trafficking, and the likely methods of transport. The template gathers information on the sources of material and knowledge, adds available means of transport, compares them to historical patterns, identifies past and present through future predicted routes, and then projects likely chokepoints and nodes. In the following example, using open-source information, we can create a baseline template for a single country. The first step is to identify available WMD sources using categories derived through the DOS and the UN. The second step uses historical data on illicit trades within the region and verifies activity through international monitoring agencies.

The third step adds data on methods of transport, and identifies methods of interception by criminal organizations. The fourth step analyzes the actual routes used by the illicit trades and determines areas of possible overlap. The fifth step analyzes the data gathered and determines likely actors, strategies, and artifacts. Once we have identified the networks, the second portion of this step is to identify the network interactions graphically. The third and final portion of step 5 overlays them on maps, and then add the assessments. The final product of the template will be a map of illicit networks. There will be areas identified as common routes, interacting networks, major nodes of grey economic activity, and chokepoints for transport. This model is actually a modified form of link-pattern analysis currently in use by military intelligence and special operations forces.

CHAPTER THREE: APPLICATION OF THEORY THROUGH FRAMEWORK TO AN INDIVIDUAL COUNTRY

The purpose of this chapter is to apply the template based on the recommended model to an example country and test the validity of the model. The example country is Thailand, and all information for this analysis is from open-source material.

Sources of Proliferation

The first step in developing the template is to identify available WMD sources using categories derived through the DOS and the UN. The initial procurement of material for WMD is in itself a complex and difficult system to model. The sources of material range from weapons grade nuclear material unaccounted for or haphazardly secured in the former Soviet Union to dual-use chemical and biological stocks commonly found in most countries. The exact nature of the threats posed by WMD materials and the likelihood of their uses dictates the sources of the material. Sources of material for proliferation fall into the categories of chemical, biological, and nuclear/ radiological resources.

In the chemical realm, the areas of concern are chemical stocks, base products, laboratories for refinement of chemical weapons, and available expertise. The Australia Group provides an excellent list of controlled materials. By conducting a simple web search using the name of the chemical and the name of the country, we can determine the location of producers, marketers, and ease of attainment. For the example case of Thailand, we will use the sample chemical diethylaminoethanol to assist in demonstrating the template. This chemical is a textile-softening agent, but has a dual use in the production of nerve agents. The web search identified over 15 chemical companies that can provide equipment, stocks, and knowledge for the sample chemical Diethylaminoethanol. Of these companies, 8 were registered with ISO (International Organization for Standardization).³⁸ These organizations were large and most were subsidiaries of international parent companies such as Akso-Nobel, or CIBA chemical. An expanded search involving more of the chemicals and materials listed by the AG provided more data on product availability, locations, and methods of shipping.³⁹ The primary function of the search was to identify manufacturers/ suppliers and their locations. The results of this search demonstrated that the majority of the chemical manufacturers and suppliers were located within 50 kilometers of major urban centers such as Bangkok, Chang Mai, and Pattaya. Naturally, the plants were located near a major water source (river or seaport), situated near a major road network, and were in a mixed industrialized/ urban area.

In the biological realm, the major threats include the intentional transfer of naturally occurring emerging and re-emerging diseases, transfer of developed human manipulated biological agents and stocks available for purchase, and development of manipulated biological agents and stocks for eventual sale and transport. The proliferation network therefore must concern itself with the attainment and transport of biological base samples, test laboratories, and

³⁸ Information on standardization and registration requirements can be found at the ISO website, <http://www.iso.org/iso/en/ISOOnline.frontpage>

³⁹ Searches were conducted using www.google.com , and www.thaiwebsites.com

dispersal methods. The ease of attainment of these resources tempers the threats posed in these areas. The swift identification of outbreaks by the host nation usually mitigates the threat of intentional transfer of naturally emerging diseases. However, the potential still exists for their transfer. The CDC identified malaria as the greatest disease threat emanating from Thailand.⁴⁰ Malaria is a chronic problem for the nation, and occurs throughout the southern and central portions of the nation. This disease, combined with the possible future mutation with HIV strains poses a considerable risk for human-to-human transfer. Currently, most strains of malaria are easily treatable, but some strains are becoming more resistant. However, the avian flu is an emerging threat that occurs in Thailand. The avian flu is a more serious concern because of its rapid onset, and initial difficulty in diagnosis. Thailand has had several H5N1 outbreaks over the past few years, with recent cases reported in October, November, and December of 2005.⁴¹ Suphanburi is situated about 90 km (56 mi.) north-west of Bangkok in the central plains and suffered an outbreak in 2004, killing 5 people.⁴² Ban Sabmanao in Klongthabung district of Kaempang Phet province (western plains) had an outbreak in 2004 that left three people dead,⁴³ and may have posed the first human-to-human transmission of the disease (this could not be verified since the bodies were immediately cremated before extensive testing could be conducted).⁴⁴ “Since the start of the outbreaks in Asia, Thailand has confirmed 19 cases, of which 13 have been fatal.”⁴⁵ The significance of these outbreaks is in their location. The greatest proportion of the outbreaks occurred in the central plains regions of Thailand. Although it is likely that migratory populations of birds associating with local poultry populations during

⁴⁰ CDC Health Information for Travelers to Countries in Southeast Asia website, www.cdc.gov/travel/seasia.htm#diseases

⁴¹ CDC Avian Influenza: Current Situation website, www.cdc.gov/avian/outbreaks/current.htm

⁴² Avian Influenza A(H5N1)- Update 17: Situation (human) in Thailand and (poultry) in China, Indonesia and Worldwide, available online at www.who.int/csr/don/2004_02_04/en/

⁴³ Cases of Influenza A (H5N1)---Thailand, 2004, MMWR Weekly, February 13, 2004, available at www.cdc.gov/mmwr/preview/mmwrhtml/mm5305a2.htm

⁴⁴ Avian Influenza- Situation in Thailand, 28 September 2004, available at www.who.int/csr/don/2004_09_28a/en/index.html

⁴⁵ Avian Influenza- Situation in Thailand, Indonesia- Update 36 website, www.who.int/csr/don/2005_10_24/en/index.html

stopovers initiates bird flu transfer in new countries, there are new factors that have become apparent. The analysis conducted by the CDC and the Thai Ministry of Health suggests that the transfer among birds was the result of unintentional human activities. The two primary activities were the movement of free-grazing duck populations from rice paddies throughout the central plains,⁴⁶ and the intentional importation and transfer of fighting cocks. This suggests that proliferators could attain samples of contaminated animals easily if the scale of the outbreak was large enough to require mass destruction of animals. The two most important factors to the proliferators are the speed with which they can move to a contaminated area and the level of activity / confusion occurring within the area to cover their activities.

The AG lists several biological stocks and materials requiring regulation, for the purpose of this example template, we will look at the availability of biological stocks in Thailand, and dual-use equipment such as centrifugal separators. The AG requires regulation and purchase controls on centrifugal separators having the following characteristics: flow rate greater than 100 litres per hour; components of polished stainless steel or titanium; double or multiple sealing joints within the steam containment area; capable of in-situ steam sterilization in a closed state.⁴⁷ However, these restrictions are concerned with the prevention of a mass production of biological weapons. Proliferators can produce biological compounds using smaller-scale, mobile equipment. A web search for biotechnology and biological stocks in Thailand led to the identification of the National Center for Genetic Engineering and Biotechnology, Thailand (BIOTEC).⁴⁸ The Government of Thailand has control over biologic and genetic research conducted within the country. They maintain biological test samples in hospitals and university laboratories at all major urban centers in the country. BIOTEC itself is located in the Thailand Science Park in Bangkok approximately ten miles away from Bangkok international airport.

⁴⁶ “Free-Grazing Ducks and Highly Pathogenic Avian Influenza, Thailand”, CDC Research report, available online at www.cdc.gov/ncidod/EID/vol12no02/05-0640.htm,

⁴⁷ See WA for listing of other equipment and specifications at www.wassenaar.org

⁴⁸ BIOTEC homepage, <http://www.biotec.or.th>

There are numerous companies in Thailand that can provide equipment, stocks, and knowledge on centrifuges and centrifugal separators for biological applications. The majority of these companies or their offices are located in Bangkok.

In the realm of nuclear uses we see four major threats. They are, 1.The theft and detonation of an intact nuclear weapon; 2.The theft or purchase of fissile material leading to the fabrication and detonation of a crude nuclear weapon - an improvised nuclear device (IND); 3.Attacks against and sabotage of nuclear facilities, in particular nuclear power plants, causing the release of large amounts of radioactivity; and 4.The unauthorized acquisition of radioactive materials contributing to the fabrication and detonation of a radiological dispersion device (RDD) – a “dirty bomb” – or radiation emission device (RED).⁴⁹ This paper focuses on threats 1,2, and 4 as particularly relevant in counterproliferation efforts against non-state actors. However, this does not discount the necessity of gathering accurate intelligence for the defense against the third threat. Because Thailand does not produced or possess nuclear weapons, this portion of the template will address base material acquisition. When the model is expanded to include the region and the world, the template will include transport of materials through Thailand. The areas of acquisition and transport for the proliferators are nuclear/ radiological material, dual use technologies for the enrichment, production, and use of this material. Thailand’s Office of Atomic Energy for Peace (OAEP) has oversight on all nuclear and radiological matters in the Kingdom. Thailand has only one research reactor listed by the IAEA that has been in operation for almost thirty years.⁵⁰ Although the reactor is located in Bangkok, universities throughout Thailand use this reactor (TRR-1/M1) for various research projects. One report indicated that an institution in Thailand as far south as Songkhla, scheduled and transported research materials.⁵¹

⁴⁹“Preventing Nuclear and Radiological Terrorism: Nuclear Security in SEA”, Ogilvie-White, p.3

⁵⁰ IAEA International Nuclear Information System web database on worldwide reactors, <http://www.iaea.org/programmes/inis/index.html>

⁵¹ “Nuclear Track-etched Pore Membrane Production Using Neutrons from the Thai Research Reactor TRR-1/M1”, Prince of Songkhla University report, Paper ID: imstec259

Thailand is constructing a second reactor for research and energy production, but the government stopped construction in February 2006, and has not released an expected completion date.

Thailand also possesses two major irradiation facilities for medical and food processing applications. These facilities are Gammaster Thailand (Ltd.), and the Thai Irradiation Centre, OAEP Demonstration Irradiator. Both of these facilities are located in or near Bangkok, and use cobalt 60 as their primary radiating source. The IAEA also lists Thai medical facilities qualified for irradiation activities. These facilities are: Maharaj Nakorn Chiang Mai Hospital (located in Chiang Mai); Rajavithi Hospital; Siriraj Hospital; Tawatchai Chaiwatnarat Poshyanon; and Tawatchai Chaiwatnarat Poshyanontha. Maharaj Nakom is the only facility not located in Bangkok, and Rajavithi is the only facility that is not university based.⁵² OAEP registers over 600 authorized users of radioisotopes in Thailand. These users include individuals and institutions. Additionally, Thailand stores its spent nuclear and radiological waste at OAEP, Chatuchak, Bangkok. This waste includes up to level 4 waste as defined by the IAEA.⁵³

Thailand is concerned with the growing amount of accumulated waste, and the fact that the majority of it is stored near or at the surface in 55-gallon drums.⁵⁴ Near surface storage poses a significant risk of leakage into groundwater. Additionally, the nature of the storage poses a security risk due to the mobility of the drums.

The NSG provides a comprehensive list of dual-use equipment for the enrichment and development of nuclear weapons. From this list, we used the example of machine tools for milling and grinding.⁵⁵ For the example case of Thailand, several companies were identified that can provide equipment, stocks, and knowledge for these machines. These companies were

⁵² IAEA web database on food and medical irradiation facilities, <http://www.iaea.org/cgi-bin/rifa-ste.selqfac.pl>

⁵³ For clarification on waste levels, see IAEA managing waste webpage, <http://www.iaea.org/Publications/Factsheets/English/manradwa.html>

⁵⁴ Near Surface Radioactive Waste Disposal: Safety Assessment of Reference Designs for Low and Intermediate Level Radioactive Waste Repositories, Sryotha

⁵⁵ IAEA *INFCIRC/Rev 6/Part 2*, section 1.B.2

located in or near Bangkok. Additionally, because Thailand is a leading producer of gems and jewelry, they have additional resources for cutting machines and vacuum furnaces.

Identification of Historical Patterns

The second step uses historical data on illicit trades within the region and verifies activity through international monitoring agency databases. Thailand has long been associated with illicit trades such as black markets, prostitution, illegal drugs, money laundering, arms trafficking, and human trafficking. Government departments of commerce and other financial watchdog agencies describe black markets as systems within larger systems of grey economic activity. Black markets themselves operate rather openly in Thailand. The venues for purchase are interspersed among legitimate businesses and vendors in regular markets. Products available in these areas range from pirated software and music, gems and jewelry, foreign currency exchanges, toys, machinery, drugs (prescription and illegal), and weapons in some portions of the country. Both street vendors and legitimate businesses in the common market districts of the major urban centers sell pirated software and music. Gems and jewelry trafficking are more commonly conducted in the border towns near Myanmar, Laos, and Cambodia. Foreign currency exchanges and money laundering occur through two venues. The first is associated with the tourism industry; the second is through the gambling industry. The major tourist hubs that accommodate currency exchange are Bangkok, Chiang Mai, Chiang Rai, Pattaya, Phuket, and Songkhla. The major types of gambling in Thailand are sports betting, fish and cockfighting, illegal lotteries, and gambling dens. The state-run lottery is the only officially sanctioned gambling in Thailand, however, it is estimated that Thailand turns over 380 million Baht a year to gambling (\$9.68 Billion US).⁵⁶ Neighboring countries have taken advantage of Thailand's prohibition on gambling, particularly Cambodia, which has opened large casino resorts in the

⁵⁶ "The Legalization of Gambling in Thailand: A Revisited Discourse in Light of Recent Developments", You, 2004

border town of Poipet. Money laundering, and currency exchange activities fall in the realm of concern for Thailand's Anti-Money Laundering Office (AMLO).⁵⁷ They require notification of all transactions above 2 million baht, property transfers of 5 million baht or more, and registering of any suspicious activities. Recently, they have focused on identification of large donations to "educational activities" that could be a method of money transfer for terrorists or other illegal groups. International attention in recent years has focused on Thailand because of its poor record in human trafficking. Human rights organizations recognize Thailand as both a major supplier and transportation hub for human trafficking, particularly for the sex industry. The United Nations Inter Agency Project (UNIAP) for the Greater Mekong Sub-Region designated Thailand as a Tier 2 Watch List trafficking nation. The Tier 2 designation indicates that the government of Thailand fails to provide evidence of increasing efforts to combat exploitation of immigrants, particularly Cambodian women. "Thailand is a source, transit and destination country for persons trafficked for sexual exploitation and forced labor. Thailand is a destination for men, women and children from Burma, Laos, Cambodia, and China who are trafficked for forced or bonded labor and prostitution. Thai women are trafficked to Australia, South Africa, Japan, Bahrain, Taiwan, Europe and North America for sexual exploitation. Internal trafficking also occurs in Thailand, involving victims from Northern Thailand. Additionally, regional economic disparities drive significant illegal migration into Thailand, presenting traffickers opportunities to move victims into labor exploitation. Widespread sex tourism in Thailand encourages trafficking for forced prostitution."⁵⁸ The networks developed for human trafficking are centered out of the major population centers, but gather their human capital from both rural and urban areas, as well as neighboring countries. The greatest centers are located once again in the tourist areas of cities such as Bangkok, Pattaya, Chiang Mai, Chiang Rai, and Songkhla. Arms trafficking networks for Thailand have a well-defined structure and provide an excellent network model. "Thailand acts

⁵⁷ AMLO homepage, www.amlo.go.th.

⁵⁸ UNIAP Trafficking In Persons (TIP) Report 2004

as the main transit area for light arms from Cambodia, with maybe as many as 80% of all illegal consignments passing through the country. Several factors account for the Kingdom's attractiveness in this regard, including its geographic proximity to Cambodia, the large turnover of foreign tourists and businessmen travelling to the country (which makes blending in easy), the existence of a relatively advanced communication and transportation infrastructure, and highly porous land borders. Moreover, Thailand is a country where 'money talks', allowing syndicates and traffickers to buy co-operation and, more importantly, silence in high places.”⁵⁹ Thailand's Economic Crimes Investigation Division works with Interpol and the FBI to stem piracy of intellectual property and copyrighted materials. The International Intellectual Property Alliance (IIPA) estimated a loss of \$174.9 million (US) in trade lost to the motion picture, record and music, business software, entertainment software, and book industries for 2004, because of piracy.⁶⁰ There are significant indicators that piracy syndicates are becoming more violent and increasingly well connected to policy makers within the Thai government.

Illegal activities cannot occur unless they are tacitly sanctioned, tolerated, or the government is too weak to oppose the structures operating the activities. Thailand has a very active and moderately well resourced military and police structure. Their greatest weakness is not their inability to oppose criminal structures, but the relative levels of corruption infecting their systems. Interpol defines corruption as, “any course of action or failure to act by individuals or organizations, public or private, in violation of law or trust of profit or gain.”⁶¹ International monitoring agencies, such as Transparency International, measure the levels of corruption in Thailand in terms of perception, both domestic and international. Both historical and ongoing events significantly shape the domestic views of government and police corruption. Thailand has endured a number of military coups over the years, and it was only the intervention of the King

⁵⁹ “Light Arms Trading in SE Asia,” Chalk, Jane's Intelligence Review, March 1, 2001

⁶⁰ IIPA Special 301 Report Thailand

⁶¹ Interpol Group of Experts on Corruption (IGEC) mission statement webpage
www.interpol.int/Public/Corruption/IGEC/Mission/Default.asp

that provided stability. Relatively recent constitutional amendments direct the separation of military and political positions. These amendments, combined with the popular support of a strong monarchy with the ability to dictate and arbitrate the nature of political positions result in a relatively stable government. However, even the monarch's influence can be misinterpreted and used to the advantage of corrupt elements. A recent example includes the concern expressed by the king in 2003 over the increase in drug use/ abuse in Thailand. This concern prompted an immediate response on the part of the Prime Minister and his government to crack down on drug trafficking. Unfortunately, there is widespread belief that many corrupt police officials used this opportunity to hide their activities or reinforce their control. The crackdown resulted in over 2300 deaths in a one-year period. The government attributes these deaths to infighting amongst gangs and organizations, and legitimate self-defense by police. However, there are also many conflicting reports accusing corrupt police of eliminating competition and informants that could implicate them. Additionally, there were repeated reports of "death-squads" that acted with impunity in attacking suspected illicit actors without due process.⁶² The areas of greatest tolerance or apathy towards local and regional government corruption are of course in the red-light districts of the major urban tourist centers such as Bangkok, Pattaya, Chiang Mai, Chiang Rai, and Songkhla; and border towns such as Mae Sot, Aranyaprathet, and Had Lek.

Available Means of Transport

The third step focuses on the modes of transport available, and the throughput capacities present in the country. Thailand has a robust infrastructure supporting air, sea, and land transport. Thailand transports domestic freight by truck, river and seaway traffic, and intra regional air. They have a well-established postal system, and numerous shipping companies, most of whom have headquarters in Bangkok. The majority of large import/export freight comes in

⁶²"Probe Urged Into All Violent 'Drug' Deaths", Bangkok Post, February, 2003

containerized cargo through Thailand's seaports. This does not discount the use of nonstandard transport methods, such as pack animals used in the border regions. Trafficking of narcotics shows the adaptive use of transport systems available to proliferation networks. Traffickers ship large quantities of heroin on a daily basis using containerized cargo systems from ports in the Gulf of Thailand. However, due to the sheer volume of cargo transported from these ports using these systems, it is extremely difficult to inspect and insure the integrity of these containers. "Heroin processed in the Golden Triangle (Burma, Laos, and Thailand) is smuggled overland to seaports in Burma, China, Thailand, Malaysia, and Vietnam for transshipment within containerized cargo through Taiwan, Hong Kong, Singapore, Japan, and Korea. From these transit countries in Southeast Asia, the heroin-laden containers are shipped to consumer markets in Europe, Australia, Canada, and the United States."⁶³ Thailand operates 6 major ports that can handle containerized cargo. They are located in Bangkok, Siricha, Rayong, Pattaya, Songkhla, and Pukhet.

In addition to the transport of illicit goods, there is also concern over the illegal interdiction of legitimate goods. Maritime piracy provides an excellent example for the template to model interdiction methods. Victims of maritime piracy often do not report the crime due to various reasons. Shipping companies often do not report it due to fears of increased insurance costs, loss of confidence on the part of shippers, some of the pirated ships may have been carrying illicit cargo and the owners of the goods would prefer to retain plausible deniability,⁶⁴ and the relative negligible risk associated with the likelihood of attack. Piracy in the coastal waters surrounding Thailand is a dangerous and difficult threat for the government. Maritime piracy grew throughout the 1980's and has only declined in recent years. The levels of piracy run the gamut from the boarding of small fishing vessels to the hijacking of supertankers. Historical

⁶³ DEA Intelligence Brief "South East Asian Heroin Smuggling Methods: Containerized Cargo", September 2001

⁶⁴*Dangerous Waters*, Burnett, p.143

evidence demonstrates that the Bight of Bangkok, also known as the Bangkok Bar, is the most dangerous area in the seas surrounding Thailand. The Bight of Bangkok is located in the Gulf of Thailand and runs parallel to the coastline between Satahip and Bangkok. The highest number of reported acts of maritime piracy in Thai waters was 13 in a year.⁶⁵

Identification of Past, Current, and Projected Routes

The fourth step analyzes the actual routes used by the illicit trades and determines areas of possible overlap. For the sample template, we will examine maritime piracy routes and networks, arms smuggling routes, narcotics trafficking routes, human trafficking routes, money laundering routes, counterfeited/ contraband and pirated materials routes. Modern maritime pirates use a variety of vessels to accomplish their activities. These include fishing boats with extended ranges, speedboats with short to medium ranges, and smaller inflatable craft for coastal raids. The pirates will commonly board ships anchored at night or are slowly navigating dangerous coastal inlays. A favorite launch point for the pirates is from the mangrove swamps located in the coastal areas north of Satahip. Their methods vary based on several factors: the size of the craft they are boarding; the nature of the organization the pirates are operating under; and the craft available to conduct the attack. Depending on these factors, they will restrain the crew or kill them, rob them of all money and valuables, remove cargo for later resale on the black market, or attempt to take the entire ship to a different port for renaming and reflagging. The pirates either move the cargo to shore and transport it to holding areas near Bangkok, or bring the cargo directly into the port. Arms smuggling routes follow distinct paths within Thailand. Weapons dealers or intermediaries with a well-established clientele set up purchases of light arms from Cambodia. These dealers operate in major urban centers such as Bangkok, Phuket and Chiang Mai. The consignments smuggled from Cambodia follow two primary routes, the first is

⁶⁵ ICC International Maritime Bureau database

overland, the other by sea. The overland route enters Thailand in Chantaburi province in the east. From this area, middle-men swiftly transport arms to major hubs such as Bangkok or Pattaya. The sea route flows from Kampong Saom, Cambodia directly north or west to Thai ports. Upon arrival in the major hubs or ports following the primary routes, the shipments move through Thailand to a regional center that can best accommodate arrangements for final or continued delivery. Narcotics trafficking routes within Thailand come in from the north, east, and west, and all flow south. Heroin enters from both Myanmar and Laos, but harsh enforcement has drastically curtailed these shipments. The current threats in Thailand are methamphetamines and their related designer cousins such as ecstasy, with Myanmar as the main supplier. The major overland routes come from the Wa and Shan controlled provinces in Myanmar to Chiang Mai and Chiang Rai provinces in Thailand. The traffickers move the drugs through the highland areas to the major centers such as Bangkok. From Bangkok, the traffickers distribute the drugs overland throughout the country, or ship them out of nearby ports or southern ports. Human trafficking routes within Thailand flow predominantly from the rural and border areas into the major urban centers such as Bangkok, Chiang Mai, Pattaya, and Songkhla/ Pukhet. Routes from Myanmar to Thailand flow through the Mae Sai District of Chiang Rai Province, the Mae Sod District of Tak Province, Sangkhaburu District of Kanchanaburi Province, and Ranong. From Laos the routes flow through Chiang Rai, Nong Khai, Nakornpanom, Mukdaharn, and Ubon Ratchathani. Cambodian trafficking routes go through the Aranya Prathet District of Sa Kaew Province, and Trad.⁶⁶ Money laundering routes flow into the major urban centers, pass through real estate, insurance, and currency exchange offices or go directly to border towns to be transferred through gambling establishments, or narcotic smuggling organizations. Suspect donations typically flow into the country from the southern regions for distribution throughout the southern provinces. International copyrighted intellectual property piracy routes in Thailand flow from their sources

⁶⁶UNIAP TIP Report 2004

of production in China and along the Thai-Myanmar/ Thai-Lao borders, to distribution hubs in Chiang Mai and Chiang Rai, then on to Bangkok and other major cities and ports.

The results of these route analyses points to a convergence in the selling, domestic distribution, and further transport of these activities. The next step looks at the actors, artifacts, strategies, and interactions that lend make these pre-existing systems attractive to proliferators.

Identification of nodes/ chokepoints

The fifth step analyzes the gathered data and uses a combination of complexity and TIN theories to determine likely actors, strategies, and artifacts, as well as their interactions and their trust relationship dependencies. The actors are those involved in organized crime, terrorist organizations, and subject matter experts. The strategies are those that include the successful transport of illicit goods, the development of organizational structures that avoid detection, and the sharing of knowledge, training, and skills. The artifacts are the proliferable materials and resources to acquire the materials. Organized criminal networks in Thailand control the majority of illicit activities in the nation. These organizations control the larger acts of maritime piracy, the flow of narcotics, human trafficking networks, money laundering, gem smuggling, intellectual property piracy, and maintenance of corruption tolerance. The actors of concern specifically addressed in Thailand are those criminal organizations operating in the major urban centers that interact with criminal and terrorist organizations in the southern portion of Thailand. The majority of the northern portion of Thailand is Bhuddist. The southern provinces of Yala, Narathawat, Pattani, and Songkhla, are predominantly Muslim. Islamic fundamentalists have conducted terrorist attacks in the southern provinces in recent years. “The base for the Islamic movements in the south of Thailand is in the privately run religious schools known as ‘pondok’”. There are an estimated 250 pondok in Pattani, Yalla and Narathiwat that teach only Islamic studies and 192 Islamic private schools that are accredited by the Thai Ministry of Education. The schools are where the indoctrination of Islamic extremism is done and where fighters are

recruited. The teachers at these schools are the backbone of the Islamic movements as they usually are the mid-level commanders and cell leaders.”⁶⁷ These fundamentalists may have connections to Jemaaah Islamiyah (JI), and other Al-Qaeda affiliates. A major indicator of possible terrorist connections to these criminal organizations was the arrest in Thailand in 2003 of Riduan Ismuddin, a.k.a. “Hambali.” Authorities believe Hambali assisted the planning for the 9/11 attacks, and was the central planner for JI bombings such as occurred in Bali in 2002, and had extensive contacts with Islamic extremists, as well as local and regional criminal organizations. These networks established themselves internationally and have many ties to other criminal and terrorist organizations. Of particular interest are the narcotics cartels in the Golden Triangle that control the greatest portion of underworld activities. They are linked to many other organizations under each of their activities. “Many of the weapons are trafficked to narco-insurgents in Myanmar, who either keep the arms for their own use or resell them, generally to groups operating in India or Sri Lanka. The Liberation Tigers of Tamil Eelam (LTTE), for instance, are known to run an intensive Thailand-Myanmar arms network that has, on occasions, been 'hired' out to other groups operating on the sub-continent. Significant quantities are also moved through ports in southern Thailand to Muslim guerrillas operating in Indonesia and the Philippines, either directly or via the Malaysian provinces of Kelantan, Sarawak and Sabah.”⁶⁸ However, the greatest requirement is in the nature of the types of relationships established within these networks. Some analysts argue that the relationship between terrorist groups and criminal organizations themselves are more marriages of convenience than actual networks. “Marriages of convenience may exist, they say, but the key difference is one of motive: Terrorist groups are driven by politics and religion, while purely criminal groups have just one thing in mind--profit. Indeed, associating with terrorists, particularly since 9/11, can be very bad for business--and while crime syndicates may be parasitical, most do not want to kill

⁶⁷ “Thailand’s South Embroiled in Sectarian Conflict”, Neuman, JINSA Online, January 10, 2005

⁶⁸ “Light Arms Trading in SE Asia”, Chalk, Jane’s Intelligence Review, March 1, 2001

their host.”⁶⁹ A counterargument also exists, that in areas of high corruption and tolerance of illicit activities where terrorist organizations are likely to continue to conduct illicit trade in order to support their cause, it is more profitable for the two types of organizations to work together than to compete. Although the motivation for the terrorist is ideological, while the motivation for the criminal is profit, both motivations are supportable through this alliance.

Establishing possible connections between organized crime and terrorists is not as difficult as establishing a link between scientists and criminals/ terrorists. The internet has opened a doorway for this connection in the form of career websites tailored specifically for fields of scientific study and application. Websites such as the Microbiology Network (www.microbiol.org), The International Chemistry Society (www.chemsoc.org), the Physics Network (www.physnet.net), and others provide direct contact information for specific fields of study, as well as offering resume hosting for potential employment. By accessing these databases under cover of identity theft or educational institutions, proliferators can research the backgrounds of potential subject matter experts for exploitation. Exploitation can occur through extortion, threat of violence, or ideological concern. This allows the proliferator or the criminal network, acting as the proxy or enforcer for the proliferator, to find potential candidates locally or internationally. The types of trust relationships that might exist between organized crime and terrorists are evocative trust, and responsive trust. Neither organization would act on the other’s behalf without the promise of some form of product or profit combined with a reasonable expectation of success. The criminal organization would initially require some act of assurance by the terrorist organization in order to evoke their trust. After continued success, both organizations would continue the relationship as long as mutual expectations were met. The understanding that both organizations would view the arrangement of activities as requiring secrecy and trust placed in the capabilities of each other to fulfill requirements leverages the

⁶⁹ “Paying for Terror”, Kaplan, US News and World Report, December 5, 2005

expectation of success. The types of trust relationships that might exist between terrorists, criminal organizations, and subject matter experts might be both anticipatory and responsive trust. If the terrorist organizations found candidates that shared their ideology, then anticipatory trust would exist, since the candidate would act on behalf of the terrorists in the belief that the situation itself would be improved or driven to a common goal. If no candidates with shared ideologies are immediately available, then the criminal organizations could use exploitive methods on behalf of the terrorist elements to pressure or entice cooperation of subject matter experts. For this portion of the template, we will look at the trust relationships between members of organized crime such as the Khun Sa Narcotics Cartel operating in the Golden Triangle, terrorist organizations such as the members of JI, and the scientific community needed to provide WMD expertise. Common links between these three communities lie in the areas of chemistry and biology, but does not discount the possible transfer of nuclear related resources and knowledge out of the country. The production and refinement of methamphetamines requires the use of minimal laboratory equipment and expertise for small-scale urban facilities. Training and expertise for these processes can come from undergraduate through graduate level education, but can begin with those showing aptitude or interest in chemistry. Common usage of amphetamines by younger Thais, particularly among college students offers an inroad for trafficking and network development. JI recruits from the population of southern Thailand and could gear particular recruits toward specific fields of study in the southern universities. Additionally, JI's interactions with the Khun Sa Cartel and other organizations provides continued marketing opportunities for weapons, software, and human trafficking with increased financing.

The second portion of this step is to identify the network interactions graphically. The final product of the template will be a map of illicit networks. The first step is to identify the proliferation sources internal to Thailand for all the categories of WMD threats. The primary sources of chemical precursors, dual-use chemical equipment, and knowledge exists in the cities of Bangkok, Chiang Mai, Pattaya. The primary sources of biological precursors were in the

central plains regions of Suphanburi and Kaempang Phet, but dual-use equipment, and knowledge exists in major cities such as Bangkok, Chachaengsao, Chiang Mai, Chiang Rai, Pattaya, Pukhet, Songkhla, and others. Nuclear materials and waste are stored in or near northern Bangkok. However, the second reactor under construction is in Ongkarak, Nakorn Nayok Province. Dual use equipment and knowledge can be found in the major cities of Bangkok, Chiang Mai, Pattaya, and Songkhla. The first map graphically portrays these areas (see Figure 4).



Figure 4

Figure 4

Next is identifying the historical patterns in and around Thailand. (See Figure 5)

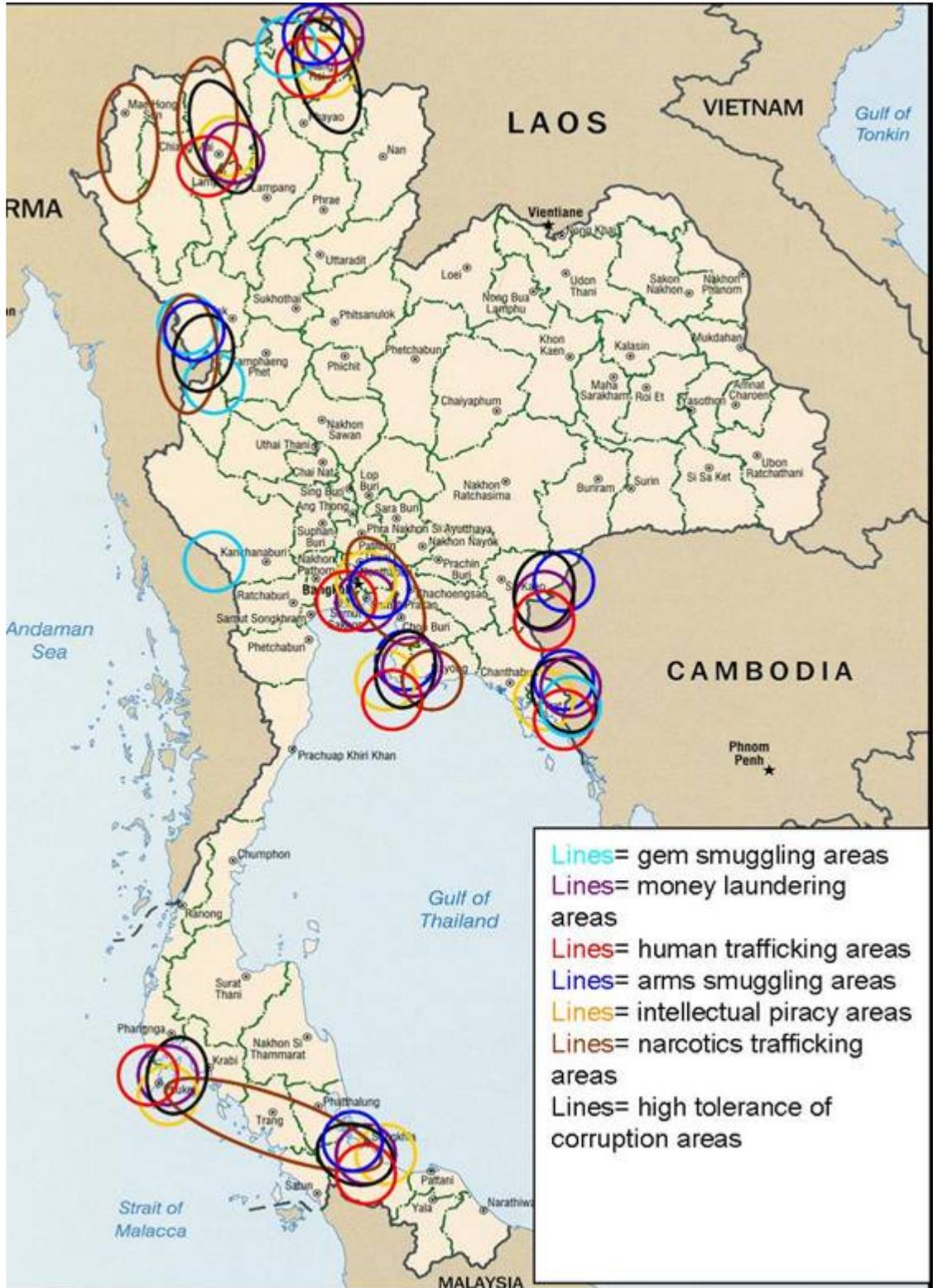


Figure 5

The next step is to identify the available means of transport in Thailand. (See Figure 6)



Figure 6

Then we overlay the past, current, and projected illicit routes. (See Figure 7)

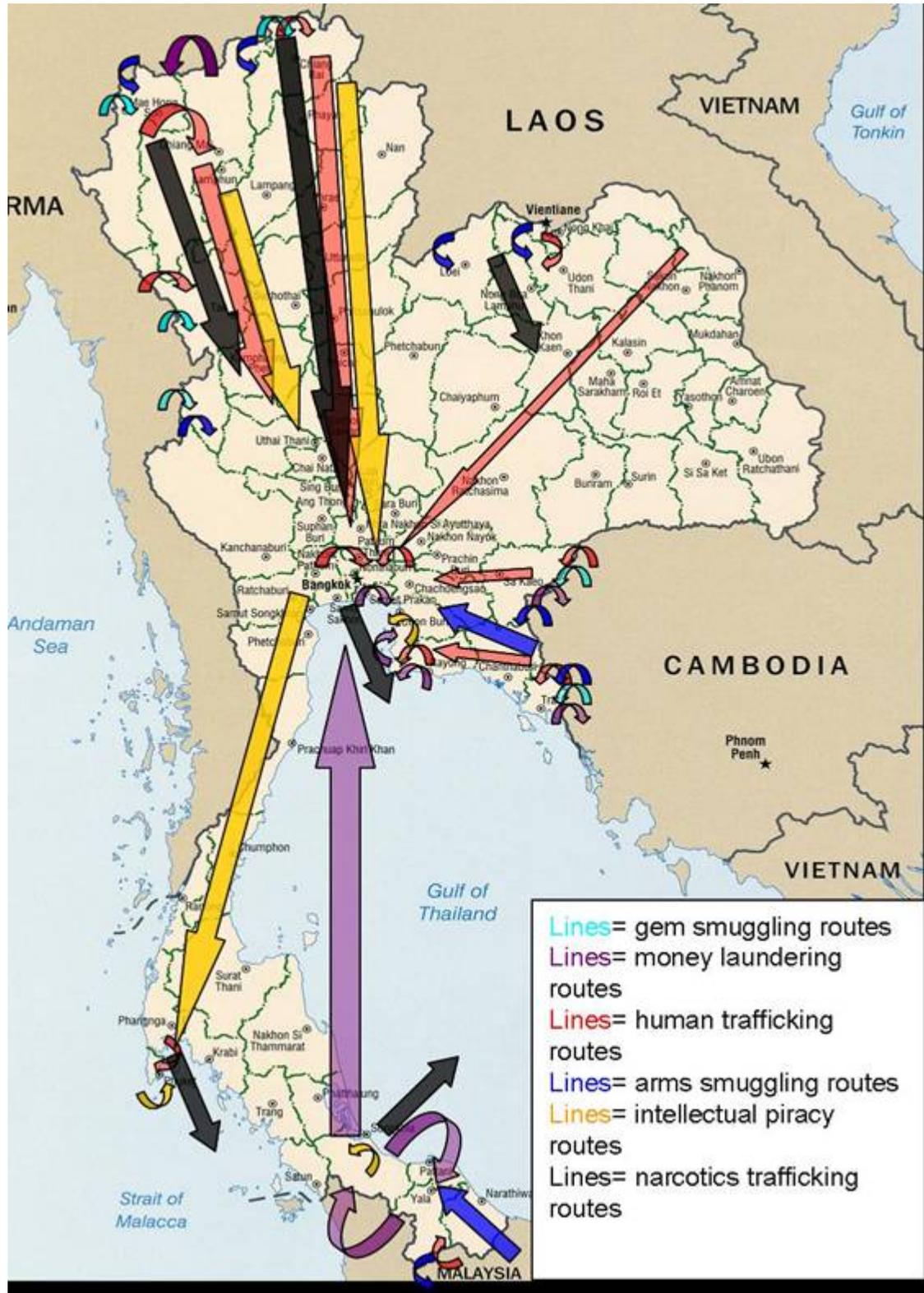


Figure 7

Finally, we add in the possible network interactions. (See Figure 8)

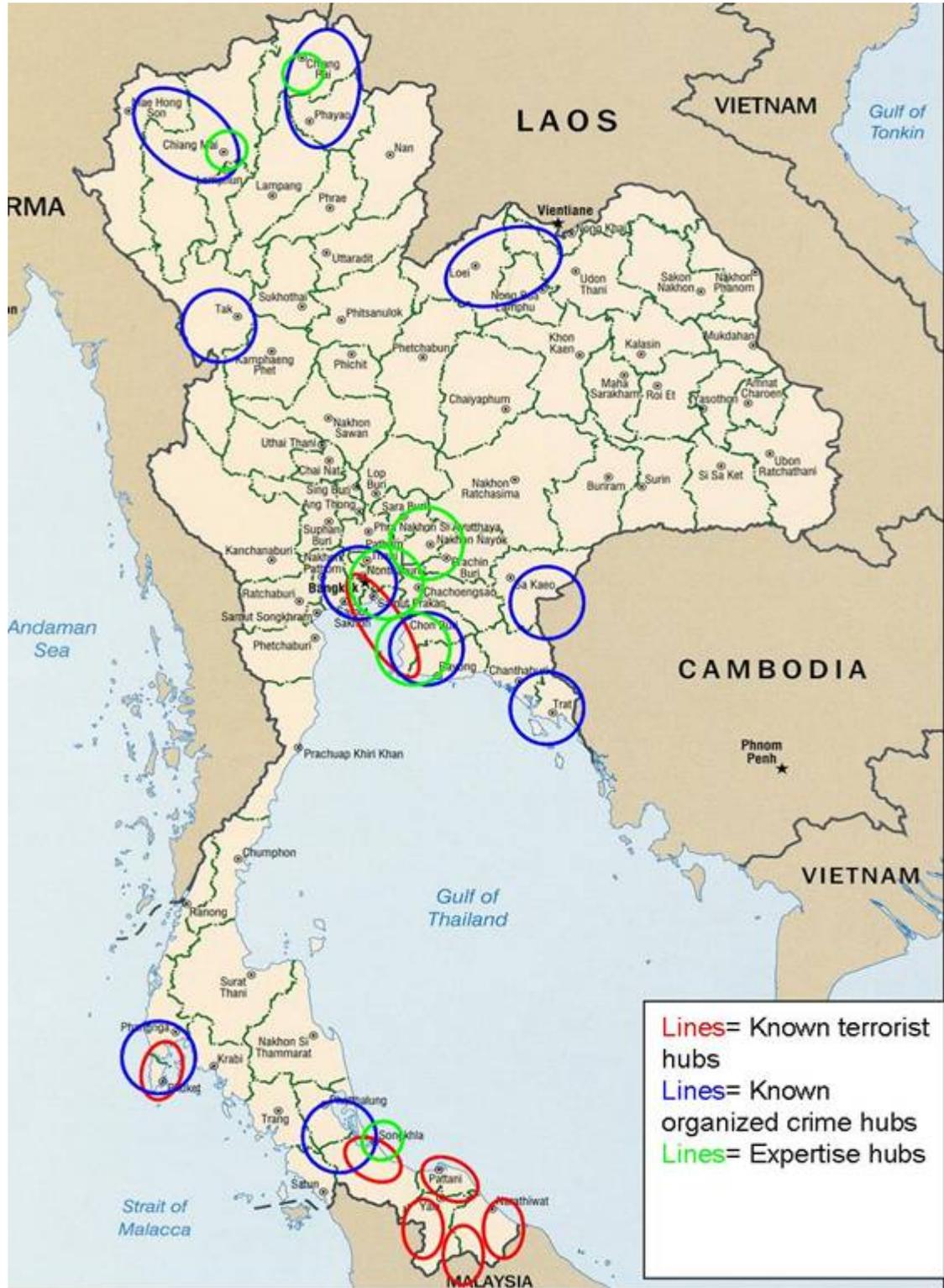


Figure 8

We can then use these final products for the allocation of intelligence assets. Nodes exist in the major cities of Bangkok, Chiang Mai, Pattaya, and Songkhla. These are also major hubs for existing terrorist, organized crime, and expertise networks. The chokepoints occur in the border areas, in the major ports, and shipping lanes. By identifying these areas and working with other agency assets, as well as host nation agencies, we can gain greater clarity on the exact nature and full interaction of these possible networks.

CHAPTER FOUR: APPLICATION TO REGION AND WORLD

Enlargement and Refinement of Recommended Model to Region

The next step for enlargement of the model is to take the templates developed for each of the individual countries, and begin identifying the areas of overlap within the region. An example of the possible expansion of the templates' steps is the use of Thai radioactive waste or source material transported by arms smugglers to Malaysia through southern Thai terrorist routes. The radioactive waste or material could be refined in Malaysian centrifuges, as was done by the AQ Khan network. This refined material could be used immediately by AQ affiliates such as JI, or shipped anywhere from the Malaccan straits. Terrorist networks in concert with organized criminal networks could operate on a regional and global scale by exploiting their combined resources. "An effective distribution network enables the drug traffickers to transport the refined heroin and amphetamines from the Golden Triangle into Thailand, which is still one of the major routes of the illicit drug trade. Narcotics are also smuggled from the Golden Triangle into China's Yunnan Province and then overland to Guangdong, Hong Kong and Macao. Moreover, Ho Chi Minh City, Manila and Phnom Penh have become important hubs in the global drug distribution. All these different destinations are used as transit points to supply domestic and international markets. The Chinese triads trade most of Asia's narcotics and collaborate with other transnational criminal organizations, such as the Japanese yakuza, Vietnamese gangs, Nigerian groups and Colombian cartels, to distribute illicit drugs worldwide. The drug trade, but also to an increasing extent human trafficking, has provided these mafias with exceptional financial

resources. These funds enable the criminal syndicates to dispose over modern military equipment and to corrupt politicians, judges and police authorities. Consequently, to refer to these mafias, especially in the case of the Chinese triads, as mere criminal groups tends to minimize the threat that they pose to the political, economic and societal stability of regional states.”⁷⁰ Other reports indicate the South East Asian Region is a particularly necessary hub for proliferation transit. (See figure 9).

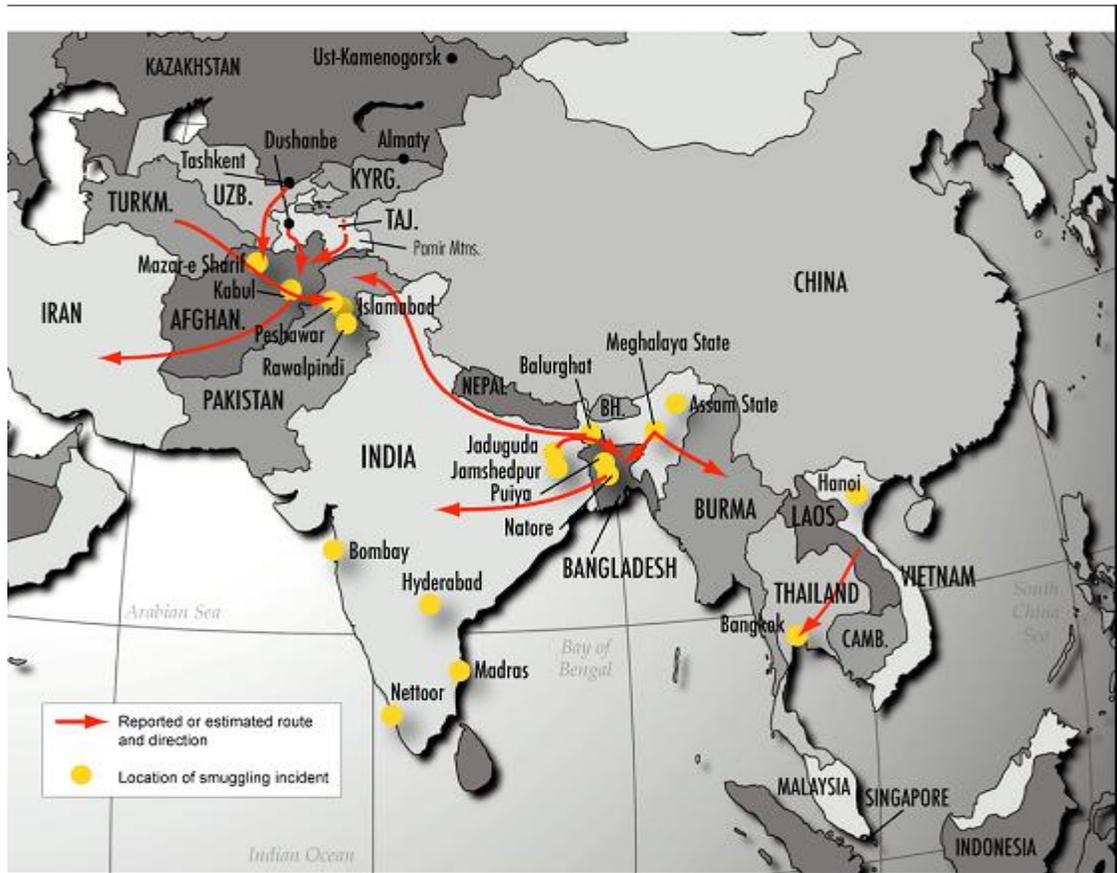


Figure 9

The straits themselves pose a significant risk for both the flow of illicit materials and the possible interception by terrorists and organized criminals. The straits have been the site of several confirmed counterproliferation activities, including the interception of the BBC China

⁷⁰DEA Intelligence Brief “South East Asian Heroin Smuggling Methods: Containerized Cargo”, September 2001

with its load of uranium-enrichment equipment enroute from North Korea to Libya in 2003.

(See figure 10).

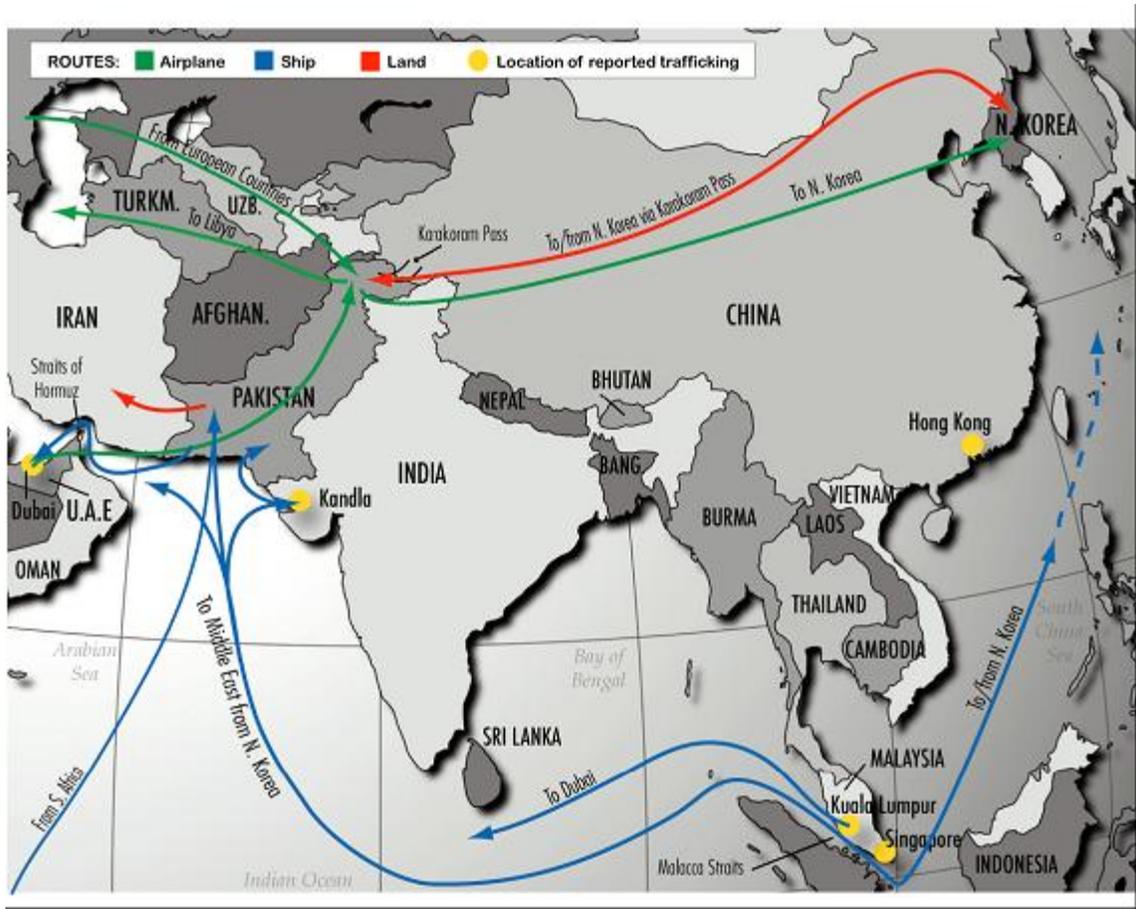


Figure 10

Additionally, the straits encounter hundreds of reports of maritime piracy annually. Potential terrorist-pirate networks could stop the flow of a third of the global shipping by downing a supertanker in the straits, or could capture a cargo ship transporting radioactive waste. An additional threat is in the potential of traffickers using human carriers to transport CBNR materials through airlines. The DEA has reported an increase for drug trafficking via airlines using human carriers or “mules” to deliver drugs in the island nations of South East Asia.⁷¹

⁷¹DEA Intelligence Brief, “The Pacific Islands Region”, August 2004

Many of these island nations serve as shipping points directly to the United States. Each of these reports demonstrates the need for greater interagency cooperation and information sharing.

Enlargement and Refinement of Recommended Model to World

Expanding the template to look at global networks requires RCCs to share the information gained from their regional templates. This information would allow the RCCs the flexibility of coordinating their counterproliferation efforts, and prevent proliferators from taking advantage of the “seams” created between the artificial RCC boundaries. As an example for PACOM, the next possible area for acquisition of biological weapons stocks might come from the former Soviet Union. Following the collapse of the Soviet Union, a large number of biological facilities closed or simply ran out of funding to continue their research. Many of the facilities are loosely guarded, and it is difficult to verify full accountability of their materials. Additionally, there is the concern for knowledgeable managers and scientists to develop these materials. Many of these technicians are jobless and easy prey for terrorist/ criminal networks. In June 2003, Thai police working with American authorities recovered an undisclosed amount of Cesium 137 from a former school principal in Bangkok. The man was attempting to sell the highly radioactive material to what he thought was an active proliferation network in Thailand.⁷² The fact that the man attempted to gain \$240,000 from the sale was not as disconcerting as the original source of the material. The Cesium came from the former Soviet Union, and transported through Laos into Thailand several years before. The networks that allow movement of such materials on a global scale can easily adjust to transport equipment and expertise as well. The interactions that expand to encompass the region can further expand to tie into global networks. The original template remains valid for this purpose. Using the same categories identified in the original template, we can now look at possible expertise with greater trust relationships between the terrorists and the

⁷²“Radioactive Cesium Seizure in Thailand: Riddled with Uncertainties” CNS report, July 17, 2003

experts. Additionally, we will be able to identify relationships between terrorists and criminal networks with greater duration. The assets available through international agencies provide greater fidelity and increased comprehension of the overall scale of the networks.

CONCLUSION

OPTIONS FOR DEALING WITH THE IDENTIFIED NODES

The question of what do we do once we have identified possible nodes and chokepoints poses many challenges. The military is not solely responsible for the allocation of resources for monitoring and further refinement of information gathering. The US government and particularly its intelligence agencies cannot be everywhere at once. Therefore, we should continue to develop multi-national interagency task forces for this purpose. A May 2001 CSIS report on combating CBRN terrorism identified the need for a joint multi-agency and multinational forces that can rapidly react to and counter the threat of CBRN terrorists.⁷³ The report went so far as to suggest the use of preemption in the face of impending WMD attacks, and implementation within 180 days of the publishing of the report to “Conduct interagency exercises of preemption capabilities.”⁷⁴ The 2006 QDR recommends the establishment of a Joint force to address reaction and interdiction.⁷⁵

Interagency Requirements and Challenges

There is no open-source database of common interagency data. As was pointed out earlier, each agency reports data in different ways, with necessarily different foci. The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) identified many of the glaring problems existing within the US intelligence community, and is meant to serve as a means

⁷³ CSIS report, Combating Chemical, Biological, Radiological, and Nuclear Terrorism: A Comprehensive Study, Cilluffo, Cardash, & Lederman, May 2001

⁷⁴IBID, p.26

⁷⁵“Ability to Wage ‘Long War’ Is Key to Pentagon Plan”, Tyson, February 4, 2006

of addressing the interagency shortcomings. The US Government has identified the need for a central hub to synchronize and direct global counterproliferation efforts. The IRTPA established a Director of National Intelligence to act as the as well as requiring the establishment of the National Counter Terrorism Center (NCTC), the National Counter Proliferation Center (NCPC), and other National Intelligence Centers. The IRTPA required the establishment of the NCPC within 18 months of the enactment of the National Security Intelligence Reform Act of 2004. The NCPC was officially established on 21 December 2005. The IRTPA further identified the following missions and objectives for the NCPC, “

“(1) Establishing a primary organization within the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States pertaining to proliferation.

“(2) Ensuring that appropriate agencies have full access to and receive all-source intelligence support needed to execute their counter proliferation plans or activities, and perform independent, alternative analyses.

“(3) Establishing a central repository on known and suspected proliferation activities, including the goals, strategies, capabilities, networks, and any individuals, groups, or entities engaged in proliferation.

“(4) Disseminating proliferation information, including proliferation threats and analyses, to the President, to the appropriate departments and agencies, and to the appropriate committees of Congress.

“(5) Conducting net assessments and warnings about the proliferation of weapons of mass destruction, their delivery systems, and related materials and technologies.

“(6) Coordinating counter proliferation plans and activities of the various departments and agencies of the United States Government to prevent and halt the proliferation of weapons of mass destruction, their delivery systems, and related materials and technologies.

“(7) Conducting strategic operational counter proliferation planning for the United States Government to prevent and halt the proliferation of weapons of mass destruction, their delivery systems, and related materials and technologies.”⁷⁶

These requirements encourage the active tracking of potential networks, and the open sharing of information between agencies. Understandably, the creation of these templates is a daunting task. As was stated in the introduction, many agencies have developed their own individual templates. However, a common template is needed within the military that can translate the data from these individual efforts and apply them to proactive counterproliferation efforts. The DNI and the NCPC have no directive authority over military intelligence assets. Additionally, the Department of Defense identified STRATCOM as the lead command for counterproliferation, but has also given counterproliferation responsibilities to the Defense Threat Reduction Agency. This dizzying array of agencies and responsibilities leads to greater difficulty in information sharing. Figure 11 demonstrates the command and control relationships associated with these directives. The regional combatant commanders can act as a common starting point and liaison for coordinating these efforts.

⁷⁶IRTPA, p.39

Hierarchy for CP Efforts

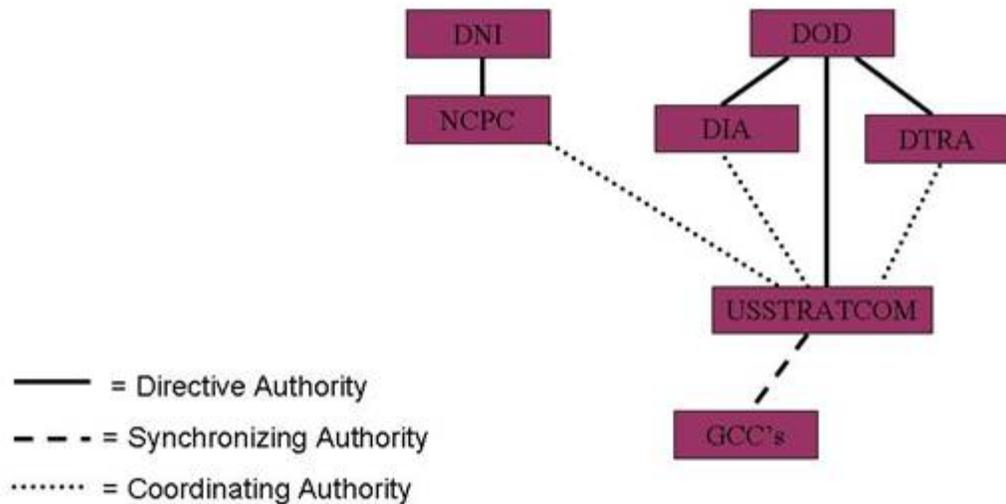


Figure 11

Multinational cooperation requirements

Actively engaging other nations to encourage their participation in supporting counterproliferation is the responsibility of all US government agencies. However, this engagement is not without its challenges. Many of the governments we need to engage are weak or failing. The perception often is that the governments themselves that are complicit in illicit activities. “it is the governments themselves that are the criminal enterprises, so mired in corruption that entire countries could be indicted under U.S. antiracketeering laws. Together, they help make up a criminal economy that, like a parallel universe, runs beneath the legitimate world of commerce. This global shadow economy--of dirty money, criminal enterprises, and black markets--has annual revenues of up to \$2 trillion, according to U.N. estimates, larger than the gross domestic product of all but a handful of countries...But taking on a worldwide plague of

crime and corruption might be more than the public bargained for.”⁷⁷ Another challenge is the direction that the host nation government perceives as critical versus that of the individual agencies representing the US. For example, DEA efforts naturally focus on the problem of interdicting and reducing the overall amount of illegal drugs produced and smuggled out of South East Asia. Additionally, they attempt to assist partner nations in reducing the trafficking of drugs within the individual nations’ borders. This is an important distinction, since U.S. interests do not always match the primary concerns of the individual nations. In the example case of Thailand, the DEA wishes to address and reduce the flow of heroin and poppy-related drugs present within the Golden Triangle in order to prevent their eventual smuggling to the US. However, the Thais are more concerned with the presence of methamphetamine-related drugs that pose a dramatically increasing domestic issue to Thailand. In the example of the DEA, we see that the model must accomplish the task of reducing drugs in both Thailand (methamphetamines) and the US (heroin). The model addresses both interdiction efforts by first identifying the nature of the products and their users, then proceeds back to the production methods, and finally focuses on the markets/ methods of transfer or trafficking. For the Thais, the key area of emphasis is on the reduction of the production labs, since they are mostly domestic. For the DEA, the key area of emphasis is on the reduction of flow from Burma, Cambodia, China, and Laos, through and out of Thailand to the US. However, if we continue to emphasize the necessity of gathering information, and coordinating all interdiction efforts as vital to both counterproliferation and counterterrorist efforts, we can continue to make progress.

Individual agent requirements

The research conducted for developing the example template presented in this paper is a start point. The next stage after the development of the template is the allocation of intelligence

⁷⁷ “Paying for Terror”, Kaplan, US News and World Report, December 5, 2005

resources to verify the applicability of the template. Staff members can use this template to develop a verification plan. This plan can include a task list for individual agents. It could be as simple as asking representatives from foreign companies, “Can you create or acquire this piece of equipment/ stock/ sample? If so, has anyone else approached you to do this?” This list of questions and areas of concern can then be addressed over a greater duration, with heightened areas of concern being addressed first. The RCCs have additional responsibilities as the regional WMD information source gatherers. This includes granting DIRLAUTH between country SAOs and DAOs and acting as the coordinator for interagency efforts.

Summary

The model developed in this study is one small part of the knowledge base required for an overall ONA necessary in developing regional campaign plans and global strategies for counterproliferation efforts. Perhaps the greatest value gained from this paper is not the system or template that is developed, but the advocacy of an interagency process that promotes the gathering and sharing of existing information, and providing a central point of analysis to be used in focused application of resources for the counterproliferation effort at the theater level. One of the greatest shortcomings identified during the research of this monograph was the lack of a coherent strategy for counterproliferation within the DOD. The DOD identified USSTRATCOM on January 6, 2006 as the lead agency for synchronizing counterproliferation efforts within the DOD,⁷⁸ but has not yet released a strategy for the geographic combatant commanders as a base document for development of regional campaign plans. Developing a campaign plan for addressing counterproliferation efforts within a RCC’s AOR requires an understanding of and matching a system of systems approach against the complex systems in place within the area. The identification of networks, nodes, and chokepoints within SEA is itself merely a system

⁷⁸USSTRATCOM News release, ‘U.S. Strategic Command Center for Combating WMD achieves IOC’ http://www.stratcom.mil/News/WMD_IOC.html

within the overall counterproliferation system. Identification enables RCCs flexibility in proper allocation of resources towards monitoring, interdicting, preventing, and refinement/ contingency identification of WMD.

BIBLIOGRAPHY

- Abuza, Zachary. "Terrorism in Southeast Asia: Keeping Al-Qaeda at Bay" *Terrorism Monitor*. The Jamestown Foundation Volume 2, Issue 9 (May 06, 2004)
- Allison, Graham. *Nuclear Terrorism* 2004. Times Books, New York
- Andersen, Bedeski, Darnosumarto. "Small Arms Trade and Proliferation in East Asia: Southeast Asia and the Russian Far East" Working Paper No.24, Institute of International Relations, University of British Columbia (September 1998)
- Arquilla, John & Ronfeldt, David. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA, RAND, 2001.
- Andreaoni, Alessandro & Ferguson, Charles. "Radioactive Cesium Seizure in Thailand: Riddled with Uncertainties". Monterey, CA, Center for Nonproliferation Studies, July 17, 2003 available online at <http://cns.miis.edu/pubs/week/030717.htm>, last retrieved March 20, 2006
- Baker, Richard ed. *Nuclear Terrorism*. Hauppauge, New York, Novinka Books, 2002.
- Bangkok Post, "Probe Urged Into All Violent 'Drug' Deaths". Summary of the News: February 9 to February 15, 2003, Bangkok Post, February, 16, 2003 available online at <http://archives.mybangkokpost.com>, last retrieved March 20, 2006
- Barrows, Kucik, Skimmyhorn, & Straigis, "A Systems Analysis of the A.Q. Khan Network" Social Science Seminar Presentation for the Center for International Security and Cooperation (CISAC), Reuben W. Hills Conference Room, East 207, Encina Hall, Stanford University, presented December 8, 2005, available online at http://iis-db.stanford.edu/evnts/4290/Khan_Main_Paper.pdf, last retrieved March 28, 2006
- Blussé, Leonard, Leiden University "Changes of Regime and Colonial State Formation in the Malay Archipelago, 1780-1830." Asia Research Institute, May 2005
- Burnett, John. *Dangerous Waters: Modern Piracy and Terror on the High Seas*. New York Dutton, 2002.
- Centers for Disease Control and Prevention (CDC), United States Department of Health and Human Services, CDC websites: "Cases of Influenza A (H5N1)---Thailand, 2004", MMWR Weekly, February 13, 2004, www.cdc.gov/mmwr/preview/mmwrhtml/mm5305a2.htm; "Avian Influenza: Current Situation", www.cdc.gov/avian/outbreaks/current.htm; "Health Information for Travelers to Countries in Southeast Asia", www.cdc.gov/travel/seasia.htm#diseases, all last retrieved March 24, 2006
- Chalk, Peter. "Light Arms Trading in SE Asia". *Jane's Intelligence Review*, March 1, 2001
- Chanlet-Avery, Emma. *Thailand: Background and U.S. Relations*. Washington DC, CRS, The Library of Congress, January 13, 2005
- Chomsky, Noam. *Pirates and Emperors, Old and New: International Terrorism in the Real World*. Cambridge, MA, South End Press, 2002.
- Cilluffo, Cardash, & Lederman. *Combatting Chemical, Biological, Radiological, and Nuclear Terrorism: A Comprehensive Strategy*. Washington DC, The CSIS Press, 2001.

- Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. *Report to the President of the United States*, Washington DC, US Government Printing Office, March 31, 2005
- Corrigan, Michael. *A Month in Money Laundering*. London, UK, Deloitte & Touche LLP, December 2004
- Crossette, Barbara. "U.N. Warns That Trafficking In Human Beings Is Growing." *The New York Times*, (June 25, 2000), p. 9
- Davis, Antony. "Bangkok as Crime Central" *AsiaWeek.com*, Vol. 26, No. 40 (October 13, 2000). Available online at www.pathfinder.com/asiaweek/magazine/2000/1013/nat.thailand.html , last retrieved on March 20, 2006
- DEA-04012, "Drug Intelligence Brief, The Pacific Islands Region". Alexandria, VA, Drug Enforcement Agency, *Microgram Bulletin*, August 2004
- DEA-02026, Drug Intelligence Brief, "Anatomy of a Southeast Asian Heroin Conspiracy". Alexandria, VA, Drug Enforcement Agency, *Microgram Bulletin*, August 2002
- DEA-03052, Drug Intelligence Brief, "Methamphetamine: The Current Threat in East Asia and the Pacific Rim". Alexandria, VA, Drug Enforcement Agency, *Microgram Bulletin*, September 2003
- DEA-01022, "Drug Intelligence Brief, Southeast Asian Heroin Smuggling Methods: Containerized Cargo". Alexandria, VA, Drug Enforcement Agency, *Microgram Bulletin*, September 2001
- Director of the Office of National Intelligence, *The National Intelligence Strategy for the United States of America*. Washington DC, US Government Printing Office, October 2005
- Dorner, Dietrich. *The Logic of Failure*. New York, Metropolitan Books, 1996.
- Emmers, Ralf, IDSS. "The Threat of Transnational Crime in Southeast Asia: Drug Trafficking, Human Smuggling and Trafficking, and Sea Piracy" UNISCI Discussion Papers. UNISCI, Spain (May 2003)
- FBI Intelligence Website, <http://www.fbi.gov/intelligence/process.htm>, last retrieved March 20, 2006.
- FBI Organized Crime Website, <http://www.fbi.gov/hq/cid/orgcrime/aace/asiancrim>, last retrieved March 20, 2006.
- Forum for Nuclear Cooperation in Asia. *FNCA Consolidated Report on RWM (Thailand)*. Sydney, Australia, FNCA, 2002
- Gilbert M, Chaitaweesub P, Parakamawongsa T, Premashtira S, Tiensin T, Kalpravidh W, et al. "Free-grazing ducks and highly pathogenic avian influenza, Thailand". *Emerging Infectious Diseases* (vol.12, no. 02), February 5, 2006, available at <http://www.cdc.gov/ncidod/EID/vol12no02/05-0640.htm> , last retrieved March 20, 2006
- Human Trafficking.org provides statistics and regional indices of levels of trafficking. They are available online at www.humantrafficking.org, last retrieved March 20, 2006
- Institute for National Strategic Studies. *Strategic Assessment 1999: Priorities for a Turbulent World*. Washington DC, National Defense University, 1999.

- IAEA internet data bases, <http://www.iaea.org/DataCenter/datasystems.html> , last retrieved March 20, 2006
- IAEA, Information Circular, *INFCIRC/254/Rev.6/Part 2: Communications Received from Certain Member States Regarding Guidelines for Transfers of Nuclear-related Dual-use Equipment, Materials, Software and Related Technology*. New York, 2005
- International Chamber of Commerce, International Maritime Bureau maintains a database on reports of piracy, they are available online at www.icc-ccs.org/imb/dbsearch.php, last retrieved January 10, 2006
- IIPA, *International Intellectual Property Alliance 2003 Special 301 Report: Thailand*. Washington DC, February 14, 2003 Other special reports available at the IIPA website, www.iipa.com/countryreports.html, last retrieved March 20, 2006
- Interpol International Group of Experts on Corruption website, available at <http://www.interpol.int/Public/Corruption/IGEC/Mission/Default.asp> , last retrieved on March 28, 2006
- International Organization for Standardization (ISO), website available at <http://www.iso.org/iso/en/ISOOnline.frontpage> , last retrieved March 20, 2006
- Kaplan, David. "Paying for Terror: How Jihadist Groups Are Using Organized-Crime Tactics--and Profits--to Finance Attacks on Targets Around the Globe" US News and World Report, (December 5, 2005).
- Karasik, Theodore. *Toxic Warfare*. Santa Monica, CA, Rand, 2002
- Knobler, Mahmoud & Pray eds. *Biological Threats and Terrorism: Assessing the Science and Response Capabilities*. Washington DC, National Academy Press, 2002.
- Lee, Dr. Henry C. *Cracking Cases*. Amherst, NY, Prometheus Books, 2002.
- Leventhal & Alexander eds. *Nuclear Terrorism: Defining the Threat*. Mclean VA, Pergamon-Brassey's, 1986.
- Mukundan & Richardson. "Political and Security Outlook 2004: Maritime Terrorism and Piracy" Trends in Southeast Asia Series: 3, Institute of Southeast Asian Studies, Singapore (January 2004)
- Neuaman, Zohar. "Thailand's South Embroiled in Sectarian Conflict", JINSA Online, January 10, 2005. Available at www.jinsa.org, last retrieved March 20, 2006
- Newhouse, John ed. *Assessing the Threats: Instabilities and Deadly Weapons*. Washington DC, Center for Defense Information, 2002
- Office of the President of the United States, *National Strategy to Combat Weapons of Mass Destruction*, Washington DC, US Government Printing Office, December 2002
- Office of the President of the United States, *National Security Strategy of the United States*, Washington DC, US Government Printing Office, September 2002
- Ogilvie-White, Tanya. "Preventing Nuclear and Radiological Terrorism: Nuclear Security in Southeast Asia" University of Canterbury, The Australian Centre for Peace and Conflict Studies Occasional Paper Series, 2004
- Parritt, Brian ed. *Violence at Sea: A Review of Terrorism, Acts of War and Piracy, and Countermeasures to Prevent Terrorism*. Paris, ICC Publishing S.A, 1986.
- "Piracy." The Economist. (December 16, 1999): pp. 91-93

- Prosser, Andrew. "Nuclear Trafficking Routes: Dangerous Trends in Southern Asia." Center for Defense Information. (22 November 2002)
- Ramsay, Ambassador William C., *ASIAN OIL: Current Trends, Outlook and Issues Presentation*, Deputy Executive Director, International Energy Agency, Paris to the Roundtable Conference on Regional Cooperation: Key to Energy Security New Delhi, 6 January, 2005
- Raymond, Catherine Zara. "Maritime Terrorism in Southeast Asia: A Risk Assessment" Singapore, Institute of Defence and Strategic Studies, March 2005
- Royal Kingdom of Thailand, *Executive Summary of Thailand National Chemicals Management Profile*. Bangkok, Thailand, 1998
- Schmid, Alex P. "The Links between Transnational Organized Crime and Terrorist Crimes." *Transnational Organized Crime*. 2 (no. 4, Winter, 1996): 40-82.
- Schweitzer, Glenn. *Superterrorism: Assassins, Mobsters, and Weapons of Mass Destruction*. New York, Plenum Trade, 1998.
- Small Arms Survey website tracks the global reported legal and illegal trafficking in small arms, www.smallarmssurvey.org, last retrieved March 20, 2006
- Sryotha, Pirat. *Near Surface Radioactive Waste Disposal: Safety Assessment of Reference Designs for Low and Intermediate Level Radioactive Waste Repositories*. Bangkok, Thailand, OAEP, December 5, 2000.
- Tenet, George, Director of Central Intelligence. "The Worldwide Threat in 2000: Global Realities of Our National Security." Testimony before the Committee on Foreign Relations, U.S. Senate, March 21, 2000, p. 7
- Towell, Pat. "Russian Nuclear Material Vulnerable to Theft." Congressional Quarterly Weekly Report. February 5, 2000, p. 265
- "Transnational Security Threats In The Asia-Pacific Region", 2002 Pacific Symposium Highlights
- Transparency International Corruption Indices website containing data on levels of perceived corruption, http://www.transparency.org/regional_pages/asia_pacific, last retrieved on March 20, 2006.
- Turabian, Kate L. *A Manual for Writers of Term Papers, Theses, and Dissertations*. 6th ed. Chicago: University of Chicago Press, 1996.
- Tyson, Ann Scott. "Ability to Wage 'Long War' Is Key to Pentagon Plan", Washington Post, (February 4, 2006)
- Umbach, Frank, German Council on Foreign Relations. "International Cooperation and Its New Challenges in Fighting the New Security Threats." Fritz Thyssen Foundation, at the Research Institute of the German Council on Foreign Relations (DGAP), Berlin
- United Nations Office on Drugs and Crime website, www.unodc.org, last retrieved March 20, 2006.
- United Nations Inter-Agency Project on Human Trafficking in the Greater Mekong Sub-region (UNIAP). *Trafficking In Persons (TIP) 2004 Report: Thailand*. New York, UN, 2004.
- United Nations World Health Organization (WHO) Avian Influenza websites: Avian Influenza A(H5N1)- Update 17: Situation (human) in Thailand and (poultry) in China, Indonesia

and Worldwide, www.who.int/csr/don/2004_02_04/en/ ; Avian Influenza- Situation in Thailand, 28 September 2004, www.who.int/csr/don/2004_09_28a/en/index.html ; Avian Influenza- Situation in Thailand, Indonesia- Update 36 website, www.who.int/csr/don/2005_10_24/en/index.html

United States Army, FM 7-100. St. Louis, MO, USAPA, 2003

United States Congress, Public Law 108-458. *Intelligence Reform and Terrorist Prevention Act of 2004*. Washington DC, US Government Printing Office, December 17, 2004

United States Congress Committee on International Relations, Oversight Plan of the Committee, 109th Congress (Adopted February 9, 2005)

United States Congress Committee on Governmental Affairs United States Senate, Hearing Before the Financial Management, the Budget, and International Security Subcommittee, *International Smuggling Networks: Weapons of Mass Destruction Counterproliferation Initiatives*. Washington DC, US Government Printing Office, June 23, 2004

United States Department of Defense Joint Electronic Library, *DOD Dictionary of Military Terms and Acronyms*. www.dtic.mil/doctrine/jel/doddict/acronym_index.html, last retrieved March 20, 2006.

United States Department of Defense Joint Electronic Library, *JP 2-01.3*. www.dtic.mil/doctrine/jel/, last retrieved March 20, 2006.

United States Department of Defense, *National Defense Strategy of the United States*, Washington DC, US Government Printing Office, March 2005

United States Department of Defense, USTRANSCOM News website, “U.S. Strategic Command Center for Combating WMD achieves IOC”, http://www.stratcom.mil/News/WMD_IOC.html, last retrieved March 20, 2006

United States Department of State, Bureau for International Narcotics and Law Enforcement Affairs. *International Narcotics Control Strategy Report*. March 2000. Washington DC

United States Department of State, Bureau of International Security and Nonproliferation PSI FAQs website, <http://www.state.gov/t/isn/rls/fs/46839.htm>, last retrieved March 28, 2006.

United States Department of State, Bureau of International Security and Nonproliferation Terrorism Threat website, <http://www.state.gov/t/isn/wmd/c16583.htm> , last retrieved March 20, 2006.

United States Department of State, Bureau of International Security and Nonproliferation website, Nonproliferation Regimes Fact Sheets, <http://www.state.gov/t/isn/c10528.htm>, last retrieved March 20, 2006.

University of Texas Library, Perry Castaneda Map Collection, background maps for template, available online at www.lib.utexas.edu/maps/thailand.html, last retrieved on March 20, 2006

Wassenaar Arrangement website, www.wassenaar.org, last retrieved March 20, 2006.

Whine, Michael. "Cyberspace-A New Medium for Communication, Command and Control by Extremists." *Studies in Conflict and Terrorism*. RAND. 22 (no. 3, August 1999): 231-246.

Yoshihiko Yamada, Director, Department of Marine Affairs. "Defending Asian Seas from Marauding by Pirates" *Japanese Dynamism* #6. The Nippon Foundation. (March 2004)