TRANSGOVERNMENTAL NETWORKS AS A TOOL TO COMBAT TERRORISM:

HOW ICE ATTACHÉS OPERATE OVESEAS TO COMBAT TERRORIST TRAVEL

By

KEITH COZINE

A Dissertation submitted to the

Graduate School-Newark

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Global Affairs

written under the direction of

Dr. Norman Samuels Ph.D: Professor and Provost Emeritus

and approved by

_____

_____

_____

_____

Newark, New Jersey

January 2010

ABSTRACT OF THE DISSERTATION

TRANSGOVERNMENTAL NETWORKS AS A TOOL TO COMBAT TERRORISM:

HOW ICE ATTACHÉS OPERATE OVESEAS TO COMBAT TERRORIST

TRAVEL

By KEITH COZINE

Dissertation Director:

Dr. Norman Samuels Ph.D.: Professor and Provost Emeritus

Globalization has led to a shift in the perceived threat to security from states to trans-border issues such as financial collapse, global warming, pandemics and threats from a variety of non-state actors. As a result of the terrorist attacks on New York, Bali, Madrid, London and Mumbai; international terrorism has become one of the most highly visible of these new threats. One mechanism of global governance employed to combat this threat is the use of transgovernmental networks comprised of government officials from various nations, forming both formal and informal global networks that reach out to their foreign counterparts. These networks are the foundation of a strategy of confronting "networks of terror with networks against terror." This research seeks to understand how these networks operate to achieve their mission. The literature relating to transgovernmental networks and transnational advocacy networks (TANs) suggests that these two network types share numerous characteristics. These similarities led to the development of the hypothesis that transgovernmental networks operate to accomplish their missions in much the same way as TANs operate. To test this hypothesis, a single case study design was utilized to examine how one agency, U.S. Immigration and Customs Enforcement (ICE), utilizes its officers assigned to foreign jurisdictions as part of a transgovernmental network to combat terrorist travel. The research revealed that these officers are not only part of a transgovernmental network that operates to prevent terrorist travel, as well as other transnational crimes, in much the same way as TANs, but also mirrors the structure of the terrorist networks they are charged with combating. Furthermore, a foundation has been laid for continued investigative research of transgovernmental networks; while providing a potential blue print for a strategy of combating threats to global security with networks of government officials that are as fluid and effective as the groups that are posing these threats.

Preface

On September 11, 2001, I was working as an inspector for U.S Immigration and

Naturalization Service at Newark International Airport. That morning, I was assigned to

the International Arrivals Area of Terminal B. The far wall of the terminal was made up

of large windows that overlooked the runways and beyond that, the New York skyline. It

was through those windows and the various television monitors that were scattered

throughout the area that I watched in disbelief with my fellow inspectors, airline

representatives and passengers, who arrived to the United States just moments earlier, as

the events of that morning unfolded and the New York skyline changed forever.

In the months that followed, as more details about the attacks and those who

carried them emerged, my emotions changed from shock and anger to a sense of failure

and guilt. As an Immigration Inspector, I was entrusted to protect the citizens of the

United States from individuals like those terrorists who had carried out the September 11

attacks and I had failed. These emotions created these need for me to understand how

these terrorists were able to enter the United States and what steps could be taken to

prevent others like them from gaining entry into the United States in the future. My

original inquires into the topic were informal but rather than satisfying my appetite, it left

me wanting more. I knew I had to pursue my quest for knowledge in a more formal

manner.

When I completed my Master's degree in 1998, I had planned to return to school

to complete a doctorate as some point. What I lacked was both the opportunity and the

motivations. Now I had the motivation and in 2004, Rutgers University provided me the

opportunity. While studying within the Rutgers's Division of Global Affairs, I quickly

learned that terrorism was far from the only security threat facing the world. Those

threats that existed during the cold war remained and were now compounded by new

threats such as; violent and criminal non-state actors, global warming, financial collapse

and pandemics. I also discovered that these new threats were not just dealt with through

traditional means of international relations between states, but rather a wide array of tools

of global governance. As a government official who regularly interacted with officials

from other nations, it was the governance mechanism of transgovernmental networks that

I identified with most, and, despite the various other threats to security, terrorism as

remained my primary interest. It is the merging of these two interests that has led to this

dissertation.

Despite my name appearing on the title page, I am far from the only contributor to

this project. Over the past five plus years I have had the pleasure of working with and

studying with some wonderful people. Through their support, their knowledge, expertise

or their encouragement, they too have made significant contributions to this dissertation.

In pursuit of my research special recognition needs to be given to both current and former

members of Rutgers University's Division of Global Affairs. Dr. Rey Koslowski, who

served as my faculty advisor and mentor when I first return to Rutgers in 2004, whose

knowledge in the areas of immigration, governance and border security was the

foundation on which I built my studies. My dissertation advisor, Dr. Norman Samuels,

whose knowledge in the areas of terrorism and intelligence were invaluable; and who was

able to guide me through storms while helping me stay focused towards my goal. My

dissertation committee; Dr Yale H. Ferguson, Dr. Leslie Kennedy and Prof. Richard

taught me more could be accomplished with a smile and a kind word then ever could with

a badge and a gun. She was the inspiration for this dissertation.

Dedication

For Nancy, Jack and Delaney, you are a constant reminder of what is really important.

Table of Contents

INTRODUCTION:

Since the Treaties of Westphalia marked the birth pangs of the state system, the primary perceived security threat to states has come from other states. With globalization, this security threat has shifted from states to trans-border issues such as financial collapse and global warming, pandemics and threats from a variety of non-state actors. The barriers lifted by the end of the Cold War and the openness of globalization has created an environment in which the illegal trade of drugs, arms, intellectual property rights and money is booming, and has allowed for terrorist organizations to operate globally as well. Governments, in an attempt to control these illicit markets and harmful organizations, are pitted not against the armies and navies of another nations, but stateless and resourceful networks that have no central government that can be engaged (Naim 2003: 29). As a result of the attacks on New York, Bali, Madrid, London and Mumbai, international terrorism has become a highly visible new threat.

The Threat of Non-state Actors to Security

The globalized world seems to continually shrink to a point where time and space are less and less important. Advancement and innovation in shipping allow for goods to be loaded onto ships, cross vast oceans, and then be unloaded and delivered to markets in days. Air travel, which not long ago was available only to the elite, is now affordable to all but the world's poorest. A phone call can be made across the globe for pennies a minute, and information travels across borders in an electronic form of zeros and ones.

This has facilitated the advance of a global economy that profoundly affects the economic health of individual states. The interconnectivity of these individual states' economies to those of other states has created an environment where small changes can have a ripple effect around the globe. The use military power against another state may no longer be the practical option if these two opponents are both militarily and economically powerful. The cost of war can become a high one, not just in the cost of lives but also the harm done to both nations' economy, as well as the global economy. Inter-state military conflict would have a devastating effect on not just the parties involved, but also all their trading partners. This environment has led to a decrease in inter-state wars; however the decrease has coincided with a rise in intra-state conflict and non-state actors who use violence as means to achieve their goals.

This current era of globalization has been decades in the making. However, few argue with the notion that the end of the Cold War and East-West divide was a catalyst, speeding up the process and bringing its benefits to the world as a whole. The end of the Cold War brought feelings of jubilation and hope to the world. Many saw this as a new opportunity to usher in a prolonged period of peace. These hopes were quickly dashed as conflict moved from inter-state conflict to intra-state conflict. Today, most wars are fought either within states or between state and non-state actors (Carment 2003: 208). Ethnic, national and religious military conflict within countries continues to grow, and often threatens to or actually spills across borders. In extreme cases, this has led to state failure, which has not only threatened regional security and stability but global security as well. This explosion of intra-state conflicts has coincided with the growth of non-state

actors, such as international criminal organizations and international terrorist organizations who use violence in an attempt to achieve their goals.

The globalization of non-state actors, terrorist organizations in particular, who use violence to promote their goals, have become a significant new security threat for the 21st century. The advancements in international travel, shipping and communication that are responsible for the globalized and interdependent world have coincided with the internationalization of terrorist organizations. An organization such as al-Qaeda may have relied on states such as Afghanistan and western Pakistan to provide a safe haven, but the organization, its members, its influence, its ideology and its reach were global in nature and without ties to a particular state. This globalization of terrorist organizations has required terrorists to "travel abroad to foster ties with potential allies, to conduct training exercises, to raise money and attract political support for their cause" (Smith 2001: 1). Most importantly, as demonstrated by the September 11 attacks, terrorists must travel to carry out acts. Today's global economy has made this travel easier for the terrorist. The result of increasing economic interdependency of states is a diminishing of borders as a new openness develops in order to facilitate international trade and travel. Terrorists have been able to take advantage of this openness to move around the world to achieve their goals.

Compounding this threat from international terrorist organizations is that the members do not identify themselves by the country listed in their passport and in many cases have passports from more than one country. Their allegiance is to their cause, not to any one nation (Naim 2003: 35). Terrorism is not the exclusive tool of one ethnic group or even one religion; rather, it has been an instrument of choice for a variety of

movements around the world. It is those organizations, however, that carry out their activities based on an extremist interpretation of the Koran and the teachings of the prophet Mohammed, and the acceptance of the use of violence as a tool, that are deemed the primary threat to the West (Rees 2006: 54). It is this extremist version of Islam, which is labeled the "global Salafi jihad movement" (Sageman 2004) that has also united the followers of this movement together on a global scale. But these organizations are not the only threat to security.

The openness and interconnectivity of globalization has created an environment that has also allowed transnational crime to flourish. Advancements in technology and transportation that facilitate trade and travel have not been exclusively to the benefit of legitimate transnational actors; they have also benefited international criminals and their organizations (Rees 2006: 7). The members of these organizations might have a prerequisite of belonging to a particular ethnic group, though loyalties are linked to the organization and to profits rather than nationality. While religious or political goals drive most terrorist organizations, criminal organizations are driven by the promise of enormous financial gains. Tragically, profit is no less a motivation for murder, mayhem and creating a global threat to security than political or religious zeal (Naim 2003: 29). This phenomenon of the internationalization of criminal organizations has coincided with the internationalization of terrorist organizations based on religious ideology like the one that carried out the September 11 attacks. However, because of these attacks and others like it, terrorism has remained a more visible security threat presented by non-state actors than international criminal organization.

A New Strategy

The shrinking of time and space resulting from globalization has allowed non-state actors who threaten global security to expand their areas of operation and influence, and carry out activities with a speed and effectiveness not seen before in history. As a result, law enforcement and intelligence agencies tasked with combating these activities must find new ways to share information and intelligence, and coordinate investigations with their foreign counterparts (Rees 2006: 22). These new approaches must allow them to work at the same speed and efficiency as their targets. The traditional means of international interaction, like diplomacy and treaties, seem less effective in dealing with today's threats to international security as they were in dealing with past threats.

Today's threats require the development of relationships between similar agencies across governments, rather than dealing exclusively through foreign ministries (Slaughter 2004: 55). Just as terrorists, arms dealers, money launderers, drug dealers and human smugglers all operate through global networks, increasing so do governments. They operate as transgovernmental networks comprised of government officials from various nations, forming both formal and informal global networks that reach out to their foreign counterparts to help address the problems that arise when national actors or issues spill beyond their borders (Slaughter 2004: 1). It is these types of transgovernmental networks that are behind the counter-terrorism strategy of confronting "networks of terror with networks against terror" (Bendiek 2006: 5); which may also be adapted to combat other networks of non-state actors who threaten global security.

The value of transgovernmental relationships of this nature is not new in global governance literature (see Keohane and Nye 1974); however, as transgovernmental

networks have emerged as a key feature of global governance in the 21st century, so to their presence in the global governance literature (Slaughter 2004, Hajer and Versteeg 2005, Pawlak 2007, Slaughter and Zaring 2007). Interestingly, a blurring of boundaries between international and domestic arenas simultaneously occurred in various other social issues as well. As transgovernmental networks have grown in importance, so too has global civil society and the number of social movement organizations, especially transnational advocacy networks (TANs). As these organizations have grown, so too has the literature about them (Keck and Sikkink 1998, Tarrow 2002, Kaldor et al 2003, Schock 2005).

Just as with transnational crime and terrorism, many social and human rights issues spill beyond one nation's border and become global in scope. When this occurs, domestic actors must reach out to their foreign partners for assistance in effectively dealing with a problem that is no longer contained within just one country or when that country is unable or unwilling to address this problem. When this joint action by actors from various nations and locations occurs, transnational advocacy networks form. These networks are comprised of those relevant actors working globally on a particular issue, who bring together shared values, a common discourse, and a dense exchange of information and services (Keck and Sikkink 1998: 1-2). These networks are built on trust and cohesion in an attempt to serve as a structure for cooperation beyond political, social and cultural boundaries (Kaldor, Anheier and Glasius 2003:9-10). This results in fluid and open relationships among committed and knowledgeable actors in specialized issue areas who operate through transnational networks to address global problems (Keck and

Sikkink 1998: 8). Having such characteristics, TANs may be the best model of transgovernmental networks to combat international terrorist and criminal organizations.

Exploring Transgovernmental Networks

In an attempt to deal with the thriving illegal trade in drugs, arms, and intellectual property rights, law enforcement and intelligence agencies are officially assigning their officers to foreign countries to work directly with their foreign counterparts. When, following the September 11 attacks, international terrorism became the overriding focus of many law enforcement agencies, the practice of assigning officers overseas provided a robust platform on which counterterrorism activities could be based (Winer 2004: 11). What this research project seeks to achieve is a better understanding of how these officers operate overseas in order to combat the threat to global security posed by transnational crime and international terrorism. In order to accomplish this goal, the qualitative research method of a single case study design was employed in order to explore the ways in which one agency, U.S. Immigration and Customs Enforcement (ICE), utilizes its officers assigned to foreign jurisdictions to combat a particular activity of international criminal and terrorist organizations — more specifically, these officers operate in foreign countries in order to combat terrorist travel.

One of the strategies adopted in an attempt to prevent terrorists from crossing borders has been to assign immigration officers from one country to work with foreign counterparts within their counterpart's jurisdiction (IOM 2003: 6-7). While trying to determine the success of this strategy would be a noble pursuit, there is no way to accurately measure success, only failure. Like members of a criminal organization, terrorists pursue their activities covertly because they want to avoid detection and

apprehension (Rees 2006: 7). There is only data available on those individuals who were identified as carrying out an activity relating to terrorism or who were detected in the process. Those individuals who were encountered and prevented from carrying out their activity would not be included if the true intention of their actions were never known. For this reason, this research explores only how officers from ICE who are assigned overseas operate to prevent terrorists from crossing borders to support, finance and carry out operations, not whether this strategy is actually successful. I will accomplish this goal by conducting a case study of how immigration officers operate within foreign jurisdictions.

Terrorist travel was chosen as the focus of this study for several reasons. First, when terrorists are prevented from traveling across borders, they are prevented from operating effectively (White House 2007: 16). Second, while terrorists crossing borders is not a crime in itself, terrorists often engage in various criminal activities in order to facilitate their border crossing. Third, regardless of their ideology, goals or modes of operation, international terrorists by definition must operate across borders (Smith 2001: 1); however, individuals connected to the global Salafi jihad movement will be the specific focus of this research as they are viewed as the group that currently poses the biggest threat to global security. Lastly, in the past, terrorists have utilized every method to clandestinely cross borders, including using fraudulent documents, stowing away on ships, and soliciting assistance from human smuggling organizations. Through the examination of terrorist travel strategies, we can better understand the strategies of not just terrorist but most other clandestine border crossers.

If international terrorists are required to cross borders, clearly immigration enforcement agencies are at the forefront of trying to combat this activity. Immigration

agencies, like many other regulatory and law enforcement agencies, have created their own international affairs arms that operate independent of their government's foreign ministries. They enter into agreements with similar agencies in foreign countries through memorandums of understanding and assigning officers to each others jurisdictions to work together to combat a shared problem. The belief is that these officers have specific expertise, skill-sets and share professional cultures with their foreign counterparts that do not exist within foreign ministries which allow them to work collectively on joint problems more effectively. In addition, foreign ministries usually operate using traditional diplomatic methods that may be too slow and cumbersome to combat certain problems in a globalized world. These are the theories behind the strategy of assigning immigration officers overseas directly with their foreign counterparts, resulting in faster communication and coordination of activities to better deal with the challenges of a globalized world. This research hopes to understand how this strategy is being carried out by these ICE officers assigned overseas, identify best practices that may be shared with other stakeholders, identify ways in which this strategy may be improved in order to better combat terrorist travel, and determine if this strategy can be applied to combat other transnational crimes.

The existing literature on transnational advocacy networks and transgovernmental networks suggests numerous similarities in the way these two types of networks operate to achieve their goals. This assertion is drawn from the belief that members of various global civil society organizations, such as transnational advocacy networks, interact with one another based on a shared set of norms and identification with one another concerning a particular issue that, in some instances, supersedes national identity

(Wapner 1997: 78). Officials assigned overseas who work with their foreign counterparts also share a set of norms, skill-sets and identities concerning a particular issue that supersedes identification with a particular nationality (Keohane and Nye 1974: 45). Members of global civil society organizations and immigration officers overseas both operate on the premise that the ability to rapidly share information, intelligence and best practices, as well as coordinate activities, is mutually beneficial to all organizations involved. These similarities have lead to the development of the hypothesis that *immigration officers assigned to foreign jurisdictions operate and interact with one another in an attempt to prevent terrorist travel in much the same way that members of transnational advocacy networks interact and operate in order to address their target problem.*

Answering the Research Question

In order to answer the research question and test this hypothesis, a qualitative research method — a case study — will be employed. The objective of this type of approach is to serve as the "defining description of the organization" and serve as an example of similar groups (McNabb 2004: 352). Given these criteria, a case study in order to determine how these officers, officially called ICE attachés, specifically operate within foreign jurisdictions to prevent terrorists from crossing borders to support, plan, finance, train, for and carry out attacks appears to be an appropriate method for exploring the larger question of how transgovernmental networks are utilized to combat crime that is international in scope.

The most common methods of data collection in a case study are interviews, observations and document analysis. Given that this research studies the behavior of

individuals, interviews seemed to be the best data collection method. The fact that ICE attachés are scattered across the globe makes conducting face-to-face or telephone interviews, the traditional means of conducting interviews in case studies are either impossible or impractical. For these reasons, the data collection method of questionnaires is utilized in lieu of the traditional interview types. The questionnaires, which were created, posted and filled out on the Internet, are designed to: 1) Help better understand the respondent's organization and working environment; 2) Understand how the respondent in his or her official capacity attempts to curtail, combat or prevent criminals, smuggled or trafficked people, terrorists and other individuals crossing international borders in violation of the laws of any nation-state; 3) Get the respondent's opinion on how, in his or her official capacity, he or she is utilized in an attempt to be more successful in these areas. It is the hope that by understanding how ICE attachés work to combat terrorist travel through these questionnaires, valuable insight will be obtained into how transgovernmental networks behave and provide a platform for further research into this type of global governance.

Organization of Research

A great deal of time and effort was spent in the construction of the questionnaire. First, the available literature and other material related to transnational networks, criminal and terrorist organizations, terrorist travel methods, and various border security initiatives was examined. Next, the proper means of data collection and analysis had to be researched in order to discover the best-suited methods for answering the research questions. Finally, the data needed to be collected, processed and analyzed. This literature and these steps need to be understood in order to appreciate the full scope of this research

and what its results mean to the body of literature related to transgovernmental networks. The following chapters attempt to accomplish this goal.

The first chapter illustrates the threats to security that result from the current era of globalization and the various tools of governance employed to address these threats. This chapter primarily explores the security threats posed by transnational criminal and terrorist organizations, while examining the literature on how transnational advocacy networks and transgovernmental networks work to tackle global problems. Particular attention is paid to horizontal networks between regulatory agencies that are located in the executive branch of government and the practice of assigning officers overseas to work directly with their foreign counterparts.

The second chapter will examine how terrorists cross international borders in order to plan, prepare, and carry out attacks through a historical examination of how terrorists with links to the global Salafi movement have crossed international borders in the past. It will first describe the various ways that individuals can cross international borders. Next, it will show how terrorists use a wide variety of sophisticated methods to take advantage of these ways of clandestinely crossing international borders while offering insight into possible future terrorist travel methods.

The September 11 attacks focused a spotlight on the importance of combating terrorist travel as a counterterrorism strategy. The third chapter will explore the various approaches and institutions that have attempted to curtail terrorists' ability to travel following these attacks, and realization that combating terrorist travel will require international cooperation. The chapter describes the mechanisms employed in governing this global problem, including: bilateral agreements, multilateral agreements,

international regimes, regional and international organizations, global civil society groups such as transnational advocacy networks, and transnational governmental networks.   It hopes to show how these mechanisms global governance are utilized with varying degrees of success.

Chapter four describes the methods that will be used to answer the research question and test the hypothesis. First, the chapter outlines the various pitfalls that often occur when undertaking research on topics related to terrorism, and then describes the research methods employed to answer the research questions and the limitations on this research. The reason for the use of a case study approach and the data collection of a questionnaire will be explained. This chapter will detail the goal and scope of each question while illustrating the means of data analysis. Finally, the procedure for using these data for testing the hypothesis will be outlined.

Chapter five presents the data collected as a result of the questionnaire. The responses for each question are reported and basic statistical analysis is used to determine how each question relates to the research question. While the majority of the questions are close-ended, the respondents are asked several open-ended questions or given the opportunity to provide additional information they felt may have been missed by the more structured close-ended question. When this additional information provides valuable insight into the way ICE attachés operate, it is reported.

In the sixth chapter, the responses to the questionnaire are analyzed as a whole in terms of what the data reveal about the research question. This analysis is applied to the hypothesis in order to determine if the initial assumption is true. Finally, the data are compared to the literature regarding transnational networks in order to identify best

practices and steps that could be taken in order to have ICE attachés operate more effectively.

The Conclusion will analyze and assess the mean and importance of this research to the study of transgovernmental networks and the larger body of work on global governance while point out the weakness and limitations of this research. It also will address what lessons can be drawn from governance practitioners who deal with global problems as a regular part of their duties. Finally, recommendations will be made as to how this research can be adapted to conduct further inquiries into transgovernmental networks.

If the hypothesis is proven true, then ICE attachés operate and interact with one another as a transgovernmental network in an attempt to prevent terrorist travel in much the same way that members of transnational advocacy networks interact and operate in order to address their target problem. To grasp the significance of this phenomenon to the greater body of work in the field of global governance, there must first be a solid understanding of the role of these networks as well as the networks they are trying to combat. The pages that follow this chapter hope to provide this understanding.

CHAPTER ONE: A WORLD OF NETWORKS

The Security Threat of Globalization:

The terrorist attacks of September 11th were the first exposure to the dark side of globalization for many of the world's citizens. Advancements in technology and communication allowed the images of the attacks to be broadcast around the globe as they unfolded. The continental United States, which had been insulated from a massive attack other than a nuclear barrage, was now vulnerable. The enemy was not a foreign state, but rather nineteen men, supported by a clandestine organization, motivated not by national allegiance, but rather religious ideology in a phenomenon that David Rapoport calls the "fourth wave of terrorism" (2001: 424).

In the weeks following the attacks on New York and Washington, it became evident exactly how the terrorists exploited the openness and interconnectivity of globalization to carry out their plot. Globalization had allowed a group of students from the Middle East, studying in Europe, to: travel to remote areas in Afghanistan; enter the United States and enroll in flight school; plan and coordinate their attacks; remain in contact with the plot's masterminds; and, have the fruits of their labor broadcast for all the world to see. It was a scenario that would play out again in Bali, Madrid, London, and other locations around the globe.

While September 11th brought the dark side of globalization to the forefront of the debate about the globalization phenomenon; non-state actors, operating across national

borders in violation of law and evading law enforcement efforts—those whom Peter

Andreas calls clandestine transnational actors (CTAs)—have long benefited from the

ever increasing openness and interconnectivity of the world (Andreas 2003: 78-79).

Their illicit trade of drugs, arms, intellectual property, people and money has been

booming for quite some time. Like international terrorist organizations, they are

networks of agile, stateless, resourceful actors, empowered by globalization. As in the

War on Terrorism, governments are confronting CTAs involved in these illicit trades in

what Naim calls the "Five Wars of Globalization" (2003: 29). These "wars" now shape

the world as much as wars between states once did. Until governments find new

strategies to wage these wars, they are doomed to lose them (Naim 2003: 29).

Governance of a Global Threat:

The Cold War presented clear threats to security. Following the end of the Cold

War, disaggregation continued, further extending the anarchical structure that had long

pervaded world politics (Rosenau 1995: 17). Terrorist and criminal networks themselves

are disaggregated organizations, and therefore present a different sort of challenge. They

are not a single enemy, but a diffuse array of actors connected together in a global

network. They are a global threat that needs a new type of governance; one that demands

collaboration between national actors beyond just a commitment to use force (Rees 2006:

22). On a global scale, they require a form of governance that is as fluid and resourceful

as the organizations that are being targeted.

Global governance includes systems of rule at all levels of human activity,

spanning from the family to international organizations, in which the pursuit of goals by

the exercising of control has transnational repercussions (Rosenau 1995: 13). Despite

this wide spectrum of global governance, most texts on the subject dedicate the majority of their pages to international organizations, regimes, and global civil society.

The United States and Europe have found it difficult to achieve progress on terrorism issues within international organizations. This is particularly true within the United Nations' General Assembly where there are a multitude of perspectives on the subject, not the least of which are from states that supported terrorist groups or felt sympathy for their cause (Rees 2006: 131).

Regimes, as patterns of regularized cooperation between states, require states to act together systematically (Rees 2006: 11). This may restrict regime members from altering their patterns of behavior in a rapid manner to better confront new threats. In addition, as regimes become more formalized, they also become more hierarchical. Since the early 1990s, the defining characteristic of transatlantic relationships has been a hierarchical structure, which has proven to be unsuitable to deal with today's challenges of international terrorism (Pawlak 2007: 2).

Global civil society, transnational social movement organizations, and Transnational Advocacy Networks (TANs) in particular, appear, on the surface, to be an excellent model for combating international terrorist and criminal organizations. TANs are lighter on their feet than hierarchical organizations. They stress fluid and open relationships among committed and knowledgeable actors in specialized issue areas and operate through global networks (Keck and Sikkink 1998: 8). What they lack, however, are the resources available to states. TANs mirror terrorists and other CTAs who operate through global networks, increasingly as do governments (Slaughter 2004: 1).

This chapter will seek to examine the similarities and differences between TANs, CTA networks and transgovernmental networks to see if they do mirror each others' behavior. First, the current literature on TANs will be examined in an attempt to identify their networks: focus, collective identity, methods of interaction, goals, and methods for achieving their goals (tactics). Next, the literature on CTA networks will be examined, with a focus on terrorist organization which are part of the global Salafi jihad movement's network such as al-Qaeda. The aim is to determine whether these networks behave in a similar fashion. Finally, the literature on transgovernmental networks will be explored in order to assess if these networks mirror the behaviors found in TANs and CTA networks. It is my hope that comparing these three types of networks will provide the theoretical framework for answering the question as to whether the use of transgovernmental networks of law enforcement and intelligence agencies is a valuable strategy in combating the security threat to the global system that CTA networks present in a globalized world.

Transnational Advocacy Networks:

Global civil society and the number of social movement organizations and networks have exploded over the last two decades. The growth of these organizations and networks in both number and significance is the result of an era of "globalization" that followed the "Cold War" era. As they have grown, so too has the literature on global civil society, social movement organizations and their networks. In this literature there are various views of what globalization is or means. One view of globalization is that it is the integration of markets, nation-states and technologies that will spread free market capitalism around the globe (Friedman 1999: 7-8). Others view globalization as another

stage in a long process of technological advances which allows people to interact around the world without reference to nationality, government, time of day or physical environment (Langhorne 2001: 2). Still other scholars view globalization as the intensification of social relationships which link distant people from distant locations (Giddens 1990: 18-19) or the intensification of the consciousness of the world as a whole (Robertson 1992: 8). While these definitions seem to point to globalization as a positive phenomenon that will make the world a better place, not everyone shares this opinion as to the direction globalization is taking the world. Some view globalization as a social process in which social and cultural arrangements recede (Waters 1995: 3). This causes a loss of local identity. This negative view is shared by others who view globalization as "a historical transformation: in the economy, of livelihoods, and modes of existence; in politics, a loss in the degree of control exercised locally" (Mittelman 2000: 6). Those who share this view of globalization believe the phenomenon, in its current form, should be replaced by the self conscious democratic rule of society. It is global civil society, social movement organizations and their networks that have emerged as the leaders of the view of globalization they call *Globalization from Below* (Desai and Said 2001: 53).

The goal of Globalization from Below is to restore the social and political gains achieved during the latter stages of the industrial era that have been eroded by the current version of globalization. Global civil society organizations that promote this ideology of globalization from below hope to "establish the constitutive elements of cosmopolitan democracy as a political template for a globalized world," and the "increased the interconnectedness, which contains many benefits for society worldwide" (Falk 1999: 3). The ultimate goals of globalization from below are to minimize violence and maximize

economic well-being while ensuring social and political justice and upholding environmental quality (Falk 1999: 130).

The establishment of transnational social movement organizations and networks is the primary means global civil society uses to promote the hegemonic counter force of globalization from below. Transnational social movement organizations and networks are associations of global civil society organizations built on trust and cohesion in an attempt to serve as a structure for cooperation beyond political, social and cultural boundaries. These transnational networks hope to gather the social capital for the economic, political and social benefit of all. Activism, on the other hand, refers to global civil society organization acting as political, social and cultural watch dogs. They attempt to act as countervailing forces to the power of governments and corporations (Kaldor, Anheier and Glasius 2003:9-10). Not all transnational social movement organizations and networks attempt to promote the idea of globalization from below in this manner. Some act as public service providers who are subcontracted by governments, while others work closely with multinational corporations. This is often referred to as globalization from above.

Whether transnational social movement organizations and networks utilize the strategy of globalization from above or below, globalization has helped global civil society's ability to recruit, organize and carry out action. The Internet and advancements in information technologies and telecommunications are enabling global civil societies' ideas, values and political persuasion of people to be transmitted around the globe (Wapner 1995: 317). Without these advancements in information, technology global civil society would not have gained the prominence it enjoys today. Civil society has

maintained an energetic presence in cyberspace and allows for individuals to communicate and support one another (Sassen 1999: 4). The Internet, email, and the World Wide Web made it possible for civil society to radically change their capacity to communicate and organize globally at relatively low cost. Printing and distribution of newsletters were replaced by web pages; phone lists became email lists, and even membership and donations could be solicited online (Langhorne 2005: 7).

Advancements in information technology and telecommunications continue to move forward at blinding speeds. The next generation of items such as computers, software and cell phones emerge in months, not years. These advancements, in combination with greater competition, have resulted in a lowering of cost of this technology, thus making it accessible to a greater number of people. This phenomenon has also allowed for the spreading of more diverse ideas and enabling these ideas to be debated around the world. Global civil society has already learned to utilize information technology to their advantage. As this technology gets in the hands of more people, global civil society will have a greater impact on the world and will have an increased role in global governance. It is this phenomenon that has lead to the establishment of transnational advocacy networks (TANs). These networks are constructed of "nodes" of individuals or groups which utilize modern technology to connect with other "nodes" around the globe who share their ideals or beliefs. Through their collective action, the nodes of the network can turn their attention to global scale problems and issues they feel need to be addressed.

Activists Beyond Borders by Margaret E. Keck and Kathryn Sikkink is regarded as a pioneer work in the field of transnational advocacy networks (Brenner 1998:189). It

has been cited in nearly every article related to the subject since it was first published in 1998. Keck and Sikkink lay out the theoretical framework for how TANs develop and operate. They explore the role and development of TANs of various social movements in various eras throughout history including: the campaign to end slavery, the international suffrage movement, and the campaigns to end foot binding in China and female circumcision in Kenya. Keck and Sikkink use these historical overviews as a model for TANs and compare them to three modern networks. Through case studies of these three modern networks (human rights advocacy networks in Latin America, environmental advocacy networks, and transnational networks on violence against women), Keck and Sikkink hope to understand the origins, workings and conditions of effective TANs.

Keck and Sikkink describe TANs as networks of activists, distinguishable largely by the common principles, ideas and values that motivated their formation. These networks include those relevant actors working globally on a particular issue, who brought together shared values, a common discourse, and a dense exchange of information and services (1-2). TANs participate in domestic and international politics simultaneously by drawing on a variety of resources. They act as though they are part of the international society constructed of states and international organization, and use their variety of resources to affect this society (4).

TANs are characterized by their voluntary, reciprocal and horizontal patterns of communication between committed and knowledgeable actors working in a specific issue area. They organize to promote causes, principled ideas and norms. They may include a wide array of actors from individual activists, domestic or international NGOs, international organizations to members of governments. The shared values and frequent exchanges of information and services among the actors in the network reveal a dense

web of connection among these groups (or nodes, in network terminology) which is both

formal and informal in nature. In addition, they work to create categories or "frames" to

generate and organize information on which to base their campaign (8-10).

According to Keck and Sikkink, TANs are most likely to emerge around those

issues where channels between domestic groups and their governments are blocked.

Activists, or what they call, "political entrepreneurs," believe that networking will further

their mission and they establish international contacts in order to form networks (12).

Essentially, nodes of activists form links with other nodes of activists concerned with

similar interests or concerns in an attempt to coordinate collective action.

When channels between the states and its domestic actors are blocked, TANs

usually employ a "boomerang" strategy to carryout their campaign. In this strategy,

domestic NGOs (domestic nodes) by-pass their state and, through established links, work

directly with international allies - foreign nodes within their TAN - to bring pressure on

their state from the outside. These international allies often provide access, leverage,

information and in some cases, money. When domestic grievances, concerns or demands

are not heard by the state, they may resonate elsewhere and the international allies within

the TAN can amplify these grievances, concerns or demands of the domestic group,

creating new audiences for these issues and then echoing these grievances, concerns or

demands back into the domestic arena from the outside (12-13). The goal of this strategy

is to bring pressure, arm-twisting, encouraging sanctions or shaming to the state so it will

respond or take action to address the domestic group's grievances (16).

The tactics that TANs employ to carryout these strategies fall into one of four

categories: information politics, symbolic politics, leverage politics, and accountability

politics. A campaign may contain one of these tactics or contain multiple strategies simultaneously. With information politics, TANs provide information that would not otherwise be available. They hope to gain influence by serving as an alternative source of information. In addition, they strive to uncover and investigate problems, and alert the press and policy makers (18-19). By employing symbolic politics, TANs attempt to frame issues by identifying and providing convincing explanations for a powerful event which then becomes a catalyst for the TANs cause (22).

TANs hope to gain influence over more powerful actors by using leverage politics. Leverage politics come in two forms: material and moral leverage. Material leverage is usually conducted by linking issues to access money or goods. One example might be, convincing policy makers or governments to cut off aid to offenders. Moral leverage is using the behavior of the target actor to shame them into action by holding their behavior up to the light of international scrutiny (23).

The final tactic TANs utilize is accountability politics, which is the practice of using the target actor's own statements against them. Once an actor has publicly committed itself to a particular principle, TANs can use those positions to expose the contradictions between the actor's position and their practice (24).

Keck and Sikkink conclude that TANs have emerged around particular issues perceived as important on the international stage and resonate across cultures. Issues involving core values such as right and wrong have stimulated the growth of TANs among individuals, groups and organizations which see their cause as meaningful. TANs capture attention where their issues resonate within existing ideas and ideologies and

have utilized the technological advances of globalization to find the audiences for their

message to further their causes (200-201).

What may be equally important to Keck and Sikkink is that TANs create a sort of

global collective identity. Members of TANs have shared values, norms, ideas and

beliefs. They often identify themselves more by their cause and membership in the TAN

than their own nationality, ethnic group or culture. Their cause is what becomes

paramount to who they are and where their loyalties lie. Any other group with which

individuals can be identified is second to that of their cause and their network. Ironically,

this shared identity and loyalty to a cause and membership in a network is also seen

among members of networks of Clandestine Transnational Actors, especially among

members of terrorist organization networks.

Transnational Networks of Terrorists and other CTAs

Despite similarities between TANs and networks of CTAs such as terrorists, in

much of the literature on global civil society and social movements, there has been a

reluctance to include CTAs in the discussion. Many authors feel that social movements

and global civil society must be benevolent in nature; however, who is to say what is

benevolent? Terrorist organizations view their grievances as legitimate and the goals of

these organizations are similar to organizations traditionally considered part of global

civil society. The main difference between terrorists and other social movement

organizations accepted as part of global civil society is that terrorists use violence as a

means to achieve their goal of social change.

Does the use of violence as a tactic in an attempt to promote social change

preclude a particular social movement organization from being considered a part of

"global civil society?" If terrorist networks' behavior attempts to promote social change in the same way that other social movement organizations do, with the only difference being the use of violence as a tactic, are they not in fact part of global civil society? The question then becomes, do terrorist networks respond to social grievances in the same way that other social movement organizations, which are accepted as part of global civil society?

Sidney Tarrow pointed out the paradox between terrorist organizations such as al-Qaeda and other nonviolent, international, non-governmental organizations accepted as part of global civil society in his presentation on "The New Transnational Contention" at the American Political Science Association annual meeting in 2002. Tarrow contends that groups like al-Qaeda do not fit into the "global civil society paradigm'" in either methods or their goals. He argues that terrorist organizations use contentious tactics, organize *against* rather than *within* the range of international institutions, and have developed into new forms of organizations similar to domestic social movements rather than civil society groups found in modern social movement literature (3).

Kurt Schock (2005), in his book, *Unarmed Insurrections,* contends that terrorism is based on the idea of "people's war" while large scale social movements are based on "people power."   He points out that terrorism is only successful in promoting change when it is used in conjunction with other forms of mass collective action. Terrorism as a sole means of trying to effect political change is a result of lack of popular support for a movement (23).   This seems to imply that a terrorist organization on its own cannot be considered a global civil society group, but rather should be viewed as a larger social movement.

Richard Langhorne (2006) describes global civil society as not merely a new name for transnational activity, but the increased institutionalization of citizens and non-governmental organization networks in the governance of our complex world. Global civil society organizations do not fall under one definition but rather include social movements, religious groups, labor groups and associations of all kinds. He contends that of all the organizations that make up global civil society, non-governmental organizations are the most common and most important. Langhorne argues civil society also implies the rule of law, since the word civil signifies a "measure of good faith and respect for law, even amongst the most passionate proponents of a cause." Extremist organizations that seek extra-legal means such as violence or fraud to pursue their agenda are not part of civil society (Langhorne 2006). This convenient caveat added by Langhorne excludes terrorist organizations from being considered a global civil society group.

Despite these limits for an organization to be considered a global civil society group, terrorist organizations do fit into the broader paradigm of a global civil society groups. Tarrow (2002) claims that because of the contentious tactics used and their working outside international institutions, terrorist organizations cannot be considered part of global civil society. It is the tactic of violence that prevents organizations like al-Qaeda from working within the range of formal international institutions; however, those non-governmental organizations involved in the "battle of Seattle" not only worked outside international institutions, but also worked against them. Few scholars would argue that most groups that participated in the "battle of Seattle" were outside global civil society.

Schock does not state that terrorist organizations cannot be considered global civil society groups. He argues that terrorism is usually only successful when part of a larger social movement. This tends to lend credence to the idea of terrorist organizations as part of global civil society in that they are unsuccessful on their own. Finally, Langhorne argues that civil society implies an adherence to law. However, this appears to interpret law in an exclusively western democratic framework.   Law is an important element of Islamic terrorist organizations. One of their main goals is the imposition of Sharia, Islamic law, to govern all aspects of life. When these organizations use violence as a tactic they often look for interpretations of religious texts and laws to justify their actions.

Not all authors wish to exclude CTAs from discourse on social movement organizations. Adamson, views actors who use tactics of terrorism, insurgency and other forms of violence within their "repertoires of contention" as one subset of the broader category of "non-state political entrepreneurs" who engage in transnational political mobilization (2005: 32). In her article, "Globalisation, Transnational Political Mobilisation, and Networks of Violence," Adamson draws on the literature relating to non-violent social movements and TANs to examine CTAs who use terrorism and violence as a tactic to seek political change.

She contends the mobility of people, capital, goods, ideas and information across national borders and around the globe create a resource base that can be utilized by non-state actors for political mobilization. Global migration has become the foundation on which many transnational networks have been constructed. Migration rates have increased dramatically over the last several decades and this increase has coincided with decreased cost of transportation and new communication technology which have allowed

these migrants to keep in contact with their home country and be part of a virtual community that transcends borders. This has allowed migrants to maintain dense networks that stretch around the globe. This interconnection of migrant communities has also facilitated the recruitment of members into transnational networks ranging from nonviolent movements to terrorist networks. It has also allowed networks to develop a variety sources to fund their movements (33-36).

CTA networks of violence also mirror nonviolent TANs in tactics. These CTAs employ the boomerang strategy as described in Keck and Sikkink. They bypass the state by drawing on transnational migration networks to apply pressure on the state from the outside. Adamson used the example of how Kosovar Albanians, including the Kosovo Liberation Army which relied on Kosovar diaspora for both financial support and to assist in launching a political lobbying campaign targeting European states, international organizations and NGOs. Another example is the Kurdish nationalist movement and the PKK in Turkey, which simultaneously carried on armed insurgency and terrorism, while promoting a Kurdish identity within its diaspora communities and using them for political mobilization throughout Europe. The PKK members within the diaspora communities also engaged in extortion, protection rackets, drug trade, aliens smuggling and other criminal activity as a source of revenue (38-40). These activities resulted in the PKK resembling a criminal CTA network more than a political terrorist CTA network.

Similar network patterns are found in diaspora groups based on religious identity rather than national or ethnic identity. The most obvious example is the global Salafi jihad movement (discussed late in this chapter) which includes al-Qaeda and its affiliated organizations and networks. The result of this phenomenon is that CTA networks

challenge the traditional distinctions between internal and external security concerns. As governments respond to these new security threats, they must come up with new strategies to combat diverse and diffused organizations rather than state actors. This process is what Adamson calls the domestication of global security (44).

While Adamson examined how CTA networks develop in diaspora communities around the globe and utilize boomerang tactics in order to effect change in their native lands, Jacob N. Shapiro, in his paper, "Organizing Terror: Hierarchy and Networks in Covert Organizations," takes an organization behavior approach to examining CTA networks (2005). This paper describes how CTA organizations respond to increased government pressure by changing their organizational structure. He points out how al-Qaeda and its affiliated organizations have responded to increased government pressure following the September 11th attacks by adopting a decentralized, less hierarchical structure of network organizational form. This, however, is contrary to how terrorist organizations have historically responded to increased pressure. In the past, terrorist organizations responded to government pressure by reducing communications, strengthening their hierarchy and developing a security bureaucracy (3). Shapiro's hope is to better understand how these networks are organized by examining why al-Qaeda has developed differently from other terrorist organizations. His goal is to identify conditions in which these organizations will evolve in specific directions.

Shapiro found that there are three dimensions of organizational design in CTA networks. The dimensions of these "covert organizations" are: interconnectiveness, hierarchy and specialization (7). Interconnectiveness describes the level of connectivity among network members. The most highly interconnected network is one in which every

individual in the network is connected to every other member. The least connected network is one in which each member is only connected to at least two other members, forming a ring network. Between these two extremes there are many different levels of connectivity in networks, most common of which is the cellular structure of small groups of 4-6 individuals who all know each other. These small groups form a clique and only one cell member communicates with other cells (8).

While this cell size of 4-6 is common in CTA networks, it is not absolute, and often members of a clique will come and go. A cell can consist of a large group of individuals or one person. Shapiro considers the core leadership of al-Qaeda as one cell, but would argue the Khalid Sheik Mohammed could also be considered his own independent cell. Between 1995 and his capture in 2002, Khalid Sheik Mohammed traveled the world independent from any large cell while still affiliated with al-Qaeda and provided financial resources and information to support attacks carried out in al-Qaeda's name. Therefore, Shapiro argues that the best description for a cell is the smallest independent functioning unit (9).

As with interconnectiveness, the level of hierarchy within CTA networks can vary greatly. It can be highly centralized, where every decision and action is controlled by the leadership of the organization. The opposite end of the spectrum is where the leadership has little or no control over the operational elements; only providing inspiration or moral justification for actions. Networks of this type are not hierarchical in nature and have little structure, if any. In CTA networks, the level of hierarchy is measured by the amount of control those who provide the political ideological guidance for the network

have over the operational elements (11). In short, the level of hierarchy is determined by how centralized the decision making process is within the organization or network.

Shapiro measures the hierarchy of an organization or network by using a scale of four to describe how centralized control is within the organization or network. The four levels of the scale are: centralized, de facto centralized, de facto decentralized and decentralized. Centralized is when the leadership directly controls operations and resources. De facto centralized is when the leadership controls either resources or operations and delegates the other while monitoring activities and maintaining the ability to act if these activities are not carried out as prescribed. De facto decentralization is when the leadership controls either resources or operations and delegates other, but lacks the ability to monitor activities and the ability to act if these activities are not carried out as prescribed. Finally, decentralized is when the leadership provides only ideological guidance and the cells are self reliant for funding and coordinating operations (12).

The final dimension of organizational design in CTA networks is specialization. The level of specialization refers to the range of tasks that each cell or unit within a cell is expected to undertake. In CTA networks, there are a wide range of activities that require specialization in order to successfully carry out an operation. When the network is a terrorist organization these include financing, procurement, intelligence, logistics, and recruiting, just to name a few. Because success of an operation often requires coordination of various activities, the level of specialization is often constrained by both the level of interconnectiveness and hierarchy of an organization.

In decentralized networks, coordination requires information sharing which can involve significant security risks. Therefore, specialization will require these networks to

find secure means to exchange information. In a hierarchical organization, specialization is able to occur even when there is a low level of connectivity, so long as the leadership is able to allocate appropriate resources without generating unacceptable security risks resulting from the dispersal of these resources (12-13).

Specialization appears to be a key aspect of a CTA network's ability to effectively carry out an operation and the level of specialization is linked to the level of interconnectiveness and hierarchy of a network. Therefore, Shapiro concludes that there is a cost (security risk) and benefit (operational effectiveness) to the design choice in which a CTA network is organized. He divides these design choices into seven different types: cellular, centralized; interconnected, de facto centralized; cellular, de facto centralized; interconnected, de facto decentralized; cellular, de facto decentralized: interconnected , decentralized; and cellular, decentralized (17-19). He weighs the cost and benefit of each design choice as to how it carries out its activities and relates to its leadership and other groups within the organization. In addition, the design choice has a direct impact as to the security risk present in each group (19-20).

When Shapiro's cost and benefit design choice was applied to al-Qaeda, he concluded that prior to the September 11th attacks it was primarily a cellular, centralized group in nature. Following the attacks, he claims that the al-Qaeda organizational structure became interconnected and decentralized in nature (15). The reason for this shift was two-fold. First, increased pressure from the United States and other governments on its global operations, second, was the loss of Afghanistan as a safe haven. Yet the environment in which al-Qaeda is operating has again changed. Much has been written in the past few years regarding how al-Qaeda's leadership has

reconstituted itself and found a new safe haven in the Northwest Frontier provinces of Pakistan and other areas along its border with Afghanistan. If this is in fact the case, al-Qaeda may again emerge as a centralized hierarchical organization while enjoying the benefits of the interconnectiveness of its network established following the September 11th attacks.   Before this accretion can be proved, we must first have a better understanding of al-Qaeda as both an organization and a movement. For this, we turn our attention to the work of Marc Sageman.

Understanding Terror Network by Marc Sageman (2004) is a comprehensive examination of the terrorist networks that make up al-Qaeda and its affiliated organizations. He views these groups as part of the greater Salafi jihad social movement, a movement which serves as the ideological base of most Sunni Islamic terrorist organizations, including al-Qaeda and its affiliated groups. Salafi movements contend that only by returning to the way of life at the time of the prophet may Muslims once again experience a golden age. Salafi jihadists promote the use of violence to achieve this goal.

Sageman traces the roots of these organizations to the "Afghan Arabs" – the name given to Muslims from around the world that went to Afghanistan to fight against the Soviet occupation the 1980s. The end of the Soviet presence in Afghanistan eliminated the legitimacy of jihad in the traditional sense. As a result, the hardcore leadership of some of the Afghan Arab groups decided to establish a base (al-qaeda) for a social movement to carryout worldwide jihad (36). After the Soviet occupation, the members of these groups returned to their home countries but remained part of the overall movement providing a foundation for a global network. This network gave al-Qaeda a

global reach to allow the organization to recruit, train, plan finances and carryout attacks both toward "near enemy" - pagan states within the Islamic world that do not follow true Islamic principles, and the "far enemy" - those states outside the Islamic world whose actions cause harm to Muslims and the Islamic world, such as the United States and many Western European nations (44-45).

While the Afghan Arabs provided a base for a global network, in order to grow their movement, they would need to add new members to the jihad. However, joining the jihad was not a single decision, but rather a process. This process must be examined in order to understand the global Salafi jihad network. New potential members must not only have an ideology that is in line with those espoused by the Salafi jihad, but also have a means by which to join. An individual's decision to travel somewhere for terrorist training should be viewed as their first overt act that they are serious about their intentions to join the global Salafi jihad movement. Being trained as a terrorist does not in itself mean you are part of the network. You must be accepted and asked to join. In the case of al-Qaeda, new members were required to pledge baya, a formal oath of loyalty, to Osama bin Laden and al-Qaeda. In fact, only a small number, perhaps between 10 and 30 percent, of those who attended training camps were asked to formally join al-Qaeda (91-92).

Joining the network was a bottom-up process rather than a top-down process. Motivated individuals who want to be part of the Salafi jihad movement looked to join rather than waiting to be asked. But sharing the Salafi jihad ideology, a desire to join the movement and a willingness to attend training is not enough to become part of the network. Many motivated individuals want to join but do not know how to get in touch

with an organization to do so. In order to join, one must first have a link to the network. These links are the key to understanding the dynamics of the network (99).

Finding a link to a Salafi jihad network is often a chance phenomenon. This link usually occurs through four key social affiliations: friendship, kinship, discipleship and worship. Friends often decide to join jihad as a group rather than as individuals. If one person in a group of friends is able to find a link to the network, he can share that link with the others in his group. In addition, by joining as group, it allows the friends to rely on each other for support as they go through the process (107-110).

Kinship can provide a link if a family member is able to give access to networks. This link can be found in one's immediate, extended or expanding family that resulted from a marriage where new in-laws provide access that did not previously exist (112-113). Links through discipleship are somewhat unique to Salafi jihad movements in Southeast Asia. It is loyalty to a leader, who is in most cases, was an "Afghan Arab" during the Soviet occupation, which provides access to the link (114). Joining the movement is an expression of this loyalty. Finally, places of worship can provide a link to the network. They provide a place where people of like ideas may congregate. This interaction between individuals with like ideas allows for these ideas to intensify and create a bond between the individuals in a group (114- 115).

Often, loose links to the Salafi jihad will work in tandem to create a strong link to a network. For example, an individual begins to attend a mosque, at which he finds others who share his sentiments and beliefs. These shared values in turn create a bond between these individuals that is the basis of the group's initial friendship. One of the members of this group of friends has a brother-in-law trained in Afghanistan and who

still has ties there. His brother-in-law agrees to vouch for the entire group and assist

them in attending training. During the training they are formally accepted as part of the

network and swear their baya.

Links are not just important for gaining access to the Salafi Jihad movement, they

are also crucial to maintaining the networks viability. As stated earlier, individuals

usually formally join the Salafi jihad movement in groups of friends. In network terms,

these groups of friends are viewed as cliques built on human similarities. These

friendships are a reflection of common backgrounds, education and beliefs. Cliques are

dense groups that form locally based on face to face encounters and the development of

long term bonds (152). These cliques often attend training camps together were they not

only learn terroristic skills, but also build confidence among the groups and forge an

"espirt de corps" among the friends, cementing their identity as global Salafi jihadists

(121). When these cliques leave their training and return home, they become nodes in a

global network.

These nodes are connected in the same way as Shapiro describes the

interconnectivity of cells. In fact, the terms are interchangeable; a node being a more

common term in network analysis literature and its use is dictated by Sageman's social

network analysis approach to examining terrorist networks. In a social network analysis

approach, a network is viewed as an individual or a group of individuals organized in

nodes which are connected through links. Some nodes have more links than others and

therefore have greater interconnectivity. The multitude of links allows nodes to connect

to other more isolated nodes. These more interconnected nodes are called hubs. These

hubs are an important component of terrorist networks (137). Hubs use their

interconnectiveness to organize and provide logistical support for attacks. They are the links between isolated nodes and can independently direct these different nodes to carry out specific activities for the furtherance of a larger plot. This network design provides enhanced security to the operation because the separate nodes may be unaware of the other nodes activities or membership, nor would they necessarily be aware of the totality of the plot. This compartmentalization means that each mode may only be aware of their specific role and only the hub may have the overall picture of the network's goal. When a network operates in this manner, the discovery of one node or cell by a security agency does not necessarily disrupt the total plot.

Sageman points out that terrorist networks are not static; rather they develop and can expand and grow over time. The member of one node can break away and create a new node. In doing so, he not only creates a new node, but acts as the link between the two nodes. As the process continues outward and more links are establish an individual or group node can become a hub. The network development of those terrorists responsible for carrying out the attacks of September 11th illustrates this process. The "Hamburg Cell" started out as graduate students joined by their religious views. They were one node that was able to establish a link to travel to Afghanistan for training and formally join al-Qaeda. Khalid Sheikh Mohammad was the hub that linked this group node back to the "Central Staff." As the plot progressed, the "Hamburg Cell" separated and formed new nodes within the United States. Ramzi bin al-Shibh, who was unable to obtain a visa to enter the United States, remained in Europe and became the hub that linked the various nodes in the United States together while maintaining the link with Khalid Sheikh Mohammad.

Just as advancements in communications over the past two decades have strengthened links within TANs, Sageman points out that these advancements have also strengthened links between nodes within the global Salafi jihad movement. Traditionally, religious terrorism has been based on face to face interaction, which remains an important part of the social movement. The building of trust requires intense intimate exchanges and once established were reinforced and maintained by continued communication to sustain member's dedication, provide emotional support and guidance (158). The revolution in communication technologies in the 1990s made this possible on a global scale. The leadership of al-Qaeda in the mid to late 1990s was fully integrated into a new global network of communication. It allowed for the establishment of a loose, decentralized network spanning the globe, where face to face interaction was no longer necessary. The leadership was able to utilize satellite phones, e-mail, faxes and websites to oversee a truly global jihad from the sanctuary of Afghanistan (159).

The internet in particular has had a dramatic affect on the Salafi jihad network. It has allowed the creation of a new type of relationship between an individual and a virtual community. This virtual community is not tied to one nation, but rather owes its loyalty to the Salafi jihad ideology. Anyone familiar with the use of the internet can go to an internet café and anonymously reach out to others who share this philosophy and ideology. It allows for the development of cliques where the bonds can be built and communication occurs without ever meeting in person (160-162).

The internet has had a profound effect on the global Salafi jihad movement; this fact is undeniable. The internet has not, however, replaced the global Salafi jihad network, of which al-Qaeda and its affiliates remain a strong foundation. Much has been

written both in the popular press and scholarly works in recent years suggesting that al-Qaeda, due mostly to the power of the internet, has become more of a movement or ideology. Their claim is that the internet has created a virtual terrorist network, where members can meet, share ideas and learn how to carryout attacks. This claim suggests that these new groups are self starter cells that are autonomous and share ideological affinity with the Salafi jihad movement, but operate in absence of any formal training or recruitment. It is claimed that the internet serves as an operational tool and "democratizer of violence" (Kirby 2006: 415). What the internet does not provide a potential member is a real link to a Salafi jihad organization, nor does it allow for an organization to assess the reliability of potential candidates. While the internet may help in socializing a potential member to the Salafi jihad ideology, it is uncertain whether he would be willing to make the sacrifices needed to commit to the cause (Sageman 2004: 163). The London transportation system attacks of 2005 and the failed airline plot of 2006, which is often used as a case study in the virtual or self starter network theory, seem to indicate that the current global Salafi jihad network more closely resembles those networks described by Adamson, Shapiro and Sageman than those who claim al-Qaeda is now virtual.

Those responsible for both the 2005 and the 2006 plotters were British born Muslims, mostly of Pakistani decent, who lived within immigrant communities of London. In both cases, it appears the plotters had a link to jihad that allowed them to travel to Pakistan. Some of those who planned to carry out the 2006 airliner plot traveled repeatedly to Pakistan between 2002 and 2006. During some of their trips, the plotters traveled to the Federally Administered Tribal Areas of Pakistan where they received

explosive training (Greenberg et al 2008). The link that gave the plotters their opportunity to join jihad was a friend from the neighborhood named Rashid Rauf.

Rauf appears to be textbook case of Sageman's four key social affiliations of friendship, kinship, discipleship and worship to joining Salafi jihad. Rauf fled from Great Britain to Pakistan in 2002 following the murder of his uncle in which he was a suspect. Once in Pakistan, Rauf stayed at the home of a local imam who often stayed with Rauf's family while he was preaching in the UK. Rauf married the imam's daughter who was also related by marriage to the founder of Jaish-e-Mohammad (Cobain and Weaver 2008). Jaish-e-Mohammad is an organization that is widely thought to be an affiliate of al-Qaeda, thus providing Rauf his link to the Salafi jihad movement.

Following their explosive training and return to London, the airline bombing plotters were now "an al-Qaeda cell directed by al-Qaeda leadership in Pakistan" (Greenberg et al 2008). These men were now nodes in the network and Rauf served as the hub coordinating between the plotters in the UK and al-Qaeda leadership in Pakistan. In fact, it is believed that Rauf may have received his instructions directly from al-Qaeda's number two man, Ayman al-Zawahiri (Powell 2006).

It appears likely that Rauf played a similar role in the 2005 London subway bombings, although the connections are not as solid.   Mohammed Sidique Khan and Shehzad Tanweer, two of the bombing's main conspirators, attended the same Mosque as Rauf and the infamous "shoe bomber," Richard Reed (Powell 2006). Khan and Tanweer also travel to Pakistan, where it is believed they received terrorist training at camps near the Afghan boarder. These trips closely coincided with the trip to Pakistan taken by the 2006 airline bombing plotters. These facts have led some terrorism experts to conclude

that these attacks were not separate, but rather a large campaign by al-Qaeda to hit the UK in a rolling series of attacks (Greenberg et al 2008).

What these plots have shown is that the global Salafi jihad movement is alive and well. As Sageman described, it is made up of horizontal small world networks of nodes, links and hubs with an ability to adapt to changing circumstances and solve unforeseen obstacles in execution general plans (2004). These plots also suggest that the movement maintains a vertical hierarchical network component in the form of al-Qaeda and its leadership exerts control and direction to the horizontal network through hubs such as Rauf. This hierarchical network finds sanctuary along the Afghan-Pakistan boarder and will continue to grow in strength as those sympathetic to the Salafi jihad movement solidify their control in these areas and expand their sphere of influence into new areas such as Swat in the North West Frontier Province of Pakistan. This duel network structure of the global Salafi movement means that it may once again become the threat to global security it posed prior to September 11th. This will require governments to adapt new strategies to combat this threat. One strategy that has emerged is the idea of confronting "networks of terror with networks against terror" (Bendiek 2006: 5).

Network Solutions:

Transnational government networks increasingly exchange information and coordinate activities across borders and between governments in an effort to combat global crime. These networks are a key feature of global governance in the 21st Century, but they are under-appreciated, under-supported, and under-utilized (Slaughter 2004: 1). Transnational government networks have not been completely ignored in global governance literature. In fact, over thirty years ago, Robert Keohane and Joseph Nye

described how government officials began interacting with their foreign counterparts in ways similar to that of transnational, non-governmental actors in what they termed "transgovernmental relationships" (Keohane and Nye 1974: 41).

Keohane and Nye define transgovernmental relations as, "sets of direct interaction among subunits of different governments that are not controlled or closely guided by the policies of the cabinet or the chief executives of those governments" (1974: 43). They found that as the agendas and problems facing domestic bureaucracies broadened, they needed to deal directly with their foreign counterparts, rather then indirectly through their foreign ministries, in order to effectively cope with the issues that faced them. Communications among governments increased with international conferences and organizations facilitated direct contact among officials from what were once considered primarily domestic agencies (Keohane and Nye 1974: 42).

As the meetings and contact between foreign officials begin to recur, a sort of bond begins to develop. This bond reinforces the idea that they share membership in a common profession. Individuals may even begin to define themselves as part of this professional group, rather than in purely national terms (Keohane and Nye 1974: 45). As this practice becomes widespread, transgovernmental networks are created, linking officials in various governments to one another by ties of common interest, professional orientation, and even personal friendship (Keohane and Nye 1974: 46).

Anne-Marie Slaughter (2004), in her groundbreaking work, *A New World Order*, provides a comprehensive examination of transgovernmental networks in today's globalized world. In this new world, the lines between national and international issues have become even more blurry. National officials have found that they need to negotiate

across borders in order to conduct business that they could once accomplish solely at home (44). As a result, specialists from various nations form both formal and informal global networks, moving away from unitary states interacting through formal diplomatic negotiations towards networks of government officials who share common professional cultures. In a world of government networks, bureaucrats, and what Slaughter calls "regulators," members of the judiciaries and members of various legislatures around the world reach out to their foreign counterparts to help address the problems that arise when national actors or issues spill beyond their borders (16).

The defining feature of government networks is their composition of government officials or institutions linking with counterpart officials or institutions across borders in horizontal networks, or the linking of officials or institutions to their supranational counterparts in vertical networks (13). Horizontal networks are usually informal, flexible, and sometimes institutionalized within international organizations. Vertical networks tend to be hierarchical organizations that are supranational in nature and often replicate many of the governing functions of the state. In today's disaggregated, globalized world, horizontal networks are more numerous than vertical networks (20).

Horizontal networks among government officials in specific areas of expertise occur between high-level officials directly responsible to the national political process, officials at the higher levels of their respective ministry, or low level regulators such as desk officers. The members of these networks communicate and interact amongst themselves in order to share information, collect and disseminate best practices, and provide technical assistance and training to those officials who have less experience in specific areas than their network colleagues. These networks can be spontaneous,

informal, flexible, and of varying membership or the network may be institutionalized within the auspices of international organizations (19).

Transnational governmental networks among what Slaughter calls "regulators" are the most numerous. These regulators are from the executive branch of governments. Their membership may range from heads of states to low-level bureaucrats who share common roles and problems within their respective governments. These networks may be within established international organizations, within the framework of an executive agreement, or spontaneous. Spontaneous networks are not international organizations established by treaties, but are informal in nature. They often have no legal standing and operate without formal headquarters; they allow government officials to address problems which are increasingly international in scope and allow for interaction and cooperation through informal agreements, such as memorandums of understanding or even less formal initiatives. Spontaneous networks are able to respond to needs and coordinate activities quickly, as opposed to the lethargic pace of traditional treaties, and do not require the time consuming process of legislative approval to act (45-49).

The degree and scope of cooperation and interaction ranges from information sharing networks on the looser end, enforcement networks in the middle, and harmonization networks, where common regulatory standards are shared among members, as the most formal network type. In information networks, talking is the primary activity. A valuable exchange of ideas, techniques, experiences and problems is created; resulting in a sort of collective memory and identity over time (51).

Enforcement networks assist in enforcing specific regulations against specific individuals across national borders. The activities of enforcement networks are two-fold.

First, these networks share intelligence and information in specific cases. This goes beyond the general exchange of information found in information networks to actionable intelligence. Second, enforcement networks engage in capacity building. The goal here is to help less developed or weaker countries to enforce not only their national regulations, but also international and foreign laws when necessary. Not surprisingly, these types of networks are most common among law enforcement and intelligence agencies (55-7).

Harmonizing networks attempt to harmonize one nation's laws and regulations with another. Harmonization involves an agreement on regulatory standards by two or more countries. These networks are more formal than information or enforcement networks and are often the product of formal bi-lateral or multilateral agreements (59). While harmonization networks carry the strength of acting within the framework of bilateral or multilateral agreements, they lack the fluidity and ability to react quickly that is so beneficial to information and enforcements networks.

The core theme of Slaughter's book is that there is a possible future world order made up not just of states, but also parts of states. Officials within regulatory agencies would participate in many types of networks, creating links across national borders and between national and supranational institutions (6). Hajer and Versteeg (2005) complement the work of Slaughter by examining how governance networks function in absence of defined rules found within traditional state and institutions of governance.

According Hajer and Versteeg, challenges facing governments today, of which terrorism and transnational crime are included, cannot be properly addressed by political institutions in the classic sense. Government structure is hierarchical in what they call a "matrouchka system," in which governments are like Russian dolls fit inside one another.

Local governments are the smallest doll and each layer's jurisdiction gets larger with the outer doll being international organizations. Governments of each jurisdictional level operate with the authority granted to them by their constituency. Governance networks, however, break from this logic by operating autonomously. Governance networks are made up of independent actors that work on joint problem solving through collaboration with other independent actors (340-341).

Governance networks operate across jurisdictions and do not share common legal authority that govern where and how the decision making process is to occur or what rules are to be followed. In an absence of formal rules exists what Hajer and Versteeg call the three conditions of network governance: institutional ambiguity; a lack of norms or procedures to legitimize the decision making process; and, multiple significations in which the different actors perceive the world or the problem in different terms (341). The conditions governing their behavior are the joint experience of collaboration and the shared knowledge, trust and reciprocal environment in which the various networks operate. Actors within the network must first have a shared understanding of what the problem really is and then how they will address the problem. As no single language or set of rules can be universally applied to how decisions are made, the network's decisions are usually made and agreed upon through the context of mutual trust among the actors in the network (342).

Since governance networks are built on the foundation of mutual trust, they often strengthen over time. As network actors negotiate a common understanding of the problem, a shared identity begins to develop among network members. The network begins to function as a "discourse coalition" comprised of actors who share a particular

view the problem at hand (343). This discourse coalition process is similar to the process of issue framing found in social movement literature. Once the network has developed this shared discourse, the stage is set to work together to resolve conflicts within the network (346). It is the shared discourse that replaces rules and norms existent in traditional political institutions and allows for a more fluid flow of ideas, information, strategies and best practices.

Transgovernmental Networks on the Rise:

Transgovernmental networks are playing an increasing role as a mechanism for exchanging information, mutual learning, and building trust in world politics (Pawlak 2007: 15). Many agencies that are traditionally domestic in nature have created their own offices of international affairs. Regulatory agencies are now representing themselves or acting as an official representative of their nation at conferences and international organizations, rather than relying on their nation's foreign ministry to represent their interests. This shift to agencies representing their own interest in global governance is best illustrated by the resource shift that is occurring within many nations' budgets. The international affairs budgets for regulatory agencies have increased dramatically across the board, even as foreign ministry budgets have shrunk (Slaughter 2004: 36-37). Regulatory agencies have also begun assigning low level officials overseas on a permanent basis to interact directly with their foreign counterparts. It is these officials who serve as the foundation for transgovernmental, horizontal information and enforcement networks.

Transgovernmental networks have proliferated into almost every area of government regulation. These networks have become informal institutions linking actors

across national boundaries and allowing them to carry out various aspects of global governance in new and informal ways (Slaughter and Zaring 2007: 215-216). Transgovernmental networks created a sort of division of labor in dealing with problems of a global nature. They exist between high level officials and their harmonization networks and low level officials and their enforcement and information networks. High level officials are tasked with dealing with problems that require greater political clout, such as harmonizing international standards and regulations. This leaves the networks of low level officials to work together on unofficial task forces to deal with specific issues or problems (Pawlak 2007: 17-18).

Transgovernmental networks allow low level officials to interact with foreign counterparts directly, allowing for the network members to interact with little supervision or interference from their nation's foreign ministries or their home agencies. This level of freedom and independence to act is more extreme when an official is assigned in a foreign jurisdiction in a "boots on the ground" scenario resulting in loosely structured peer to peer ties developing through frequent interaction, rather than formal negotiations (Slaughter and Zaring 2007: 213). This informal structure allows these networks to respond rapidly, and often in innovated ways, when new problems present themselves. Because of the informal structure of these networks, their success in global governance often depends on the quality of the individuals that make up the network's membership.

A Culture of Cooperation:

The key element to the success of transgovernmental networks is their membership sharing common values and experiences, including a common history and culture, as well as political and economic ideologies (Slaughter 2004: 134). Often the

bond between network members goes even deeper. Since the membership is made primarily of individuals within the same profession, the members usually share similar training, experiences, and a common professional language. Members have also faced many of the same problems and shared the same frustrations that are inherent in their profession. The sharing of these experiences with one another may result in a level of trust in the membership which goes beyond that of simple political allies.

Trust is crucial if there is to be cooperation. An environment of cooperation can be difficult to nurture between agencies which are not used to working with their foreign partners, sharing information and responding to requests for assistance from other countries (Rees 2006: 23). However, when a relationship built on trust does exist, officials tend to find themselves relating better to their foreign counterparts than to officials in their own agency at home. The result can be a dynamic, long-lasting relationship that is able to respond to issues and challenges in a rapid manner.

Relationships built between members of a network are also important when changes or shifts of environment occur within the network. If the network is confronted with external challenges or new issues and problems, well established relationships between its members allow the network to respond more efficiently and effectively (Pawlak 2007:19). Strong, well established relationships are also beneficial when the membership of the network changes. This is true whether the network membership is composed of high-level officials with members leaving the network because of changes in their country's administration, or if the network's membership is composed of low level officials, when members leave the network or are reassigned. A strong relationship

among members acts as a stabilizing force as members leave and may assist new members as they become acclimated.

The Future of Network Governance:

Modern communication systems have allowed national officials to interact electronically with officials in other countries, horizontally (Slaughter and Zaring 2007: 218). Phone, emails and faxes have become the primary mode of interaction between network members. Government officials have also become linked to one another across the internet. The result is that their networks have become more durable and fluid by "virtue of being virtual" (Slaughter 2004: 53). Even when members officially leave a network, they may remain *de facto* members in that they remain in contact with the fellow network members. It is also possible that members of a network may never meet face-to-face. Even in this type of interaction, it is possible for relationships based on trust, shared experiences, and common bonds to develop and grow outward to other members of the network.

Ironically, while transgovernmental networks appear to be going virtual, so too are criminal and terrorist organizations. As discussed earlier, both transnational advocacy networks and networks of clandestine transnational actors have also benefited from these advancements in technology. It is just one more way that globalization has helped these transnational criminal and terrorist organizations to operate and penetrate the territory of the state from the outside. To stop such organizations, states need to pursue criminals and terrorists across national borders. This requires that states cooperate with their neighbors in investigation, apprehension and even prosecution on a multilateral basis (Rees 2006: 7-8). Transgovernmental networks are uniquely capable of addressing

global problems that flow from outside sources (Slaughter 2004: 170). This includes the

problems perceived as a threat to homeland security such as global crime and terrorism.

Fighting "Networks of Terror with Networks against Terror"

The terrorist attacks of September 11th, and subsequently in Madrid, and London

illustrated the efficiency and flexibility of the networks responsible. These attacks have

shown a need for modes of international cooperation and coordination as efficient and

flexible as the terrorist networks. This need was of particular importance in the

relationship between the United States and the European Union in that they were "the far

enemy" of the Salafi jihad movement and would continue to be the most obvious target

for future attacks. One strategy to combat this threat has been the establishment of

homeland security transnational networks. Patryk Pawlak examines the emergence,

development, and product one of these networks.

In his article "From Hierarchy to Networks: Transatlantic Governance of

Homeland Security," Pawlak (2007) examined how the EU-US Political Dialogue on

Border and Transportation Security (PDBTS), established in 2004, helped overcome

challenges with the governance relationship of transnational homeland security found in

more traditional hierarchical structures of governance. He argues that transnational

governmental networks enhance and improve governance at the international level. The

development of homeland security governance, an area where notions of national

sovereignty remain at the forefront, networks like the PDBTS are important factors in

avoiding deadlocks in US-EU relations on homeland security issues.

Pawlak explains how the development of the PDBTS traces it roots back to the

1990s, when it was realized that a better mechanism of cooperation was needed to

manage the complex interdependency that characterized US-EU relations. During that decade, the New Transatlantic Agenda (NTA) was established in an attempt to link US-EU cooperation and upgrade levels of commitment, widen the scope of the relationship and increase formal dialogue intended to mobilize or shape public, business and political support. The NTA created a transatlantic partnership well suited to deal with challenges that were economic or political in nature, or more traditional security threats found in the state system. The NTA, which was made up of primarily diplomats and trade specialists, was ill equipped to deal with threats related to homeland security such as international terrorism (4-5).

The participants in the NTA meetings did not have the expertise needed to work internationally on the broad array of issues to be addressed in response to the threat from global terrorism. The PDBTS, however, was made up of high-level officials with responsibility for homeland security issues. The first PDBTS meeting was held in April 2004 focusing on issues such as the introduction of biometrics into travel documents, international databases, the use of sky marshals, and aviation and rail security. These issues required a level of specialization not found among diplomats and trade specialists who participated in the NTA. The formal process of bargaining and diplomatic speak found in the NTA were not suitable for meetings of hard core homeland security specialist who engaged in frank and targeted debate. These homeland security specialists were aware that there needed to be a new way of doing business that required imagination and an environment in which action could take place as efficiently as possible (7-9).

Pawlak describes how participants in the PDBTS tried to accomplish the network's goals in three phases; the early warning phase, agreement phase and the implementation phase. The early warning phase took place in the field prior to any meeting of the participants. Information about planned initiatives was exchanged well in advance, thus allowing participants to know and try to understand others' positions prior to any formal meeting and increase credibility between members by letting each other know where they stand. The early warning phase also enhances the agreement phase by allowing participants to get involved early on in each others' policy making process, reconciling initially divergent positions and facilitating collective decision making. The implementation phase occurs after the formal meetings, when the process of policy coordination begins. Once an agreement is reached by the high level participants of the PDBTS, the low level officials of the network maintain the agreements reached and carry out the day to day interaction between the various agencies whose members make up the PDBTS (9-11).

Pawlak points out that since 2006, there has not been a formal meeting PDBTS. This fact does not mean that the cooperative US-EU relationship on border and transportation issues ceased to exist. The relationships that developed between members of the PDBTS led to the creating of new groups, centralized around more specific areas related to homeland security. These new groups include: the Transportation Security Cooperation Group, the Joint Customs Cooperation Council and the High-Level Working Group on Data Protection. These groups all benefit from the strength of previous existing relationships built through the PDBTS.

Even though the PDBTS is not overtly visible, its effectiveness is still felt and the links it established still exist informally. There continues to be communication and dialogue between the actors who were part of the PDBTS. This interaction has served as a means to keep these transitional relationships alive. In addition, the PDBTS has created a machinery of mutual learning and trust building which worked not only during official meetings, but between meetings, and after official meetings had ceased to be scheduled (14 -15).

In networks such as the PDBTS, Pawlak points out that there is a division of labor in which individuals have broadly defined roles. High-level executives should deal with problems that cannot be solved by lower level networks. Lower-level networks should be given greater freedom to take on decision making and problem solving that do not require high level approval, thus depoliticizing homeland security cooperation. Finally, the day to day maintenance of the transnational relationship is kept up by desk officers (17-18).   In matters relating to homeland security, these "desk officer" positions are often filled by professional law enforcement or intelligence officers. Increasingly, law enforcement and intelligence agencies are officially assigning their officers to foreign countries to act as liaisons and conduct a myriad of duties ranging from advising and training to coordinating investigations and sharing sensitive intelligence.

U.S. law enforcement agencies have a long history of stationing their officers in foreign jurisdictions. This practice dates as far back as the 1820s, when agents employed by custom collectors in New York were assigned north of the border to collect information about smuggling ventures from Canada. By the turn of the century, Treasury agents were assigned to at least five cities in Europe (Andreas and Nadelmann 2006:

112). During the 1970s and 1980s, U.S. law enforcement agencies were increasingly called upon to deal with international organized crime and drug trafficking. The FBI created liaison offices based overseas at U.S. embassies. The Drug Enforcement Administration, which did not even exist prior to the 1970s, had permanent overseas offices and agents engaged in investigations in Europe, Asia, Africa and Latin America by the 1980s (Winer 2004: 5). In less than a decade, the DEA became the first law enforcement agency with a global operational capacity (Andreas and Nadelmann 2006: 129).

Neither the FBI nor the DEA agents who are assigned outside the US enjoy the same authority as they do domestically. What they do enjoy are the benefits of a global network of police officers who gather information and coordinate their agencies operations beyond the territory of the United States (Rees 2006: 32). This strategy of sending liaison officers overseas was mirrored by other U.S. law enforcement agencies including : the U.S. Customs Service to combat smuggling; the Immigration and Naturalization Service to combat immigration crimes and human smuggling; Alcohol, Tobacco and Firearms for gun running; and, the Secret Service for financial crimes (Winer 2004: 5). By the end of the 1990s, there were more than 2000 U.S. law enforcement personal assigned overseas (Andreas and Nadelmann 2006: 169). This U.S. strategy was not a one way street. These U.S. agencies encouraged other countries to send there liaisons to Washington for a reciprocal sharing of information and intelligence gathering (Winer 2004: 10).

These officers' interactions and cooperation with their oversea counterparts are often based on trust, allowing them to share information and respond to requests for

support; something that is not likely to occur in the absence of this network environment of trust and common identity. Even without the existence of formal arrangements between agencies, officer to officer cooperation often continues to take place for the exchange of leads and investigative information not destined for court (Winer 2004: 6). There exist a powerful transnational police subculture bound by the basic notion that a cop is a cop no matter what badge he carries, and a criminal is a criminal no matter what his nationality or language (Andreas and Nadelmann 2006: 98). The hope of these officers is to build a network of law enforcement officers as capable and as swift as the networks criminals use (Rees 2006: 31).

The September 11th terrorist attacks produced a rapid shift from the U.S. law enforcement agencies' traditional international operations focused on narcotics, arms, human smuggling, and organized crime, to those focused on countering international terrorism, a phenomenon previously left largely to the Central Intelligence Agency in its international aspects (Winer 2004: 11). When international terrorism became the overriding focus of law enforcement agencies' international operations, pre-existing initiatives to combat traditional transnational crime provided a robust platform on which counterterrorism activities could be based. How has this strategy of assigning officers overseas to create a global network of law enforcement officers as capable and as swift and the networks criminals use been adapted to combat "networks of terror with networks against terror?" In order to answer this question, we must first narrow down our focus to how one type of network attempts to combat one important feature of an international terrorist network; the ability of it members to cross international borders without being detected in order to plan, prepare, and carry out the attack.

Terrorist networks become international when their terrorism is perpetrated across borders, or when its attacks target individuals of more than one country (Rees 2006: 8). Following the September 11th attacks, questions were asked as to how the terrorists were able to gain entry to the country to plan, prepare, and carry out this attack. The answer: the terrorists were able to cross international borders with ease and with little risk of being detected or intercepted. As a result, preventing terrorist travel has become the cornerstone of a larger counter terrorism strategy. The use of a global network made of immigration and law enforcement officer assigned overseas was part of this strategy.

Prior to September 11, 2001, the Immigration and Naturalization Service (INS) was the primary U.S. law enforcement agency tasked with combating immigration related crimes and screening individuals attempting to enter the U.S. Human smuggling and trafficking were the crimes which were the most global in reach. While like most other U.S. law enforcement agencies prior to the 1990s, the INS had little international reach. However, in 1997, it announced a major expansion of its overseas offices in an attempt to more effectively deal with the problems of human smuggling. Over 150 INS personnel were stationed at forty offices abroad. They were deployed in order to train foreign law enforcement and airline personnel to detect fraudulent documents, generate information and intelligence, and enhance cooperation and local capacities of the host countries (Andreas and Nadelmann 2006: 170).

Within a year and half of the September 11th attacks, the U.S. undertook massive government reorganization in an attempt to be better equipped to handle the security threat from international terrorism. As part of this reorganization, the investigative, detention and removal, and intelligence operations of the INS merged with the Custom

Services investigative and intelligence operations to form Immigration and Customs Enforcement (ICE) within the newly created Department of Homeland Security. Many of the international operations of the INS now are the responsibility of ICE's Office of International Affairs.

ICE has taken the INS international operations and combined them with the international operation of the former U.S Customs Service, thus creating a new law enforcement agency with a global reach. The key component of this global operational capability is ICE's attachés - their officers assigned overseas and the global network of officers it creates. The important question is how does this global network operate to give ICE the ability to meet these new security challenges presented by international terrorism, and, more specifically, global Salafi jihad networks such as al-Qaeda's ability to cross international borders? To answer this question, we must first understand how terrorist cross international borders in order to plan, prepare, and carry out attacks. The next chapter will hope to accomplish this goal through a historical examination of how terrorist with links to the global Salafi movement have crossed international borders in the past and offer insight into future terrorist travel methods. The methods employed by these terrorists first came to light as a global security threat in the wake of the first World Trade Center bombing in 1993.

CHAPTER TWO: TERRORIST TRAVEL METHODS

On August 31, 1992, Abdul Basit Karim, a 24-year old Pakistani born in Kuwait, began his journey from Peshawar, Pakistan to the United States (Miller 2002: 75). He boarded Pakistan Airlines flight 339 to Karachi with his travel companion and the next day continued on to the United States. Karim presented a fake British passport to an official and bribed the official to allow him to board Pakistani Airlines flight 703 to John F. Kennedy International Airport in New York under the name Azan Muhammad (A British passport in the name Azan Muhammad was later found in his traveling companion's luggage (9-11 Commission 2004: 48)). When Karim arrived in New York with a boarding pass in hand, he strolled into the arrivals hall with the rest of the passengers from the flight, approached an immigration inspector and requested political asylum. The inspector asked Karim his name, and Karim handed him an identification card from the Islamic Information Centre in Houston, replying, "Ramzi Ahmed Yousef" (Reeve 1999: 140).

Karim, now known as Ramzi Ahmed Yousef, was interviewed about his reasons for coming to the United States. Yousef claimed he was an Iraqi citizen and that he would be oppressed if he was not allowed to enter the United States. He presented an Iraqi passport in yet another name (Reeves 1999: 140). After Yousef was processed, he was allowed to enter the United States pending a hearing with an immigration judge regarding his asylum application. Not surprisingly, he never appeared for his scheduled hearing.

Ramzi Yousef, free on the streets of the United States, was able to plan and conduct the first World Trade Center attack on February 26, 1993. Immediately following the attacks, Ramzi Yousef obtained a Pakistani passport in his real name, Abdul Basit Karim, and fled the United States. He was the world's most wanted terrorist until his capture on February 7, 1995.

No one individual better illustrates the threat a terrorist's ability to cross borders poses to international security than Ramzi Yousef. He used over twenty aliases to travel, plan, coordinate and carry out numerous attacks. The best example of Yousef's traveling skills occurred on December 11, 1994. Yousef used an Italian passport in the name of Armaldo Forlani to board Philippines Airlines flight 434 from Manila to Cebu. He even claimed while purchasing the one-way tickets that he was a member of the Italian Parliament. While on the flight he assembled a bomb, leaving it on the plane he disembarked. The bomb exploded on the next leg of the flight, killing a Japanese businessman and seriously damaging the plane (Reeve 1999: 79). This was a test run for Yousef's Bojinka plot which, although foiled before it could be carried out, is believed to be the inspiration for the 9/11 attacks. The event is also important because of the travel document that Yousef used. An Italian passport would allow Yousef to re-enter the United States without a visa. While Ramsey Yousef illustrated how terrorists could use documents to travel and carry out attacks, the true scope of the threat was not realized until September 11, 2001.

Globalization has helped facilitate terrorists' ability to travel, communicate, organize, finance and carry out attacks. Advancements in international travel, shipping and communication have coincided with the internationalization of terrorist

organizations. This is what David Rapoport calls the fourth wave of terrorism. Concisely, these are terrorist organizations based on a religious ideology that are "distinctive in character, transcends the state bond." Rapoport continues, "This is a particular important fact in Islam, where the vast Sunni population is dispersed among so many states and where religious elements are especially active" (2001: 424). An organization such as al-Qaeda may have relied on states such as Afghanistan or the tribal regions in the North West Frontier Provinces of Pakistan to provide a safe haven, but the organization, its members, its influence, its ideology and its reach are global in nature. The organization is without ties of loyalty to a particular state; their loyalty is to the global Salafi jihad movement. This globalization of terrorist networks requires their members to clandestinely "travel abroad to foster ties with potential allies, to conduct training exercises, to raise money and attract political support for their cause" (Smith 2001: 1). Most importantly, as demonstrated by 9/11, terrorists must travel to carry out acts. Terrorists and other clandestine transnational actors cross the border in the same ways as other international travels and migrants. Where terrorist and other clandestine transnational actors (CTAs) differ is that their hope is to cross the border clandestinely, avoiding detection by border agencies. To understand how they accomplish this task we should examine how other international travels and migrants legitimately cross borders.

Traveling Across Borders

Since the Treaties of Westphalia, states have been the primary actors in the international system. The key principle behind the state's authority is sovereignty; the state is solely responsible for its own affairs unless it voluntarily transfers this responsibility in the form of a treaty or agreement. The borders that separate one state

from another are both the symbolic and a physical marker of where the sovereignty of one state ends and the sovereignty of another states begin. Acting as a centralized administrative system within its own borders, the state provides for the security of its citizens, including determining who is allowed to cross its border.

An individual who departs the sovereign territory of one state and crosses the border into the sovereign territory of another does so in one of three ways: by air, land or sea. These crossings usually take place at a port of entry or border checkpoint where the destination state can screen the would-be border crosser to determine if the individual will be allowed to enter. At border checkpoints and ports of entry, both individuals and goods are examined, though this chapter will only cover the screening of individuals.

When an individual legitimately enters a country by air, he arrives at an international airport that is a designated port of entry for that country. This port of entry can be located close to the physical border of the state or well within the sovereign territory of the state. The individual can be seeking admission into any state that is connected by flight to that port of entry. This phenomenon is complicated further when the individual applying for admission at the port of entry transited via a third country, where they may or may not have been screened.

When applying for admission after arriving by air, an individual is screened for three elements: the reason they are seeking entry, whether they are in possession of the documents required to enter the country, and whether they are an individual who is known to the state and whose entry may have an adverse impact on the state. There are many different legitimate reasons why individuals apply for admission into a particular state. They could be a citizen or resident of that state returning home. The individual

could be seeking entry for a finite period of time in order to visit family, vacation, conduct business or attend school. Finally, they could be a legal migrant or refugee permanently resettling in the state. There are also many illegitimate reasons why an individual seeks admission into a state. They may seek admission in search of unauthorized employment, are entering in furtherance of a criminal act, or to carry out activities relating to terrorism. An individual seeking entrance to a state for illegitimate purposes may use a legitimate reason as cover in an attempt to convince the state's officials who are screening them that they are not a threat.

At a port of entry, the state's officials must also ensure that the individual seeking admission has the documents required for their requested entry. The two main travel documents that allow individuals to travel across international borders are passports and visas. A passport is an identity document usually issued by a state to an individual who has citizenship or nationality claim to that state and it is recognized by other states as a legitimate travel document. In its most basic form a passport contains biographical data such as name, nationality, place and date of birth, a photograph and pages in which other nations can affix visas or place stamps indicating entries and exits across their borders. Some passports are Machine Readable Passports, which allow for biographical and passport information to be read by a machine at check-in and border crossings. In reality, a passport is much more than all this: it serves as a mini-biography, showing who you are, where you are from, where you have been and for how long. In today's world of increased international travel, the passport has emerged as a vital instrument of an individual's international mobility. The passport is the primary document by which mobile individuals are identified, tracked and regulated (Salter 2004: 72).

The passport is supplemented by the visa system, with which a country may vet potential travelers and exercise control over potential entrants before they arrive at the border (Salter 2004: 73). A visa is permission granted to an individual to apply for admission at its border. It is usually issued outside the issuing country at an embassy, consulate or other recognized authority. A visa also states what an individual may do if granted admission, as well as for how long. It allows travelers to enter a country as tourists, for business, to attend school, to seek employment or work, or for a variety of other purposes. The amount of information contained on a visa varies greatly not only from nation to nation but between different periods of issuance. Some visas may contain much of the same information that is found in a passport, or they may have as little information as a number, the status of the traveler and a date of expiration. When a person who desires to enter a country but lacks the required documents and has no hope of obtaining these documents legitimately, they will often attempt to gain entry by using fraudulent documents to trick the state's officials into believing they qualify for entry (Fraudulent documents will be covered in great detail later in this chapter).

Finally, the state's officials must ensure that the individual seeking entry into his country is not already identified as being ineligible for entry or as posing a threat to the country. Most states make lists of these individuals readily available to their frontline border officials, usually in the form of large databases numbering in the millions for some Western nations. These lists can be checked by officials when an individual applies for admission via a computer systems specially designed to be queried at a point of entry.

In some cases, these databases are shared among several states. The Schengen Information System (SIS) is one example of this sort of government partnership. The

Schengen Agreement is a European border control regime in which states have harmonized their border polices and now issue a common visa and allow for the free movement of people and goods within the member states. The SIS allows border guards and police in Schengen member states to access a common database that collects information on trans-border crime and asylum claims (Salter 2004: 87). All EU members except the United Kingdom, Norway and Iceland are connected to the system. SIS contain data on illegal migrants; lost, stolen and false travel documents; wanted or missing persons; and stolen goods and counterfeit notes. As of June 2002, approximately ten million people were listed in the system (Koslowski 2004: 10). Increasingly, these lists include not only biographical data and travel document data but also biometric data such as fingerprints, iris scans or facial recognition. Even when he has the legal documents for entry, it will be nearly impossible for a terrorist to enter a country when his name is on the database of those ineligible for entry or who pose a threat to that country. The terrorist, when faced with this situation, will often resort to attempting to enter his target country with fraudulent documents in order to avoid detection.

Individuals who attempt to cross a state's borders by sea usually do so in one of three types of vessels: passenger liners such as cruise ships, as a crewman on commercial vessels such as cargo ships, or private vessels such as yachts. Just as those who arrive by air, individuals arriving by sea can arrive from anywhere they can board an ocean-faring vessel. Those who arrive at a port of entry by sea have the same documentary requirements and face much the same process as those who arrive by air, though all three types of sea vessels provide new set of challenges. Given the secure nature of an airport, arriving at a port of entry by air and avoiding contact with border officials is extremely

difficult without the assistance of corrupt border or airport officials. Given the vastness of the oceans, the length of coastlines and the variety of vessels, the same security does not exist at ports of entry on the sea.

Someone who is trying to enter a state without detection by that state's border authorities can stow away on a vessel that is bound for his target state. This means the person boards the ship either without the crew's knowledge or with the assistance of a crew member. The stowaway then hides on the ship until they reach its destination, at which time he tries to disembark the ship without the knowledge of the crew or border officials. Given the size of many seaports, this feat is much more easily accomplished than at an airport.

Individuals or entire groups of people who are attempting to enter without detection can actually be loaded into a vessel in shipping containers. This can occur with or without the knowledge of the ship's crew, depending on the size of the vessel. Once the ship reaches it final destination, the container is then unloaded with the rest of the cargo. Unlike the case of an individual stowing away on ship, clandestinely entering a state via an ocean vessel using this method requires a great deal of coordination at both the port of departure and the port of arrival. Usually the logistics of such an operation are arranged by sophisticated smuggling operations (Alien smuggling will be discussed in greater detail later in this chapter).

Individuals can try to avoid border officials by arriving on a private vessel and landing on a state's shores somewhere that's not a designated port of entry. These vessels can range in size from very large, such as the famous case of the Golden Venture when a large vessel carrying scores of Chinese ran aground off the coast of New York in the

early 1990s, to small, make-shift rafts that are often associated with people who flee

Cuba for south Florida. Unlike with stowaways, in the cases of private vessels coming

ashore other than at a designated port of entry, the crew is always complicit. As with the

case of people hidden in a ship's cargo, this type of clandestine entry into a state usually

involves sophisticated smuggling organizations. The bigger the vessel, the more likely a

smuggling organization is involved. In addition, the likelihood of this method being

employed to clandestinely enter a state is directly related to the size of a state's coastline

and the amount of resources dedicated to protecting its shores.

Just as a long coastline can present challenges to a state securing its territory, so to

can a vast land border. Similar to official ports of entry that may dot a state's coastline,

many official ports or entry and border checkpoints may also be spread across a land

border. The documents required to and the process for entering at a land ports are similar

to those at air and sea ports of entry. The means of avoiding detection at a land port of

entry are also similar. An individual can use fraudulent documents to attempt to trick a

border official into believing that he is eligible for entry, may hide within a vehicle, or

might be loaded in the cargo of a truck or railcar. When a state's border is vast, and when

there are large distances between border checkpoints, the level of sophistication need

only be a strong set of legs to clandestinely cross the border between checkpoints. When

the environment along a state's border is particularly harsh or a state invests significant

resources to parole areas between checkpoints, an individual may need the assistance of a

smuggler to guide them safely across the border.

Those who enter a state by crossing a border over land differ from those who

arrive by sea or air, as they arrive directly from a neighboring state, unlike those arriving

by air or sea who can come from anywhere in the world. This does not mean that a state need only be concerned with its neighbor's citizens crossing the border. Often an individual hoping to gain entry into a particular state will first enter the state's neighbor by air, sea or land and then cross by land to reach his final destination. The reason for doing this is because an individual may lack the resources or the opportunity to enter their target state, or the neighboring state's ability to screen its cross-border activity may not be as sophisticated or as effective as the target country. This creates a situation where one state's ability to manage and secure its borders directly affects its neighbor's ability to do the same. Globalization has affected every state's ability to manage and secure its borders by making it harder to facilitate legitimate trade and travel while keeping out undesired clandestine transnational actors such as terrorist.

Global economic interdependence has made traveling across international borders easier for terrorists. The volume of world trade in goods and services has increased more than 39 percent between 1995 and 2001 (Andreas 2003: 79). This growth in economic interdependency of states has diminished borders as a new openness developed in order to facilitate international trade and travel. Terrorists were able to take advantage of this openness to move around the world to achieve their goals.

Al-Qaeda's Travel Operations

The importance of clandestine border-crossing was not lost on al-Qaeda and other terrorists. To understand this importance, one only needs to look at al-Qaeda's leadership and operations. Abu Zubaydah, Al-Qaeda's chief of staff before his capture, had a number of passports and aliases that enabled him to act as a hub within the network because he could move freely and coordinate activities between nodes. At the time of his

capture, he was in possession of a number of blank and forged Saudi passports (Takeyh 2002 pp. 101). Khalid Sheikh Mohammed, mastermind of the 9/11 attacks, is known to have nearly thirty aliases and has used passport from Bahrain, Saudi Arabia and Pakistan (Fouda 2003: 97). Ayman Zawahiri has used Swiss, Russian and other passports to travel the world, including arriving in the United States for a fundraising trip in 1993 (Sageman 2004 pp. 43). Even Osama bin Laden reportedly had passports from Sudan, Bosnia and Albania (Takeyh 2002 pp. 101).

Al-Qaeda has devoted extensive resources to facilitate their members' travel across borders. Part of their strategy was to acquire and manipulate passports, entry and exit stamps, and visas. High-level members of al-Qaeda were also expert document forgers who taught their craft to other terrorist, including 9/11 ring-leader Mohamed Atta (9-11 Commission 2004a: 1). The organization had a "division of passports and host country issues" located at the Kandahar airport and managed by al-Qaeda's military chief Muhammed Atef. This division would alter travel documents including passports, visa and identification card. Al-Qaeda operatives would also examine the passports of all new arrivals in Afghanistan, copying any new visas and entry and exit stamps (9-11 Commission 2004a: 56-57). This practice did not end with the training camps in Afghanistan. When Al-Jazeera TV reporter, Yosri Fouda, secretly met with Khalid Sheikh Mohammed prior to his capture, Mohammed requested Fouda's passport so that he could see the serial number on his Pakistani visa issued in London (Fouda 2003 pp 37).

The importance of the ability to clandestinely cross national borders by network members was so important to al-Qaeda that it was incorporated in their training. In an al-

Qaeda training manual seized by police in Manchester, England while searching a

member's home, an entire lesson is dedicated to teaching members how to cross borders.

This lesson reads in part:

1. **Keeping the passport in a safe place so it would not be seized by the security apparatus, and the brother it belongs to would not have to negotiate its return (I'll give you your passport if you give me information)**
2. **All documents of the undercover brother, such as identity cards and passport, should be falsified**
3. **When the undercover brother is traveling with a certain identity card or passport, he should know all pertinent {information} such as the name, profession, and place of residence**
4. **. The brother who has special work status (commander, communication link,....) should have more than one identity card and passport. He should learn the contents of each, the nature of the indicated profession, and dialect of the residence area listed in the document**
5. **The photograph of the brother in these documents should be without a beard. It is preferable that the brother's public photograph (on these documents) be also without a beard. If he already has one (document) showing a beard, he should replace it.**
6. **When using an identity document in different names, no more than one such document should be carried at one time.**
7. **The validity of the falsified travel document should always be confirmed.**
8. **All falsification matters should be carried out through the command and not Haphazardly (procedure control)**
9. **Married brothers should not add their wives to their passports.**
10. **When a brother is carrying the forged passport of a certain country, he should not travel to that country. It is easy to detect forgery at the airport, and the dialect of the brother is different from that of the people from that country.**
(al-Qaeda, undated, Lesson Three)

It is important to mention each of these steps because, as we will see, members of al-

Qaeda's network strictly adhere to the steps in this lesson, including all of the 9/11

hijackers.

The background and experiences of many members of al-Qaeda also help

facilitate their travel. Most members of the global Salafi jihad movement are better

educated than many other Muslims around the world. Most went to college and have

studied technical fields such as science, engineering or computer science. While the

image of terrorists held by many unfamiliar with the nature of the global Salafi jihad

movement is that they are relatively ignorant, naïve and unsophisticated in the ways of

the world, most members of the movement are "global citizens" familiar with many

countries. They can operate as effectively in the West as they can in the Muslim world

and are able to speak several languages with equal ability (Sageman 2004:76). It is

estimated that up 70% of those who joined the movement before 2001 did so in countries

where they had not grown up. Whether they were expatriates, students, workers, refugees

or fighting against the Soviets in Afghanistan, their travel took them away from home

and family and exposed them to the outside world (Sageman 2004: 92). This exposure to

the outside world and familiarity with international travel has helped to facilitate their

ability to move around the world in a clandestine manner and in a variety of methods.

Terrorist Travel Methods: The visa system

As stated earlier, the visa system is a way for a country to vet potential travelers

and to exercise control over potential entrants before they arrive at the border. Among the

terrorists who have used the visa system to enter the United States are all nineteen of the

September 11 hijackers. The success of the 9/11 plot depended on the ability of the

hijackers to obtain visas and pass US immigration and customs inspections. The nineteen

submitted a total of twenty-three visas application, of which twenty-two were approved,

and they used these visas to enter the United States a total of thirty-three times. It is likely

that some of these hijackers had indicators in their passports that may have linked them to

al-Qaeda. However, this intelligence was not developed prior to September and therefore

State Department personnel and border inspectors were not trained to spot these

indicators. Gaining entry into the United States on a visa was important to the hijackers

because immigration regulations offered a tourist with a visa the opportunity to stay for

six months. This six-month authorized period of admission allowed the hijackers

sufficient time to prepare for their operation. In fact, on September 11 only one of the

hijackers had an expired immigration status (9-11 Commission 2004a: 7-8).

One of the aspects of the 9/11 hijackers' travel method that makes them an

important cases study is their adherence to al-Qaeda's travel strategy as dictated by the

seized training manual. Before applying for a visa or attempting to cross a border, many

of the hijackers obtained new passports to hide previous travel or to hide perceived

"radical appearance" such as a beard. Additionally, when applying for visas the hijackers

were intentionally vague on their applications as to where they were to stay or the reason

for their trip. They might have chosen to list occupations or addresses they were familiar

with to be able to answer questions if necessary. Those who were married did not list

their wives or children, all in accordance with the manual.

The 9/11 hijackers were not the first terrorists to enter the United States with a

visa. Mohammed Salameh, a participant in the first World Trade Center bombing and

who is now infamous for trying to retrieve the deposit for the rental truck used in the

bombing, entered the United States on a six month tourist visa in 1988. He overstayed his

authorized period of admission and subsequently applied for amnesty. Despite having his

application denied he remained in the United States illegally (Camarota 2002: 25).

Another terrorist who overstayed his authorized period of admission is Laqfi Khalil who

was convicted of plotting to bomb the New York Subway system in Brooklyn. He

entered the United States in late 1996 on a transit visa, claiming he was going to continue

on to Ecuador. However, he remained in the United States until his arrest (Camarota

2002: 25). Salameh, Khalil and the 9/11 hijackers are just a few examples of terrorists

who have entered the United States with visas. However, a visa is not always required for terrorists to cross borders.

Terrorist Travel Methods: Visa-free travel

The growth of international mobility in recent decades has put a great strain on the visa issuance process and has resulted in the emergence of visa-free zones. The Schengen Agreement in Europe and the United States' Visa Waiver Program (VWP) are two examples of visa-free zones or multilateral agreements. Visa-free travel allows citizens of one county to enter others without a visa. This right is extended to all parties within the agreement. In Europe, the most important institutional mechanism for border control cooperation has been the Schengen agreement, which was implemented in 1996 and subsequently incorporated in the European Union (EU) framework. All EU countries except Ireland and Great Britain are now Schengen members (Andreas 2003: 101). The Schengen agreement has allowed not just for the free movement of people, goods and services within member countries but it also allows for citizens from countries outside the Schengen agreement to apply for visas that are valid for entry into all member countries. Once travelers are admitted into one of the member states, they are free to move between all other member states. The result has been an elimination of internal border inspections between members and a move toward tightening external borders with non-Schengen members.

The United States' Visa Waiver Program allows citizens of certain countries to enter the United States as a visitor for business or pleasure for up to ninety days without obtaining a visa. This agreement is reciprocal, so citizens of the United States do not need a visa to enter those states that are included in the VWP. The VWP was first established

in 1986 with eight countries as members. The program is currently available to citizens of

35 countries, with 8 new countries added in 2008, so long as the traveler is in possession

of a Valid Machine Readable passport if the passport was issued prior to October 26,

2005, and contains a digital photograph if passport was issued prior to October 26, 2006

and the passport contains an integrated data chip if issued after October 2006. (DHS

2006) Since the VWP is a reciprocal agreement, citizens of the United States have visa-

free access to all Schengen members.

The economic, commercial and social benefits of visa-free zones or visa-free

agreements are enormous. They also create a great security risk when terrorists in

possession of qualifying travel documents are able to use visa-free travel to circumvent

the additional vetting process provided by the visa system. As a result, VWP passports

are a valuable commodity for terrorists and other CTAs. When individuals hold VWP

passport they can gain entry to a Schengen member, the United States, and many other

states without a visa.

While the United States is not part of a regional border free zone like the

Schengen agreement, it has thousands of miles of borders with Canada and Mexico that

are porous. Therefore, the United States is affected by the border policies of its neighbors

to the north and south. Canada allows visa-free access to more countries than the United

States. Canada and the United States also have a unique entry requirement agreement.

Citizens from one country can enter the other country for up to six months without a

passport and without having to complete any immigration forms when entering the

other's territory by land.

The risk of terrorists exploiting the Visa Waiver Program and the Schengen Agreement is heightened by the rise of the global Salafi jihad movement among first and second-generation immigrants in Western Europe. Many immigrants to Western societies find it difficult to feel as if they are a part of that society. They are immersed in a culture that is quite literally foreign to them. The values of the society may be at odds with their beliefs; they may have difficulty with the language or may appear and act differently in social settings. These assimilation problems are compounded by racism by the population that subjects some immigrants not only to ridicule but also to discrimination. This discrimination may make finding suitable employment a difficult task, crushing the dream the immigrant or their parents had when they began the journey to their new home. Often these immigrants, through the technology revolution of globalization, remain in contact with their homeland and yearn for the familiarity of the society they left behind. They will often attempt to relieve these feelings of isolation they suffer as a result of alienation by looking to others who have similar circumstances in order to obtain a sense of belonging. This sense of alienation among immigrants, both first and second generation, appears to be more pronounced in Europe. The United States, with its long-standing tradition of being a country of immigrants, has enjoyed somewhat more success than Europe in absorbing immigrants and their children. In addition, immigration to the United States is primarily from Asia and Latin America, while the sources of most migration to Europe are Muslim nations (Leiken 2004a: 20)

As a result of this alienation, throughout Europe young Muslims are becoming angrier, more radical and more active. Excluded by a racist society, denied equal opportunities and denigrated by those around them, they have developed an exclusivist

mindset. They begin to see themselves first and foremost as Muslims, and any other

identity such as citizenship and immigration status are viewed only as administrative

details (Benjamin and Simon 2002: 175) It is religion and the Muslim identity that these

first and second-generation immigrants turn to for acceptance, and in the process they

become more isolated and alienated from the society in which they live. Many of these

alienated individuals who have found acceptance in the global Salafi jihad movement

possess passports which making them eligible to cross borders under the Visa Waiver

Program and the Schengen agreement.

Terrorists have and will continue to take advantage of all these situations. Two of

the most infamous cases of terrorists using the Visa Waiver Program to attempt to enter

the United States are Zacarias Moussaoui and Richard Reed. Moussaoui, who was

indicted as a co-conspirator in the 9/11 plot, used his French passport to enter the United

States in February 2001. Reid, the convicted "shoe bomber," was able to board a US-

bound plane with only his British passport. Both Moussaoui and Reed were second-

generation immigrants that experienced alienation from living in European society

(Letzing 2005: 1). Many of the terrorists who planned and carried out the Madrid train

bombings in March 2004 more easily traveled throughout Europe because of the

Schengen Agreement and examining specific instances is difficult because these

individuals did not go through border checks when traveling between Schengen

members.

The Visa Waiver Program and the Schengen agreement are not the only visa-free

agreements that terrorist have used to their advantage to plan, coordinate and carry out

attacks. Malaysia has a visa requirement policy that, though it's not a specific agreement

with other countries, many terrorists have found appealing. Until recently, Malaysia did not require visas from citizens of other Muslim nations. In addition, Malaysian security was reputed to be lax when it came to Islamic jihadists (9/11 Commission 2004b: 158). Kuala Lumpur was chosen as the spot for a meeting to put the final touches on the USS Cole attack and to discuss plans for the 9/11 plot. The meeting, which was attended by Khalid Sheikh Mohammed, Hambali and two of the eventual 9/11 hijackers, was held in Malaysia because of its lack of visa requirements for Muslims. The Visa Waiver Program, the Schengen agreement, and Malaysia's visa policy have one common characteristic: they require a traveler seeking entry to hold an eligible country's passport. When a terrorist or other CTA does not have a legitimate right to carry one of these countries' passports, lacks other required documents, or needs to enter a state using an identity other than his own, the use of fraudulent travel documents can be a valuable tool to facilitate his border-crossing.

Terrorist Travel Methods: Fraudulent Documents

For terrorists, fraudulent travel documents are as important as weapons. Terrorists must travel clandestinely to meet, train, plan, case targets and attack (9-11 2003b: 384). This often requires them to travel under false identities to avoid detection or raising suspicions. It also may require them to travel to nations they could not legitimately gain admission to because they lack the required passports or visa. Finally, a terrorist might need to conceal his previous travels in order to avoid raising the suspicion of authorities. In all these cases, fraudulent documents are the key to success. Fraudulent documents provide mobility, which is a requirement for any member of an international terrorist organization.

There is no shortage of documents available to al-Qaeda and other terrorist organizations. It is estimated that as many as ten million lost or stolen travel documents are in circulation worldwide (Levine 2004: 35). If terrorists are unable to alter a document in their possession or cannot find a look-alike they can just make their own. If that does not work they can always try to obtain one by fraudulent means or from corrupt government officials. Terrorists have used these types of fraudulent documents to travel around the world and will most likely continue to use these methods.

There are five major types of fraudulent documents that terrorists use to travel the globe. These five types fall into three different categories: illegitimate documents, legitimate documents and a combination of the two. Illegitimate documents are documents that are counterfeit or documents that have been altered. Legitimate documents are documents that are genuine and unaltered but are not being used by the true owner. This includes documents that are obtained by fraud and impostoring. The final type of fraudulent document is stolen blank documents, which is a combination of the two previous categories.

A counterfeit travel document in the most basic terms is a fake document. A counterfeit travel document can be completely counterfeit or be partially counterfeit (e.g., only the biographical data page). The goal of a good counterfeiter, whether forging documents, money, merchandise or any other item, is to get the product to look as close to the original as possible. With the technology available in today's computerized world, a counterfeiter can create convincing documents on a color laser printer; however, more sophisticated counterfeiters will use the same professional printing techniques as the manufacturers of genuine travel documents. Almost all travel documents have added

security features to help combat counterfeiting, many of which are found on paper

currency, including watermarks, holograms, digitized photographs and optical variable

ink. The closer a counterfeiter comes to mimicking these security features the better the

chance his product will fool security and border personnel.

Riduan Isamuudin (aka Hambali), the operational chief of al-Qaeda's Southeast

Asian branch, Jemaah Isamiah, is a prime example of how terrorist have used counterfeit

travel documents in order to cross borders clandestinely. Hambali was one of the most

wanted terrorists in the world at the time of his arrest in Thailand in 2003. Hambali fled

Malaysia by boat and trekked across land through Burma to Laos. He entered Thailand

over a remote footbridge in northern Thailand using a counterfeit Spanish passport. To

avoid detection the passport contained a long complicated Spanish name. Hambali also

shaved his beard and underwent plastic surgery in an attempt to hide his identity (Baker

2003). These steps allowed Hambali to successful avoid detection at a border crossing;

however, going to the extreme of undergoing plastic surgery in an attempt to conceal

one's true identity from border officials would only be required by the most wanted

terrorists.

When document forgers have genuine travel documents available, they can alter

the documents so they can be used by terrorists or other CTAs to travel across borders.

There are several techniques that forgers use to prepare altered travel documents. The

forgers may substitute the photo in the document, which entails removing the original

photo from a passport or visa and replacing it with the photo of the intended user. The

forger may also alter the biographic data in order to change the identity listed on the

document, so that an individual who may be known to authorities can travel under a new

identity. Forgers might also attempt to change their client's travel history by adding or

eradicating entry-exit stamps and visas contained within the passport. These types of

altered documents were used by Ahmad Ajaj, Ahmed Ressam and many of the 9/11

hijackers to fool border officials and facilitate their entry.

Ahmad Ajaj was Ramzi Yousef's traveling companion on August 31, 1992, when

he attempted to enter the United States at JFK International Airport. Unlike Yousef, Ajaj

did not present himself to border officials and request political asylum as a means of

entry. Rather, he attempted to enter the United States under the Visa Waiver Program

using a photo-substituted Swedish passport. After he was intercepted, his luggage was

searched and found to contain bomb-making manuals, terrorist videos and literature, and

other fraudulent documents including the passport Yousef used to board a flight in

Pakistan (9-11 Commission 2003a: 47-48). Many of the 9/11 hijackers also had their

documents altered. Knowing that previous travel to certain destinations might raise the

suspicions of border officials, they had stamps and visas eradicate or added to their

passports to hide their travel prior to entering the United States (9-11 Commission 2004a:

pp. 54).

Terrorists can also travel with genuine travel document by impostoring or

documents obtained by fraud. Impostoring is when a traveler uses the legitimate travel

documents of someone who looks like them in order to trick security officials into

thinking that they are the individual in the document's photo. This technique is similar to

an under-age drinker attempting to enter a bar using a family member's identification. In

cases of impostering, the user may try to alter their appearance by growing a beard,

getting their hair cut a certain way, or trying to conceal or add facial features such as

moles, instead of altering the document. The added benefit of impostering is that a document can be recycled after it is used.

Documents obtained by fraud are genuine documents in which deceit occurs or false information is provided at the time of application or issuance. The fraud may be perpetrated by the applicant or by a corrupt official who has access to documents. Passports and other documents can also be obtained by fraud with the use of breeder documents, which are documents that are presented at the time of application in support of the identity of the applicant. For example, in the United States, when applying for a passport a birth certificate and driver's license are two examples of documents that can be presented in support of the applicant's claim to US citizenship. This means that a passport identifies an individual according to other documents, and these documents can be fraudulent (Salter 2004: 86). If the applicant provides false breeder documents at the time of application and this fraud is not detected, the applicant will then be issued and be able to use a genuine travel document to which he is not entitled. The large number of jurisdictions who issue breeder documents such as birth certificates and drivers' licenses compounds this problem. The problem is compounded even further when false information is detected before issuance but, and this is the case with many of the 9/11 hijackers, a genuine visas is still issued anyway, allowing them to apply for admission into the United States.

The mastermind of the 9/11 plot, Khalid Sheik Mohamed, also obtained a US visa through fraud. On July 23, 2001, Mohamed applied for a tourist visa at the US Embassy in Riyadh, using a Saudi Arabian passport in the name of Abdurrahman al Ghamdi. Since Mohamed used an alias, his visa application was approved despite having been on a

terrorist watch list since 1996. There is no evidence that Mohamed used this visa to enter the United States but he listed his intended address as New York (9-11 Commission 2004a: 29). Given the date of issuance and the intended address, it could be surmised that Mohamed may have been contemplating coming to the United States in order to assist in the 9/11 plot but may have felt that this would cause an unnecessary security risk.

The third category of fraudulent documents is a combination of illegitimate documents and legitimate documents. These are stolen blank passports. When passport manufacturers ship passports to the issuing authority they are completed products, except for the biographical data, a photograph and perhaps a machine-readable zone. If a passport is stolen before it is issued, a document forger needs only to add a photograph and biographical data and he may create an almost foolproof document for his clients. Since all of these documents are genuine except for the photo and biographical data, this leaves few, if any, detection points for security officials to spot fraud. The security risks of these types of documents are compounded by the fact that nearly two million blank EU passports have been stolen in recent years (Salter 2004: 82). Most of these passports could be used to enter the United States without a visa under the Visa Waiver Program. The only real defense is placing the document numbers of these stolen black documents in border lookout systems if they are provided by the issuing state. Unfortunately, the better document vendors are well aware that their products may be listed in border lookout systems and will attempt to alter the passport number, decreasing the likelihood of their detection.

Stolen blank passports have been and will continue to be used by terrorists. On September 9, 2001, Northern Alliance leader Ahmed Shah Massoud was killed in a

suicide attack in Afghanistan. His assassins traveled to Afghanistan on stolen blank

Belgian passports (World News 2004). The way in which blank passports are stolen is

also becoming increasingly violent. In July 2003, two gunmen hijacked a van near

Marseille, France, and stole 5,000 blank French passports. In February 2004, thieves in

France took another 9,300 blank passport and burned a stolen van in an attempt to destroy

evidence. Individuals with possible links to terrorist organizations have been intercepted

trying to use these very same passports while attempting to enter the United States

(Jennings 2004).

Terrorist Travel Methods: Avoiding border inspections

The most desired method for a terrorist to cross a border is by using a legitimate

travel document. When one cannot be obtained or used because the individual's links to

terrorism may be known, the terrorist can attempt to enter through a border checkpoint

with a fraudulent travel document, and the lack of travel documents will not deter a

determined terrorist from crossing a border through other avenues. These methods,

including stowing away on ships, entering without inspection by illegally crossing the

border, requesting political asylum, and utilizing professional alien smugglers all allow

the terrorist to circumvent travel documents requirements.

Abdelghani Meskini and Abdel Hakim Tizegha, who were involved in the

millennium plot to detonate a bomb at LAX international airport, both entered the United

States by stowing away on ships from Algeria to Boston. Tizegha arrived in Boston in

1993 but was detected while on route and turned over to immigration authorities upon his

arrival. He requested political asylum and was released. Meskini successful avoided

detection when he reached Boston in January 1995 and lived in Boston, New York and

Canada. He still lives in the United States under the witness protection program because of his testimony against the other conspirators (Camarota 2002: 34).

Gazi Ibrahim Abu Mezer, who conspired with Lafi Khalil to bomb the New York subway system, entered the United States by crossing the US-Canadian border without inspection. Mezer, after being denied a student visa for the United States, obtained one for Canada. He never intended to study in Canada and was apprehended three times attempting to illegally cross into the United States. Canada refused to take Mezer back after his third apprehension, so US border officials released him pending his deportation hearing. Not surprisingly, he did not show up for his hearing and his lawyer told the court that he had voluntarily returned to Canada, a claim proven to be false when he was arrested and police found pipe bombs in his apartment (Camarota 2002: 30).

Requesting political asylum is another technique used by terrorist to gain entry into countries. This technique is not an attempt to avoid border officials but rather is an attempt to gain entry into a country by asking for protection from political persecution. This was part of the technique used by Ramzi Yousef to gain entry into the United States. However, this technique is risky for individuals whose terrorist affiliations may already be known to security agencies. When someone requests asylum, they are alerting border officials to their presence. This may lead to additional scrutiny and to security officials uncovering the true intentions of their arrival. Ramzi Yousef was not known to security officials before his arrival to New York and was released with little investigation. Ironically, it was the case of Ramzi Yousef that led to increased scrutiny being placed on individuals seeking asylum when crossing the border, leading to the detention of many asylum seekers who would not have otherwise been detained.

Most terrorists who have used asylum to gain entry into a state did so prior to joining global Salafi jihad movement. Osman Hussain, one of the failed London subway bombers, is one example. Hussain, an Ethiopian whose real name is Hamdi Issac, claimed when he arrived in London for the first time that he was a Somali and requested political asylum (Lewis 2005). What makes Hussain's case interesting is that he is an example of an immigrant who became alienated because he was unable to assimilate into British society. This resulted in his turning against the country that had offered him protection.

Terrorist Travel Methods: Alien Smuggling

While stowing away on ships, clandestinely crossing land borders and arriving at a state's border and requesting asylum are all methods available to some terrorists, they can be out of reach for others. When terrorists can't take advantage of these options, they may turn to professional alien smugglers to achieve their goal. Alien smuggling is known by many names, including: people smuggling, human smuggling and migrant smuggling. Equally as diverse are the definitions of alien smuggling, which range from legal definitions, descriptive definitions found in social science text, to definitions given by advocacy networks that see it as a global problem and that frame the issue in an attempt to promote action. Governments and activists construct the problem in different ways (Kyle and Koslowski 2001: 5-6). When discussing alien smuggling as it relates to terrorists' travel methods, Peter Andreas provides the most appropriate definition. Andreas defines smuggling as "the practice of bringing in or taking out without state authorization…what has varied across time and place is the degree, nature, methods, and organization or such smuggling" (2001:108). When people are smuggled it becomes alien

smuggling. Mahmoud Youssef Kourani is one such person. Kourani was successfully smuggled across the US-Mexico border in February 2001 in the trunk of a car. He was later arrested in Dearborne, Michigan and indicted as a member of the terrorist group Hezbollah (U.S. v. Kourani 2003). While Kourani was not affiliated with al-Qaeda, alien smuggling may be the future strategy for terrorist travel.

With the elimination of bases of operation in Afghanistan, al-Qaeda no longer has the complex infrastructure to move terrorists around the world. The US invasion also spread al-Qaeda's membership around the world with what many believed to be little or no means of operational support. Even with the resurgence of the Taliban and those sympathetic to the global Salafi Jihad movement in Afghanistan and the North Western Frontier Provinces of Pakistan, al-Qaeda still lacks the capabilities it possessed prior to September 11. What has not changed is the importance of terrorists' ability to cross borders that al-Qaeda's networks provided. Alien smugglers may be utilized by terrorist to fill this void. Another factor that may require terrorists to turn to alien smugglers is target-hardening efforts at ports of entry throughout the world. The terrorist attacks of September 11 have turned the spotlight on the vulnerability of border crossings. The result has been tighter security and entry requirements and border crossings in the United States and around the world. As a result, many clandestine border crossers have to use remote land borders in an attempt to gain entry to a country. These areas, like the United States-Mexico border, are often harsh environments that are not easily crossed. A terrorist who is unfamiliar with the area or crossing route would have little choice but to rely on a professional smuggler to assist him in his journey, and there is no shortage of smugglers willing to lend their services to terrorists, so long as the fee is high enough.

There is evidence that terrorist organizations are already using alien smugglers or are in the business themselves, as a means to both cross borders and in order to raise funds to carry out operations. Salim Boughadr Mucharrafille ran an alien smuggling ring out of the La Libanesa café in Tijuana. He is believed to have smuggled members of Hezbollah and to date he is the only alien smuggler with ties to terrorism convicted in the United States. While security officials maintain that they know of no case of an al-Qaeda operative using smuggling operations to enter via the northern or southern border, they warn that intelligence suggests al-Qaeda is eyeing these borders as a way into the United States (Arrillaga 2005).

There is evidence that al-Qaeda-affiliated organizations are not only using smuggling operations but are running them in other parts of the world. Abu Zarqawi, the man called the leader of al-Qaeda in Iraq prior to his death, and his al-Tawhid network established an alien smuggling and document-forgery ring as a two-way "underground railroad" between Western Europe and the Middle East. This pipeline allowed radicalized European Muslims to flow into Iraq and the Middle East and later moved the global Salafi jihadists back into Europe. Other individuals linked to al-Qaeda and its affiliated networks involved in alien smuggling include some of the terrorists who were involved in the 2004 Madrid Train bombings (Leiken and Brooke 2004a). It seems likely that terrorists will turn to existing smuggling networks for assistance rather than trying to reinvent the wheel.

Terrorist Travel Methods: The Case of Ahmed Ressam

When terrorists need to travel clandestinely across international borders they will employ any means available. No one terrorist exemplifies this fact more than Ahmed

Ressam, who became known as the "Millennium Bomber" for his plot to bomb Los Angeles International Airport. For almost a decade, Ressam used a variety of different techniques previously discussed in this chapter to cross borders. Ressam made his first border crossing as an adult in September 1992 when he entered France from Algeria, using a visa that was issued to him as a child so he could enter France for medical treatment. Since his visa was issued to him as a child, it expired soon after he arrived in France. As a result, Ressam obtained a counterfeit French passport in the name of Nasser Ressam to travel around Europe and re-enter France (Bernton 2002: 5). Ressam was arrested in 1993 on immigration violations and, facing deportation back to Algeria, he decided to flee France. Ressam next used a photo-substituted French passport in the name of Tahar Medjadi to try to gain entry into Canada. Ressam was intercepted at Montreal's Mirabel Airport, but was released on bond and given a date for his asylum hearing after requesting political asylum. He never appeared for his hearing and easily blended into Montreal's Muslim community.

While in Canada, Ressam became involved with radical Muslims connected to al-Qaeda. It was these links to the global Salafi jihad movement that allowed Ressam to go to Afghanistan to attend a terrorist training camp. However, to leave Canada and journey to Afghanistan he needed a new identity. In March 1998, Ressam used a baptismal certificate stolen from a church in Montreal to obtain a genuine Canadian passport in the name of Benni Antoine Norris. As Benni Norris, Ressam flew from Toronto to Germany and then on to Pakistan. Once in Pakistan Ressam travel to Peshawar were he met Abu Zubaydah, al-Qaeda's number three man and chief travel facilitator. Zubaydah made arrangement for Ressam to illegally cross the border into Afghanistan so that he could

attend al-Qaeda's training camps. After completing his training, Ressam crossed illegally back into Pakistan. Then, under his assumed identity of Benni Norris, Ressam flew from Pakistan to Seoul to Los Angeles and finally on to Vancouver. With his Canadian passport Ressam was able to fool both Canadian and American border officials. Ressam was not intercepted until December 1999 when US Customs officials caught him trying to enter the United States with his fraudulently obtained Canadian passport in order to carry out a bomb attack on Los Angeles International Airport.

Over the course of eight years Ressam used legitimate travel documents, counterfeit documents, altered documents, and documents obtained by fraud, as well as crossing illegally over land borders. By employing a variety of methods, he was able to travel around the world despite the knowledge within the intelligence communities of several nations that he had ties to the al-Qaeda network. What the Ressam case demonstrates is the variety of options terrorists have available to successfully cross borders, as well as showing the weaknesses in border security around the world. What these examples do not provide is a broad picture of what methods members of the global Salafi jihad movement use to cross borders and data on what country's nationals are the biggest threat to the West. Without a solid understanding of *what* methods are used, *how* these methods are used, and *where* the threat comes from, can an effective strategy to combat terrorist travel be constructed? This chapter has already explored the how, and to fill in the voids of *what* and *where* we turn to the work of Robert S. Leiken and Steven Brooke.

Terrorist Travel Methods: A Quantitative Approach

Leiken and Brooke, in their 2006 article "The Quantitative Analysis of Terrorism and Immigration: An Initial Exploration," take a quantitative data analysis approach to examine the biographical data of 373 individuals charged, convicted and/or killed in connection with terrorist attacks in Western Europe and North America between 1993-2004 that were carried out as part of the global Salafi jihad movement. Through their analysis, Leiken and Brooke hope to better understand the relationship between terrorism and immigration. They find that 87 percent of terrorist in their sample were immigrants and conclude that "while most immigrants are not terrorists, most terrorists are immigrants" (507). More important than this conclusion is what Leiken and Brooke find regarding how those individuals in their sample crossed borders, what they call "immigration vehicles" (510).

Leiken and Brooke find that members of the global Salafi jihad movement have used every conceivable method to gain entry to target states, though they were able to find entry data on only 206 of their sample of 373 individuals. Of those individuals that Leiken and Brooke were able to find data; 33 percent use visas to gain entry into their target state, 23 percent gained entry through an asylum claim and only 6 percent entered their target state illegally (510). These figures, however, while a good starting point, do not appear accurate, as it is likely that the number of their sample that entered illegally is much higher than 6 percent. Firstly, no entry method was determined for 45 percent of Leiken and Brooke's original sample of 373. One reason for this high rate may be that many of these missing sample members entered their target state illegally by crossing a land border clandestinely, stowing away on a ship or by successfully avoiding detection

through the use of fraudulent documents. Secondly, as Leiken and Brooke admit,

collecting data on terrorists is inherently difficult because they operate secretly. Given

this fact, it appears likely that many terrorists have traveled illegally. Finally, Leiken and

Brooke wrongfully use asylum as one of their immigration vehicles. While the sample

members ultimately gained entry into their target state through an asylum claim, most

often this claim is only made after the terrorist is detected trying to gain entry illegally.

One needs to look no further than the millennium plot to find two examples. Ahmed

Ressam used a photo-substituted French passport in an attempt to gain entry into Canada

and claimed asylum. Abdel Hakim Tizegha requested asylum after arriving in the United

States by stowing away on a ship. In both cases, Ressam and Tizegha requested asylum

only after first attempting to enter their target state illegally. Even not including the entry

data on the 45 percent for whom no information could be found, if the 23 percent of

Leiken and Brooke's original sample of 373 who gained entry were correctly classified

by their initial entry attempt, there is little doubt that the number who entered illegally

would be significantly higher.

The important group of Leiken and Brooke's sample is the remaining 38 percent

for whom entry date could be located. This group consists mostly of European nationals

who entered other European nations under the Schengen Agreement. These individuals

would also be granted visa-free access to the United States under the Visa Waiver

Program. In essence, the nationality of these terrorists was their immigration vehicle

(510). Leiken and Brooke's data on terrorists who benefited from their nationality by

allowing them to utilized visa-free travel to enter a target state is supported by data on the

nationalities of the terrorists in their sample. When Leiken and Brooke examined the

biographical data of their sample and controlled for nationality, they found that 41

percent of the 373 terrorists in their sample held citizenship from a country in either

North America or a member state of the European Union (508). It is also important to

note that Leiken and Brooke's data set only includes those terrorist identified as part of

the global Salafi jihad movement prior to December 2004. This means that Leiken and

Brooke's data set does not include those individuals involved in the 2006 British airline

bombing plot. If their biographical data was added to Leiken and Brooke's sample, it is

likely that the percentage of terrorists who used their nationality as an immigration

vehicle and the percentage that held citizenship from a country in either North America

or a member state of the European Union would both rise. The 2006 British airline

bombing plot also illustrates a new set of problems border security officials must address.

Terrorist Travel Methods: New Challenges and a Need for Innovative Solutions

As chronicled in the previous chapter, it is believed that individuals connected to

both the 2004 London transportation system bombings and the 2006 British airlines

bombing plot were primarily second generation immigrants who have traveled to the

tribal regions of Pakistan to receive training in terror tactics. This phenomenon is not

exclusive to the citizens of the United Kingdom. Intelligence accounts appearing in

various media outlets have reported that since mid-2006 an influx of new recruits from

Western nations have joined the global Salafi jihad movement and entered the tribal areas

of Pakistan to train in terror camps. It is suspected that these terrorists, believed to come

from Great Britain, the Netherlands, Denmark, Germany, Romania and Estonia, may

have been dispatched to plan attacks against Europe and possibly the United States

(Thomas and Date 2008). Ironically, this was reported in the popular press just as the

Untied States expanded the Visa Waiver Program to include eight additional countries, including Estonia. There have also been numerous reports in the popular press concerning young men of Somali decent who are recruited in Minneapolis and other cities in the United States with large Somali populations and then journey to Somalia, train with al-Shabaab, an al-Qaeda linked terrorist group in Somalia, and return to the United States (Levine 2009).

What these two situations illustrate is a shift for officials tasked with border security. Traditionally, border officials were concerned with external threats in the form of individuals attempting to gain entry to a state in order to inflict harm on that state's population. Now, states have citizens who identify themselves with the global Salafi jihad movement. This has resulted in a greater blurring of the line separating external threats from internal threats. Border security officials must concern themselves not only with foreigners entering their state's territory but also with where their citizens have been. These circumstances have resulted in an environment in which those tasked with border security cannot act unilaterally. It requires borders officials to act together with international partners to collectively develop strategies to prevent terrorists from crossing borders to plan, coordinate and carry out attacks.

Following the terrorist attacks of September 11, it became evident that the perpetrators were able to exploit the openness of the Untied States and its border security apparatus in order to gain entry to train and carry out the attacks. While the United States talked of a collective effort with many nations to combat global terrorism, when it came to its efforts to prevent terrorists from crossing its borders, the Untied States initially acted unilaterally. Almost immediately following the attacks, the United States

effectively sealed off its borders. Cross-border traffic at land border checkpoints came to a standstill, planes ceased to arrive and depart, and the unloading of ships at seaports stopped while those not yet in port remained anchored at sea. While it is difficult to criticize this initial response given the confusion following the attacks, cross-border traffic at land border checkpoints, airports and seaports continued to move at a snail's pace for months as officials wrestled with ways to secure the border while facilitating legitimate trade and travel.

One of the initial strategies employed by the United States in an attempt to strike a balance between facilitating legitimate trade and travel while preventing terrorists from entering was to focus their attention on the citizens of countries they believed terrorist came from, putting those countries through increased scrutiny. Citizens of predominately Muslim nations were subject to special registration procedures when entering the United States and those same nations' citizens who were already within the United States with a status other than lawful permanent residency or US citizenship were required to register with the US Immigration and Naturalization Service. This strategy was flawed for at least two reasons. Firstly, the policy was seen as discriminatory against Muslims and it alienated the citizens of many countries whose assistance the United States needed in order to carry out its larger counter-terrorism strategy. Secondly, it ignored the citizens of North American and European states who may have a greater loyalty the global Salafi jihad movement. According to Leiken and Brooke's statistics, 41 percent of terrorists attempting to enter the United States to plan, coordinate and carry out attacks would not be subject to this increased scrutiny.

The special registration of individuals from predominately Muslim nations was not the only unilateral action taken by the United States to prevent terrorists from crossing borders. In the wake of September 11, the United States demanded that airlines provide detailed information about the reservations of passengers arriving at a US port of entry. This requirement, however, did not comply with the strict privacy laws of the European Union. The United States also imposed strict requirement on the travel documents that could be used to gain entry into the United States, including the incorporation of biometric technology. However, the United States' own passports did not meet these requirements and the US was not able to bring their passports up to these standards within the time frame imposed on other nations. While both these issues were eventually resolved, it was not without intense negotiations and concessions by both the United States and those nations opposed to these requirements.

International terrorism, and the Salafi jihad movement in particular, is a global problem that cannot be solved unilaterally. The United States quickly learned that trying to prevent terrorists' ability to travel across state borders was no exception. Globalization has given the terrorists unheralded ability to travel around the world to train, plan, coordinate and carry out attacks. Like many other threats resulting from globalization, preventing terrorists' ability to travel internationally requires a strategy of global governance. There are many approaches and institutions employed in governing this global problem, including: bilateral agreements, multilateral agreements, international regimes, regional and international organizations, global civil society groups such as transnational advocacy networks, and transnational governmental networks. As we will see in the next chapter, in the years following the September 11 attacks all these

approaches and institutions have attempted to curtail terrorists' ability to travel, or limit

their use of specific immigration vehicles such as alien smuggling organizations, with

varying degrees of success.

CHAPTER THREE: INTERNATIONAL BORDERS AFTER 9/11

In the wake of the September 11 attacks, people around the world questioned how nineteen men, armed only with box cutters, were able to launch a devastating assault against the world's last superpower on its own soil. While blame for the attacks can only lie with those nineteen men and the people who aided and supported them, the United States security strategy had many problems that hindered the attackers' detection and interception. It is quite obvious that the hijackers' ability to travel undetected around the world was an important part of the success of their operation. They knew the weakness in the system and were able to exploit those weaknesses.

In hopes of better understanding how the September 11 attacks occurred the United States Congress passed legislation that created The National Commission on Terrorist Attacks Upon the United States, more commonly known as the 9-11 Commission. The Commission was tasked with preparing a full and complete account of the circumstances surrounding the September 11, 2001, terrorist attacks, including preparedness for and immediate response to the attacks, and was also to provide recommendations designed to guard against future attacks (9-11 Commission 2004c). It quickly became apparent to the Commission that the terrorists' ability to successfully gain entry to the United States was a key element in their ability to carry out the attacks. The topic of terrorist travel was deemed so important that it was covered in much greater detail in the form of a staff monograph separate from the Commission's final report.

The Commission concluded that prior to September 11, 2001, and at the time of its final report border security still was not considered a cornerstone of national security policy, but that it must be made one (9-11 Commission 2004c). The Commission, in its final report, made recommendations in the areas of Homeland Security, Emergency Preparedness and Response; Reforming the Institutions of Government; and Foreign Policy, Public Diplomacy, and Nonproliferation. The topic of border security was covered in Homeland Security, Emergency Preparedness and Response. The Commission's recommendations for improving border security included the development of better strategies to combat terrorist travel; development of a comprehensive screening system; inclusion of a biometric entry-exit screening system; improved international collaboration on borders and document security; and issuance of standardized secure identifications that are acceptable for federal purposes (9-11Commission 2004b 383-390).

The 9-11 Commission recognized that strategies to stop terrorist from traveling the globe require information sharing between government agencies tasked with providing security for the nation's borders. The Commission also understood that the U.S. government couldn't meet its own obligations to the American people, the prevention of terrorists' entry, without a major effort to collaborate with other governments. It concluded, "we should do more to exchange terrorist information with trusted allies, and raise U.S. and global border security standards for travel and border crossing over the medium and long term through extensive international cooperation" (9-11 Commission 2004b: 390). The Salafi jihad movement is global and requires a strategy

of international governance to prevent its members from crossing borders to train, plan

and carry out attacks.

Global Strategy to Prevent Terrorist Travel: Beyond the 9-11 Commission Report

Following the end of the 9-11 Commission in August 2004, ten members of the

Commission created the 9/11 Public Discourse Project to educate the American people

about the recommendations of the 9-11 Commission and to issue its reports, with the goal

of driving needed reforms (Kean & Lee 2005). In December 2005, the Project issued its

final report on the government's progress in implementing the recommendations of the 9-11

Commission. In this final report, they gave the government a "D" grade in the area of

international collaboration on borders and document security. The project concluded,

"There has been some good collaboration between US-VISIT and INTERPOL, but little

progress elsewhere" (9-11 Public Discourse Project 2005). In a related issue, the Project

gave an "Incomplete" on the recommendation that the government develop a

comprehensive strategy to prevent terrorist travel. The reason for the incomplete grade

was that the first "Terrorist Travel Strategy" was not scheduled to be released until

December 17, 2005 (9-11 Public Discourse Project 2005).

On May 2, 2006, The National Counterterrorism Center released the unclassified

version of the *National Strategy to Combat Terrorist Travel* (NSCTT). Outlined in the

report is a strategy to fight terrorist travel globally by employing eight steps: Identify

known or suspected terrorists; ensure broad data sharing; screen travelers effectively

before reaching and at ports of entry; build partner capacity to limit and screen for

terrorist travel; detect and apprehend terrorists; dismantle infrastructures and networks

that facilitate terrorist travel; strengthen travel and document security; and collect,

analyze and disseminate all terrorist travel information (2). The report addresses two

main topics or "pillars," each supported by three strategic objectives. The first pillar is

"Enhance US and Foreign Partner Capabilities to Constrain Terrorist Mobility Overseas"

and the second pillar is "Deny Terrorists the Ability to Enter, Exit, and Travel within the

United States" (2-3).

The three strategic objectives under pillar one hope to combat terrorist mobility

outside the United States. These strategies are to: suppress terrorists' ability to cross

international borders; help partner nations build capacity to limit terrorist travel; and deny

terrorists access to resources that facilitate travel (9). The three strategic objectives under

pillar two hope to deny terrorists the ability to enter, exit, and travel within the United

States. This pillar's strategies are to: inhibit terrorists from crossing U.S. borders;

enhance the U.S. government's ability to detect and constrain terrorist travel within the

United States; and strengthen U.S. identity verification systems (25). Essentially, pillar

one outlines the United States' international efforts to combat terrorist travel; while pillar

two's primary concerns are domestic.

The NSCTT attempts to achieve its first strategic objective of suppressing

terrorists' ability to cross international borders by first collecting and analyzing

information on matters related to global terrorist mobility and then sharing this

information with foreign partners (9). The U.S. Government hopes to accomplish this by

enhancing border security capabilities of those countries at risk of terrorist activity by

providing participating countries with a computerized watchlist system to help constrain

terrorist mobility globally. The U.S. would work within the G8's Secure and Facilitated

International Travel Initiative (SAFITI), whose members are committed to: developing

mechanisms for real-time data exchange to validate travel documents, watchlist

information, and advance passenger information; providing effective and timely information exchange on the terrorist watchlist and lookout data of participating countries on a bilateral basis; providing input to the INTERPOL database that allows for real-time information sharing on lost and stolen international travel documents; and sharing best practices on effective cooperation between intelligence and law enforcement officials. The strategy calls for enhanced cooperation with foreign governments, beginning with the Visa Waiver Program countries, to establish appropriate access to the terrorist screening information of participating governments. The plans also include sharing newly developed technologies with international counterterrorism partners as appropriate (10-11).

The NSCTT attempts to achieve its second strategic objective of helping partner nations build the capacity to limit terrorist travel by working with foreign governments and with regional and international organizations to adopt and implement policies, strategies, and best practices to combat terrorist mobility globally, and to also identify capacity gaps while working with bilateral and multilateral assistance providers to ensure that such gaps are filled (13). For example, The Department of State's Antiterrorism Assistance Program provides foreign partners with training on the identification of fraudulent travel documents. The G8 established a Counterterrorism Action Group to provide and coordinate training and assistance for countries that have the desire but lack the ability to combat terror. Finally, U.S. and foreign law enforcement agencies can work together to focus resources on illicit travel facilitators abroad and to improve our understanding of the terrorist travel problem (14-15).

The hope of accomplishing pillar one's third strategic objective, denying terrorists access to resources that facilitate travel will, is that it will be more difficult for terrorists to forge travel documents, and that the government will be able to monitor and defeat terrorist travel facilitator networks and the financial networks that support them (17). The strategy calls for international standardized practices for passport issuance, and encourages their adoption and implementation by all governments (18). In addition, it calls for the U.S. to encourage other countries to identify and close down alien smuggling networks and document forgery cells, to criminalize alien smuggling and document forgery in countries where current laws are insufficient, and to target the financial networks that support their operations. (23)

In essence, the NSCTT is promoting a global governance approach to preventing terrorist travel, with the United States taking the lead. Perhaps the U.S. government, seeing the poor grade it received in international collaboration on borders and document security, realized they needed to do more. They are far from alone in understanding the importance of international collaboration in order to prevent terrorist travel. Great Britain learned first-hand from the 2004 attacks and plots on the London transportation system and the 2006 airline plot of the need for an international counterterrorism strategy to prevent terrorism. The U.K. Border Agency has concluded that they cannot achieve their goal of securing the border in isolation and will work in partnership not only with the rest of the U.K. government but also with their international partners, industry and the public (Home Office 2007: 26). However, when attacks are perpetrated by your own citizens who travel to their ethnic homeland for training, cooperation on border security often needs to be expanded beyond those countries with which traditional cooperation

agreements exist. In today's interconnected world any state can be a place or embarkation or transit point for a terrorist to plan, coordinate and carry out attacks. Combating terrorist travel requires a governance strategy on a truly global scale.

The liberal tradition in international relations emphasizes mutual interests as the motivating factor to encourage states to cooperate and the development of international institutions that facilitate such cooperation (Andreas & Nadelmann 2006: 8). The desire to prevent terrorists from entering a state's territory is no different than other mutual interest. What is needed, however, is a common approach to addressing the problem. While military action is needed to deal with conditions and states that provide terrorist safe havens, real progress in the "War on Terrorism" will not come in the form of a decisive victory on the battlefield. Rather, victory will require years of small steps forward such as arresting key individuals or nodes in the global Salafi jihad movement, disrupting terrorist plans, seizing their finances and curtailing their ability to cross borders (Rees 2006: 147). In Europe, law enforcement has been viewed as the main instrument to fight terrorists. Instead of engaging them on the battle field, European nations attempt to combat their terrorists though civilian means of law enforcement cooperation, prosecution of terrorists before criminal courts and sharing intelligence (Rees 2006: 73). If cooperation as a strategy to combat terrorist travel is to be successful, a mutual approach to combating the problem must be coordinated.

The September 11 attacks provided a catalyst for an unprecedented global antiterrorism campaign. However, much of the international law enforcement infrastructure utilized was already in place (Andreas & Nadelmann 2006: 189). Drugs, the illegal arms trade, and alien smuggling were already understood as transnational

crimes that required international law enforcement cooperation to combat. If terrorism is framed as a transnational crime on a massive scale, and a law enforcement approach is taken to combat it, these same institutions could then be adapted and utilized to combat international terrorism. With the globalization of transnational crime and international law enforcement, borders remain the focus of most concern and activities (Andreas & Nadelmann 2006: 108). International terrorism is no different, though when it comes to intelligence sharing and law enforcement cooperation bilateral communication, rather than multilateralism, has been the primary means of international cooperation (Rees 2006: 90). When the border is the main focus of activity and concern, it is likely that bilateral law enforcement cooperation will begin with one's neighbors.

Global Strategy to Prevent Terrorist Travel: Bilateral Agreements and Action

The United States – Canadian border has long been touted as the world's longest demilitarized border and is a great sense of pride for both countries. The lack of military presence is not the only unique feature of this border; the two countries have had a long history of openness and lax regulation economically and with the movement of goods and people. Since the September 11 attacks, the attitude towards the border has changed greatly, especially among the American public. The issue of deeper economic interdependency has become subordinate to the immediate demands of national security (Hufbauer and Schotts 2004: 2). In the immediate aftermath of the September 11 attacks, U.S. authorities immediately imposed stringent security measures at both the northern and southern borders. Security concerns after September 11 continued to rise and significant border delays continued. The initial hardening of the border in the immediate aftermath of the terrorist attacks seemed like a reasonable response at the time. The

continental United States had never faced an attack of that magnitude in its entire history, and in the confusion that followed; it was the proper short-term solution. This was not, however, viable long-term. Finding a long-term solution would require continued cooperation between both states, building upon bilateral law enforcement cooperation and institutions already in place to combat other types of cross-border crime.

Although September 11 was a defining moment in U.S.-Canadian border relations, cooperation in cross-border issues has a long history. It is in the law enforcement field where this cooperation was must visible as it relates to border security. Three examples of this pre-9/11 cooperation are Project North Star, Cross Border Crime Forum (CBCF) and the Integrated Border Enforcement Teams (IBET). Project North Star was created in 1989 as a voluntary means of coordinating U.S. and Canadian law enforcement efforts, with a primary emphasis on counter-drug activity along the border. The CBCF was created in 1997 as a bilateral consultative mechanism made up of 150 senior law enforcement, intelligence and justice officials from both countries in order to work to better address various cross border crime issues. The IBET is a multi-agency law enforcement team made up of officers from both sides of the border which work together to coordinate both countries' efforts to target cross border criminal activity (Noble 2004:10-11).

In the aftermath of the border chaos that followed the September 11 attacks, it was clear a new approach to dealing with the U.S.-Canadian border was needed. As a result, the U.S. Canada Smart Borders Declaration and 30 Point Action Plan was announced in December 2001. The goal of this declaration and action plan was to "Enhance the security of our shared border while facilitating the legitimate flow of

people and goods" (White House 2002). The action plan had four pillars: the secure flow of people, the secure flow of goods, secure infrastructure, and information sharing and coordination in the enforcement of these objectives. What made this declaration so important were the thirty points that provided a road map for bilateral cooperation on border security.

Many of the thirty points described is the declaration and action plan were already in place. However, they needed to be adapted or expanded to deal with the threat presented by international terrorism. Other points, while discussed in the past, required a level of harmonization that was once thought highly unlikely or impossible. Two of the points once thought unlikely to be adopted are closely linked: the use of biometric identifiers in border inspections and a single alternative inspection system. What is meant by an alternative inspection system is a process of inspecting individuals seeking entry into a state beyond the normal processes of passport and visas, which was described in great detail in the previous chapter. Usually these alternative inspections system are put in place to facilitate the entry of frequent border crossers thought to be a low security risk. The US-Canadian NEXUS program is one such example. NEXUS is an alternative inspection program that allows pre-screened, low-risk travelers to be processed originally at land border ports of entry with little or no delay by United States and Canadian border officials. Individuals who participate in the program are issued a photo-identification/proximity card. Program members are allowed to cross the border in a dedicated lane where they present their NEXUS card for entry into the country (CBP 2005a). Following its initial success at land borders, the program was expanded to citizens of the U.S. and Canada who arrive at ports of entry by air. Participants in the

program have an image of their iris captured at the time of enrollment. Participants can then enter the United States and Canada by utilizing automated kiosks, where they present their membership card, submit their iris for biometric verification, and make a declaration. Upon successful completion of the above, they are then directed to the exit, unless chosen for a selective or random secondary referral (CBP 2005b).

What NEXUS tries to accomplish is the facilitation of the entry of low risk individuals so that greater scrutiny can be given to those individuals who are thought to be a higher risk to security. The backbone of international cooperation on border security is information and intelligence sharing. The United States and Canada understand this connection and haven taken steps in the form of a bilateral information sharing agreement in order to better provide for each other's security, formalized with the Statement of Mutual Understanding (SMU).

The SMU (also part of the 30 Points Action Plan) replaces the information-sharing arrangements that had been in effect since 1999 and similarly provides for the exchange of information on a case-by-case basis in accordance with the domestic laws of both Canada and the United States. It allows for the proactive sharing of information that is pertinent to the enforcement of each country's citizenship and immigration laws (CIC 2003). The original statement was an agreement between Citizenship and Immigration Canada, U.S. INS and the U.S. Departments of State, but was expanded to the current agencies involved in border and immigration management after reorganization of these agencies occurred in both countries. Both countries view the SMU as an important tool for securing their borders. The agreement outlines condition and procedures for the exchange of information, the type of information that can be exchanged, which includes a

wide variety of biographical information as well as past immigration and criminal histories, and how the information may be used (CIS 2003).

Entering into bilateral agreements with one's neighbors as a means of governance to prevent terrorists from traveling into your state is important. Today's globalized world, with its interconnected air transportation system, requires cooperation not only with states next door but with states across the globe. Often a state will agree to cooperate or enter into a formal agreement with another state in return for some sort of preferential treatment. A bilateral agreement between the United States and the Republic of Estonia is one such example.

As stated in the previous chapter, in 2008, eight countries were added to the United States' Visa Waiver Program, including the Republic of Estonia. Earlier that year, the governments of the United States and Estonia signed a Memorandum of Understanding, stating that Estonia's membership in the Visa Waiver Program required a formal arrangement between the countries for the sharing of information on certain criminal activities (DHS 2008). The requirement was met when the two countries signed the agreement on Enhanced Cooperation in the Preventing and Combating Serious Crimes. The agreement "prompted by the desire to cooperate as partners to prevent and combat serious crimes including terrorism more effectively," recognized that information sharing is an essential component in the fight against serious crime including terrorism (USA & Estonia 2008). The agreement included the sharing of personal data, fingerprint data, DNA data, and providing points of contact for the implementation of the agreement. In addition, the agreement also took steps towards providing for privacy and data protection, and for transparency (USA & Estonia 2008).

Estonia was not alone in entering into a bilateral information sharing agreement as a requirement for membership in the Visa Waiver Program. The other seven new members entered into similar agreements with the United States as a term of admission into the program. In fact, when the United States Congress passed legislation in 2007 allowing for expansion of the Visa Waiver Program to include these additional 8 countries, it required that these countries cooperate with the United States, specifically in regards to sharing information in security and law enforcement matters (DHS 2008). As a result, the United States now has bilateral information sharing agreements with all eight new Visa Waiver Program member states. When bilateral agreements such as these are expanded to include other nations, the foundation is laid for multilateral agreements for the mutual benefit of all parties.

Global Strategy to Prevent Terrorist Travel: Multilateral Agreements and Action

Following the September 11 attacks, it quickly became evident that the goal of facilitating legitimate trade and travel while simultaneously providing for secure borders and international travel required international cooperation in sensitive areas of state sovereignty, much of which would have been unthinkable before the attacks. The European Union and the United States have been at the forefront of these international efforts and have entered into various agreements centered on the issues of border controls, government surveillance, data collection and exchanges, and travel document security (Koslowski 2008: 33-34). Some agreements aimed at providing for greater border and travel security, however, were created between members of the European Union, outside the legal framework of the Union. The Treaty of Prüm is one such agreement.

Despite the recognition by states that an effective counterterrorism and border security strategy requires global cooperation, the power to tackle terrorism and provide for increased border security remains primarily in the hands of national governments. Even within the European Union, cross border cooperation in security matters usually occurs bilaterally. Despite numerous agreements between EU members designed to promote intelligence sharing and cooperation, national police forces continued to not share information and mechanisms were put in place to compel them to do so (Keohane 2005). As the security threat of terrorist travel and other cross border crimes was realized, government officials from Germany, France, Belgium and Luxembourg recognized that the rules to combat serious cross border crime and terrorism under Schengen and the Third Pillar of the EU treaty were not sufficient and there remained a need for closer police cooperation among these neighbors (Luif 2007: 6). After several rounds of negotiation and the inclusion of the Netherlands, Austria and Spain, the Treaty of Prüm was signed on May 27, 2005.

The Treaty, officially known as "the Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration," sought the "further development of European cooperation, to play a pioneering role in establishing the highest possible standard of cooperation, especially by means of improved exchange of information, particularly in combating terrorism, cross-border crime and illegal migration, while leaving participation in such cooperation open to all other Member States of the

European Union" (The Council of the EU 2005: 3). The treaty hoped to obtain these

goals by putting in place agreements and mechanisms for the signatory states to better

coordinate their activities and efforts. These agreements and mechanisms include sharing

DNA files and fingerprint data, establishing "national points of contact" to coordinate the

information sharing, sharing the personal data of individuals where there is reason to

believe the subject will commit a terrorist act, sending "document advisers" to states

regarded as source or transit countries for illegal migration, and providing for joint police

operations where officers participate in operations outside their own country (Luif 2007:

8-10).

The fact that only seven nations were signatory partners was important to the

treaty's quick development and implementation. Since the treaty involved only seven EU

members, it did not trigger the closer cooperation provisions of the Treaty on the

European Union, which only applies when eight or more member states are involved. As

a result, all EU institutions were outside the mechanisms of the treaty, which allowed the

treaty's parties to avoid the cumbersome process that accompanies agreements that are

within the framework and institutions of the Union (Guild 2007:1). The text of the treat

provides that "The provisions of this Convention shall apply only in so far as they are

compatible with European Union law" (The Council of the EU 2005: 33). The treaty also

provides for expansion by being "open for accession by any Member State of the

European Union" (The Council of the EU 2005: 35).

Even before the treat came into effect, other EU member states announced their

intentions to accede to the treat. Within two years of the signing of the Treaty, ten

additional Union members expressed their interest in joining (Luif 2007: 8-10). In 2007,

the Treaty was submitted to the European Council for integration into the Third Pillar of the European Union (Guild 2007:1). The following year the European Parliament voted to accept the Treaty of Prüm after requiring the increased protections for ordinary citizens within the treaty (Ballard 2008). The treaty has also served as a model for other cooperation agreements that combat terrorism and provide for increased border security. In March 2008, the United States and Germany entered into an agreement on the Enhanced Cooperation in the Preventing and Combating Serious Crimes, following the Prüm model. In the months after this agreement, other European Union states entered into similar agreements with the United States (Bellanova 2009: 3-4). The United States began to make such agreements a prerequisite for receiving a benefit such as entry into the Visa Waiver Program, as was the case regarding the joint cooperation agreement between the United States and Estonia discussed earlier. As a result, the Treaty of Prüm has had a profound effect on international cooperation on border security and counterterrorism effects well beyond its impact on the original seven members of the treaty. It has the potential to evolve into a regime that will help prevent terrorist travel, if not on a global level, then at least on a transatlantic level.

Global Strategy to Prevent Terrorist Travel: International Regimes

Regimes can best be defined as "sets of implicit or explicit principles, norms, rules and decision-making procedures around which actors expectations converge in a given area of international" (Krasner as cited in Koslowski 2008: 2). For a regime to exist there needs to be a set of issues that require collective action. Members must act together consistently by rules and agreements they've drawn up together. They must act within the constraints of the regime and there needs to be a mechanism to resolve

conflicts between members should disputes arise (Rees 2006: 11). Regimes are social

structures that have limited power to impose rules. Rather, members become tied to

formalized patterns of behavior in which they feel obligated to cooperate so as not to be

viewed as untrustworthy (Rees 2006: 13). As a result of the social structure of regimes,

they tend to develop between states with shared norms and values and between whom a

tradition of cooperation already exists, especially when that cooperation is centralized

around a particular issue.

The transatlantic relationship between the United States, Canada and Western

Europe has had a long tradition of cooperation centered on security issues, and even

before the final shots of World War II, North America and Western Europe shared a

common antipathy for the Soviet Union, leading to the development of strong bonds of

cooperation. Military cooperation on transatlantic security issues became institutionalized

through NATO. However, these nations' common values and their collective identity as

liberal democracies led to the expectation of further cooperation beyond the realm of

military action (Rees 2006: 19-20). At the end of the Cold War, this cooperation shifted

from dealing with the military threat posed by the Soviet Union to the "new security

agenda" of combating international organized crime, drug trafficking and illegal

immigration (Rees 2006: 21). The terrorist attacks in New York, Washington, Madrid

and London highlighted yet another threat to transatlantic security: the dangers of

international terrorism. The fear once rooted in the threats posed by the Warsaw Pact has

been replaced not by a state or group of states but the global Salafi jihad movement,

which views these transatlantic partners as the enemy.

Long-established military security cooperation provided the infrastructure for the development of transatlantic security cooperation that would deal with the new security threats. However, combating terrorism requires cooperation across many fields of activity (Rees 2006: 22). International cooperation on the security threat presented by international terrorism is in its infancy and most cooperation remains bilateral in nature. An international or transatlantic regime to combat terrorism, let alone combating terrorist travel, is far from a reality. This is not to say that the groundwork for further cooperation has not been laid. International cooperation that focuses on better managing global mobility, in combination with the data sharing processes outlined in the Treaty of Prüm, may be the impetus for a transatlantic regime designed to prevent terrorists and other clandestine transnational actors from crossing international borders.

In the past, regimes related to managing cross-border flows of persons have existed almost exclusively to handle the flow of international refugees. On a global level there has been very little cooperation regarding international migration, referring to individuals who have lived outside their country of nationality or birth for more than one year (Koslowski 2008: 2-3). Looking at the movement of people across borders from the much larger perspective of "global mobility" may allow for greater international cooperation and the foundation of transatlantic regimes that will prevent terrorists and other clandestine transnational actors from crossing international borders. "Global mobility" refers to the movement of all people across international borders regardless of the length of stay or purpose of travel (Koslowski 2008: 5-6). As described in great detail in the previous chapter, terrorists have utilized almost every possible method to cross international borders. Therefore, the effective management of a global mobility

regime is necessary to any transatlantic strategy to prevent terrorists from crossing borders to carry out an attack.

In the years since the September 11 attacks, there has been considerable progress towards an international approach to global mobility management. The most significant progress has been made in the areas of biometric entry-exit systems, electronic passports, passenger data sharing agreements and electronic travel authorization systems. However, this cooperation has been limited primarily to member states of the Organization for Economic Cooperation and Development (Koslowski 2008: 40). It is cooperation in the areas of biometric information sharing and the standardization of collection methods that offer the best hopes for a transatlantic regime that will manage global mobility in order to combat terrorist travel and border crossings by other clandestine transnational actors.

The United States began collecting biographical data from individuals who apply for a visa or seek admission at a port of entry in 2004 as part of its US-VISIT program. While biometrics were initially only collected from nonimmigrant visa holders, the program was expanded to include individuals seeking admission under the Visa Waiver Program. The Australia government planned full implementation of its biometrics Borders Program by June 2009 (DIAC 2007: 21). In 2007, Japan began requiring all foreign nationals above the age of 16 to allow the collection of their facial and fingerprint biometrics upon entry, and the European Commission plans for the deployment of an automated biometric entry-exit system by all Schengen member states by 2015 (Koslowski 2008: 40). Currently, there are a variety of biometric identifiers that are being employed by various nations for border management. Fingerprints, however, appear to be the most suitable form for use in a global mobility management regime.

Fingerprints have long been employed by law enforcement agencies throughout the world to provide the identification of individuals beyond basic biographical data such as name and date of birth. As fingerprints have been associated with criminal activity, the collection of fingerprints in border management has received a great deal of criticism and is viewed by some as intrusive. Fingerprints, however, provide distinct advantages over other forms of biometric identifiers. They have been collected for so long and by such a large number of agencies that the sheer size of data for comparison is enormous. More importantly, fingerprints are comprised of friction skin, the type of skin found exclusively on the inner portion of the hands and the bottom of feet. Their composition allows for fingerprint classification and identification, and allows for samples to be collected passively. When a location where terrorists have been know to congregate, such as a safe house, is identified, samples of the friction skin left behind can be collected and entered into biometric storage systems for further use. This provides two benefits. First, these fingerprints can be checked against the existing databases for possible identification, and second, they can be entered into the border screening system as a lookout. This will allow border security officials to be alerted if a person encountered at the border has fingerprints that match the collected sample. The sharing of fingerprint databases between agencies and countries provides a net-widening effect, leading to the higher probability that an individual who may pose a security risk is identified.

The Treat of Prüm formalized how various Europeans states share biometric data. The United States, using the treaty as a foundation, has entered into similar agreements with some of its international partners. The treaty and subsequent agreements have already provided a mechanism for sharing biographical data. When biographical data are

submitted for comparison, the sender will receive a "hit/no hit message." If a hit is

received, the sender will receive a hit identification number to reference when contacting

the national point of contact of the country in whose records the hit was found. The

contact will then provide the information to the inquiring agency according to the

guidelines of the agreement (Luif 2007: 9). This process for comparing biometric data

closely resembles the United States' National Crime Information Center's (NCIC)

process for verifying and submitting fingerprints. The center, managed by the Federal

Bureau of Investigations, has provided information regarding criminals, wanted persons

and fingerprint records to various jurisdictions throughout the United States since 1967.

NCIC may serve as a model for a data sharing mechanism for an international regime that

will combat travel by terrorist and other clandestine transnational actors.

While cooperation in the areas of biometric entry-exit systems, electronic

passports, passenger data sharing agreements, and electronic travel authorization systems

may have laid the foundation for a global mobility regime that could be used to combat

terrorist travel, these agreements did not occur without a great deal of negotiation. When

disputes did arise, the parties that took part in the negotiations often turned to

international organizations with particular expertise in the given area to resolve the

dispute. When biometric standards for new passports were being negotiated, the United

States allowed the International Civil Aviation Organization (ICAO) to set these

standards (Koslowski 2008: 35). Likewise, when the transfer of information contained in

airlines' passenger name record (PNR) data became a contentious issue due to privacy

concerns, the ICAO again intervened, developing a set of "recommended practices" for

the transfer of PNR data (Koslowski 2008: 39). Unfortunately, aside from intervening

when disputes arise during bilateral and multilateral negotiations, international organizations have contributed little to efforts aimed at combating terrorist travel.

Global Strategy to Prevent Terrorist Travel: International Organizations

While various international organizations have made small contributions to international efforts to combat terrorist travel, no one organization has stepped up to take the lead in confronting the problem. The reason for this is twofold. First, combating terrorist travel is not the primary mission or mandate of any existing organization, and second, there is a level of distrust among member states of many existing organizations that makes finding a consensus on sensitive issues such as terrorism difficult. One example of this is the International Civil Aviation Organization. As stated above, the ICAO set biometric standards for new passports and also developed recommended practices for PNR data. However, the ICAO's main objective is to "achieve its vision of safe, secure and sustainable development of civil aviation through cooperation amongst its member States" (ICAO 2009). While terrorism is clearly a threat to the ICAO's ability to achieve this objective, combating terrorism travel is not explicitly part of its mandate. Instead, the organization can only create agreed-upon standards among it member states to help facilitate international air travel, which may have the added benefit of making it more difficulty for terrorist to cross borders.

Two organizations that at first glance appear to be best-suited to provide an institutional mechanism for combating terrorist travel, given their roles in managing migration, would be the United Nations and the International Organization for Migration (IOM). Both the UN and IOM have played an active role in trying to combat and curtail human smuggling and human trafficking. The UN and its predecessor, the League of

Nations, have targeted human trafficking since the early 20th century, and since the 1990s

they have created and enacted numerous anti-smuggling and anti-trafficking committees

and conventions (see Koslowski 2004b: 11-12). The same cannot be said for combating

and curtailing terrorist travel, an issue both the United States and Europe have found it

difficult to achieve progress in. The General Assembly itself has proven to be a particular

obstacle for the UN becoming a more relevant actor. One reason for this lack of

cooperation is the multiplicity of perspectives held by the assembly's member,

particularly from states that support terrorist groups or have sympathy for groups that

employ terrorist tactics (Rees 2006: 131).

   The IOM has also emerged as a major actor in the area of combating human

smuggling and trafficking. In particular, the organization has become a leader in the area

of research and policy dialogues devoted to human smuggling with the primary focus of

preventing the trafficking of women and children for forced prostitution (Koslowski

2008: 30). Despite its success in the areas of human smuggling and trafficking, the

primary mandate of the IOM is "promoting humane and orderly migration for the benefit

of all. It does so by providing services and advice to governments and migrants" (IOM

2009). As such, the IOM is primarily an international social service organization that is

poorly suited as a vehicle that will prevent terrorist travel. Unfortunately, international

law enforcement organizations have also proven to be unsuited to combat terrorist travel.

   The International Police Organization (INTERPOL) has tried to take an active

role combating terrorist travel. In 2002 INTERPOL, beginning with a few thousand

entries from a handful of countries, created its Stolen and Lost Travel Documents

(SLTD) database. INTERPOL's SLTD database enables law enforcement anywhere in

the world to instantly run a check against the database, allowing border control officers to verify if a document is reported stolen or lost nationally and internationally. As of 2007, the database contains information on more than 14 million stolen and lost travel documents from 123 countries, including nearly seven million passports. Searches conducted within this database have resulted in the detection of more than 5,000 people attempting to enter countries with travel documents that have been reported lost or stolen (INTERPOL 2007).

Despite the successes of the SLTD database, INTERPOL has had little success elsewhere in combating terrorist travel. INTERPOL's efforts have been stymied in much the same way as the United Nation's efforts to combat terrorism have failed to materialize. As with the United Nations, for a variety of reasons a true spirit of cooperation and joint action does not exist within the organization. INTERPOL's 187 members do not necessarily trust each other. Many members assume, and in some cases rightfully so, that the criminal networks they are fighting have penetrated the law enforcement agencies of other member states. In addition, there exists a feeling that allies of today may become the enemies of tomorrow. But it is not only a lack of trust that has impeded INTERPOL. Some member states may face domestic legal impediments to sharing information with international partners, or member states' law enforcement and intelligence agencies many have a culture of holding onto specific valuable information, making effective collaboration almost impossible (Naim 2003: 36) Given this situation, it appears that finding a global consensus on how to combat terrorist travel is unlikely. Regional organizations, where members share a common political and social culture,

would appear to be more likely candidates for effective cooperation to combat terrorism. Unfortunately, this is not necessary the case.

The European Police Office, EUROPOL, was established to provide a central European Union mechanism for greater cross-border cooperation and communications among member states' police agencies. EUROPOL, in addition to fostering greater cross-border cooperation and communications, established the Europol Computer System, a vast database of criminal suspects and stolen goods. The system has been linked to the Schengen Information System for use in border enforcement (Andreas and Nadelmann 2006: 186-7). Beyond this system, however, EUROPOL has been plagued by many of the issues that have led to INTERPOL's ineffectiveness in combating terrorism, mainly mistrust and professional competitiveness. As a result, member states' national police forces continued to not share information and there is no mechanism in place to compel them to do so (Keohane 2005).

The European Union has also moved to create an organizational mechanism for greater police cooperation in the specific area of border security. In 2004, the EU established FRONTEX, which became fully operational in October 2005. It was created for the purpose of "Coordination of intelligence driven operational cooperation at EU level to strengthen security at external borders." Its organizational goal is to "strengthen the freedom and the security of the citizens of the EU by complementing the national border management systems of the Member States" (FRONTEX 2009). FRONTEX, with its limited focus on border security, appears to show promise as a global governance organization capable of forming the foundation for an effective strategy to combat terrorist travel. To be successful, however, it will have to encourage greater cooperation

not just within Europe but also with Europe's transatlantic security partners. On the other hand, FRONTEX is a relatively new organization, so it is unclear at this point whether it will suffer from the same impediments as both INTERPOL and EUROPOL. FRONTEX, like these two other agencies, provides for institutionalized cooperation, and so it will likely suffer the same bureaucratic symptoms of lack of trust and competition that may hamper its ability to effectively combat terrorist travel. To counterbalance these possible impediments, FRONTEX will need to work in concert with governance mechanisms built on an environment of trust, common identity and cooperation found within transnational networks.

Global Strategy to Prevent Terrorist Travel: Transnational Networks

As discussed in great detail in chapter 2, Transnational Advocacy Networks (TANs) stress fluid and open relationships among committed and knowledgeable actors in specialized areas. These networks are constructed of "nodes" of individuals or groups that utilize modern technology to connect with other "nodes" around the globe, informally sharing ideals or beliefs. Through their collective action, the nodes of the network can turn their attention to global-scale problems and issues they feel should be addressed. TANs have been used in the past as a tool of global governance in matters related to border security. They have fostered cooperation between activist and other non-state actors while interacting with states to address human smuggling and trafficking (Bertone 2008: 4). These networks have played a particularly important role in framing problems related to human trafficking and have helped in the development, acceptance and implementation of anti-trafficking norms (Bertone 2008: 6).

Despite TANs' contributions to the governance of border security issues such as human trafficking and smuggling, there is little they could do to effectively combat terrorist travel. The strategies employed by TANs to combat human trafficking are known as the "3Ps" – prevention, protection and prosecution – and the "4Rs" – rescue, rehabilitation, repatriation and reintegration (Bertone 2008: 10). The motivation of terrorists seeking to cross borders and those who facilitate their travel is much different than those who traffic or those trafficked, whose motivation is financial or the hope for a better life. Members of the global Salafi jihad movement are motivated by their ideology, and therefore the 3Ps and 4Rs would not serve as an appropriate model. TANs also lack hard power of states, such as military, law enforcement or prosecution powers, to combat terrorist travel. Where TANs' contribution to the global effort to combat terrorist travel is most effective is in providing a model for inter-state cooperation that is based on fluid and open relationships among committed and knowledgeable actors in specialized areas and operating through global networks.

When government agencies are faced with problems that are international in nature, they may adopt a strategy of assigning officers to foreign jurisdictions to work directly with the domestic agencies within that jurisdiction to address the problem jointly. It is these officers, and their domestic contacts that comprise the membership of some transgovernmental networks. These networks, as covered in detail earlier, communicate and interact among themselves in order to share information, collect and disseminate best practices, and provide technical assistance and training to those officials who have less experience in specific areas than their network colleagues. They are built on the foundation of mutual trust, which often strengthens over time. As network actors

negotiate a common understanding of the problem, a shared identity begins to develop among network members. When the problem faced is the need to combat terrorist travel, the membership of the network is comprised of officers from national agencies that are tasked with regulating migration and providing border security.

Even before the September 11 attacks, the immigration and border security agencies of Canada, Australia, the United Kingdom and the Netherlands have been deploying officers as airline liaison officers (ALOs) or immigration control officers (ICOs) to work with their foreign counterparts as part of a border management strategy. ALOs are border officials posted abroad to work with and train airline staff in preventing the travel of persons with fraudulent documents. ALOs help a nation's border agency by stopping an illegitimate traveler before he or she arrives at a port of entry. This not only helps the destination country prevent an illegitimate traveler from arriving at its border, it also helps airlines save money. ICOs are similar to ALOs except that they work more closely with the government officials of a host country, rather than with private stakeholders such as airlines. ICOs are usually posted close to the center of criminal activity in source countries in order to work with the local law enforcement and international agencies (IOM 2003: 7).

Canada has pioneered the practice of stationing immigration control officers abroad. There are approximately 50 such officers in foreign airports and still more stationed at consulates overseas. These officers assist in the detection of persons heading for Canada with false documents or contraband. The program has been extremely successful and has allowed Canada to implement a strategy of extending its security

perimeter. This has given Canada the ability to anticipate and thwart the plans of dangerous travelers before they reach North America (Rekai 2002: 20-21).

In December 2004, Canada's immigration and customs services were merged to form the Canada Border Services Agency. The agency is responsible for "for providing integrated border services that support national security and public safety priorities; and facilitate the free flow of persons and goods, including animals and plants" (CBSA 2009a). The cornerstone of the CBSA's overseas operations are the agency's Migration Integrity Officers. These officers, who are part of the CBSA's larger Immigration Intelligence Network, work overseas with international partners, local immigration and law enforcement agencies, and airlines to combat irregular migration, including people smuggling and trafficking. They also support document integrity and anti-fraud activities by detecting and intercepting fraudulent travel documents or fraudulently obtained travel documents (CBSA 2004). It is through the Migration Integrity Officers' continued interaction with foreign immigration and law enforcement officials that an environment of mutual trust and identity is established and the foundation for a transgovernmental network is laid.

Great Britain has adopted a similar strategy for border protection. In April 2008, Great Britain brought together staff from Customs, the Border and Immigration Agency and U.K. Visas Services to create the U.K. Border Agency. The agency was formed to "improve the United Kingdom's security through stronger border protection while welcoming legitimate travelers and trade" (Home Office 2009a). The new agency now has uniformed officers with police powers to need to deal with immigration and customs crime. It is the agency's hope that these new officers will be the foundation of a "A

strong new force at the border" that will protect the United Kingdom with a triple ring of checks including offshore controls such as pre-arrival screening, a stronger U.K. border, and tougher checks in the United Kingdom (Home Office 2009b).

A key component of the U.K. Border Agency's attempts to implement offshore controls and pre-arrival screening is the agency's Risk and Liaison Overseas Network (RALON). RALON is comprised of Immigration Liaison Managers (ILM), a new position that encompasses officers previously known as Airline Liaison Officers at airports overseas and Risk Assessment Officers that were assigned overseas to visa service centers. ILMs provide training to airline staff and local authorities in United Kingdom passport and visa requirements, and forgery awareness. They also give on-the-spot advice to the check-in staff of flights departing for the United Kingdom on which documents presented by passengers may make those passengers ineligible for entry upon arrival. In addition, ILMs work to develop and maintain effective working relationships with airlines, local airport authorities and other countries' liaison officers (Home Office 2008). Through the deployment of ILMs overseas, the U.K. Border Agency has been able to develop a global border security intelligence network made up of its own officers, private sector stakeholders, local law enforcement authorities and other countries' liaison officers.

The U.S. and the Use of Transnational Networks to Prevent Terrorist Travel

The United States differs from Canada and Great Britain in that it has two separate agencies responsible for border security, both within the Department of Homeland Security. Prior to the creation of the Department of Homeland Security in 2003, the Immigration and Naturalization Service's (INS) Inspections Branch screened

individuals attempting to enter the United States at ports of entry while the U.S Border

Patrol, also part of INS, was responsible for apprehending individuals attempting to enter

the United States between ports of entry. The agency also had an investigative branch, a

branch responsible for detaining and deporting violators of immigration law, and a

branch responsible for adjudicating applications for immigration benefits. The United

States Customs Service's (USCS) Inspection Branch was primarily responsible for

screening individuals and cargo suspected of carrying prohibitive items into and out of

the United States. USCS also had an investigative branch as well as an intelligence

branch.

Following the September 11 attacks, the new security threat presented to the

United States by international terrorism was recognized and on March 1, 2003, the

Department Homeland Security was formed. Within the Department, the inspections

branches of INS and USCS were merged, and along with the U.S. Border Patrol, formed

the U.S. Customs and Border Protection (CBP). The investigative branches of the two

agencies were combined and along with INS's Detention and Deportation Branch and

USCS's intelligence branch they formed the newly minted U.S. Immigration and

Customs Enforcement (ICE). The remaining component of the INS responsible for

adjudicating applications for immigration benefits was renamed U.S. Citizenship and

Immigration Service and remained separate from the two new agencies.

The primary mission of the U.S. Customs and Border Protection is to prevent the

entry of terrorists, human and drug smuggling, illegal migration, and agricultural pests

both at and between the official ports of entry, while simultaneously facilitating the flow

of legitimate travel and trade (CBP 2008a). CBP does have an international component,

assigning its officers overseas. However, this has primarily been a part of the Container Security Initiative (CSI). Officers assigned to CSI work jointly with a host nation's counterparts to identify and screen containers that pose a risk at the foreign port of departure before they are loaded on vessels bound for the U.S. As of 2008, officers assigned to CSI work at a total of 58 ports worldwide (CBP 2008b). This is not to say that there are no CBP programs overseas dedicated to preventing the entry of terrorists into the United States. In February 2004, the Commissioner of CBP announced the Immigration Security Initiative (ISI), which is modeled after the Canadian Immigration Controls Officers as well as similar programs in Australia, the United Kingdom and the Netherlands (Koslowski 2004b: 7). While the number of officers overseas as part of the ISI program, which is now called the Immigration Advisory Program (IAP), pales in comparison to the officers assigned to similar programs by Canada, Australia, the United Kingdom and the Netherlands, officers assigned to IAP are only in Amsterdam, the Netherlands, Warsaw, Poland, London, the United Kingdom, Frankfurt and Tokyo. With that said, expansion to additional locations is currently pending (CBP 2007)

The U.S. Immigration and Customs Enforcement's primary mission is to protect United States national security by enforcing our nation's customs and immigration laws. It is comprised of four main operational components: the Offices of Investigations and Intelligence, which are the investigative and intelligence arms of DHS, charged with preventing terrorist and criminal activity by targeting the people, money, and materials that support terrorist and criminal organizations; the Office of Detention and Removal, which is primarily an enforcement arm within ICE for the identification, apprehension and removal of illegal aliens from the United States; and the Office of International

Affairs, which is the overseas investigative arm of ICE (ICE 2009a). As the primary overseas investigative arm or ICE, the Office of International Affairs is responsible for coordinating and supporting all foreign investigative activities of ICE. It also assists partner countries in the development and implementation of legislation and regulations, provides training to foreign officials, acquires and develops intelligence related to cross-border criminal activity, and provides operational support to ICE attachés at foreign embassies and consulates worldwide. (ICE 2009b)

Attaché Offices around the world are the backbone of ICE's overseas operations. An ICE attaché's responsibilities include conducting and coordinating ICE investigations and supporting the Department of Homeland Security's missions overseas. They initiate, oversee and are the primary points of contact for several DHS components including ICE's Office of Investigation, Office of Intelligence and Detention and Removal Operations, as well as agencies outside ICE such as Customs and Border Protection and the Federal Air Marshals Service. In order to support these various components, ICE attachés are responsible for the coordination of international investigations with foreign counterparts. They provide investigative case support to domestic and international ICE offices as part of the effort to combat transnational crime, as well as acquiring and developing intelligence related to cross-border criminal activity and fostering lawful international trade and travel through liaison with a host country's government and industry. ICE attachés cultivate and maintain close contact with law enforcement, intelligence, regulatory and trade representatives and organizations throughout their geographic area of responsibility (ICE 2009c).

ICE attachés are the United States' largest overseas network of law enforcement and intelligence officers directly responsible for the nation's border security. The officers assigned to ICE attaché offices overseas are not just responsible for their own agency, but are also the primary overseas contact for U.S. Customs and Border Protection, the agency tasked with preventing the entry of terrorists, human and drug smuggling and illegal migration both at and between the official ports of entry. Given this role an ICE attaché may be the best candidate for confronting "networks of terror with networks against terror" as a means of combating terrorist travel and travel by other clandestine transnational actors.

Chapter 2 discussed in great detail how both the global Salafi Jihad movement networks and transnational advocacy networks are comprised of informal relationships that stretch across nation borders, with a stress on fluid and open relationships among committed actors. These relationships are built on trust and a common identity that supersedes national identity, and which, with the assistance of modern technology, allows them to carry out their activities with great speed and efficiency. Both these network types have a leadership that is hierarchical in structure as well as a horizontal network made up of nodes of individuals responsible for the day-to-day activity of the network. Transnational government networks too increasingly exchange information and coordinate activities across borders and between governments in an effort to combat global crime. Like the global Salafi Jihad movement networks and transnational advocacy networks, a key element to the success of transgovernmental networks is that their membership shares common values and experiences, including a common history

and culture, as well as political and economic ideologies. On initial investigation ICE's attaché offices around the globe appear to be such a network.

Chapter 2 examined the importance of terrorists' ability to cross international borders to plan, train, and carry out attacks, and various environments and situations that have allowed terrorist to cross these borders undetected. Through the historical examination of how terrorists have successfully crossed borders in the past and by exploring current treads, the chapter hoped to illustrate the nature of the threat. This chapter, meanwhile, examines how various governments have worked with their international partners to combat the problem. The remainder of this paper will investigate if U.S. Immigration and Customs Enforcement is utilizing its attaché offices as the foundations for a transgovernmental network capable of combating terrorist travel. In order to accomplish this investigation, qualitative research methods will be employed in order to assess, first, if ICE's attaché offices view combating terrorist travel as a critical mission that they are indeed carrying out, second, what methods they are employing to combat this threat, and finally, how officers interact with members of their own agency as well as with their international partners. It is my belief that this inquiry will reveal that ICE attaché offices are in fact a transgovernmental network being utilized to combat terrorist travel and are doing so in much the same way that transnational advocacy networks work to combat problems that are global in nature.

CHAPTER FOUR: RESEARCH DESIGN AND METHODS

One of the most important aspects of conducting social science research is selecting an appropriate research design in order to achieve the project's goals. The researcher must first decide whether to use a quantitative or qualitative approach. Once the appropriate approach is selected the researcher must decide on the proper methods to employ to answer the research question. A frame for the research must be established that operationalizes and conceptualizes the research, the units of analysis, data collection design and establishes the data analysis methods. These steps can be further complicated when the phenomenon being studied presents particular problems to any one of the steps. This is particularly true when conducting research on topics related to national or international security, given the secretive nature of the data or the subjects being studied.

Challenges presented by when researching topics related to terrorism

Conducting a scientific investigation into terrorism and the effectiveness of border security is a challenging endeavor. There are two reasons for this: first, collecting data on terrorism is obviously a difficult task given that terrorists, by necessity, operate clandestinely and are secretive about details of their operations (Leiken and Brooke 2006: 504). Second, all clandestine transnational actors (CTAs), including members of a criminal organization, drug traffickers and terrorists, pursue activities related to crossing international borders covertly because they want to avoid detention and apprehension

(Rees 2006: 7). This means that gathering data on what facilitated or prevented the border crossing of unidentified CTAs in most cases is difficult if not near impossible.

It would be easy to conclude that since no large-scale terrorist attacks have been successfully carried out by members of the global Salafi jihad movement since the September 11 attacks the United States' efforts to prevent terrorists from crossing its border have been successful. This claim of success however would be little more than specious reasoning. The same claim of success could have been made of the United States' attempts following the 1993 World Trade Center bombing to improve border security and increase enforcement of immigration laws up until September 10, 2001. In fact, at this moment individuals with close ties to organizations affiliated with al-Qaeda and the global Salafi jihad movement may have already defeated the United States' attempts to strengthen border security and have successfully entered the United States to plan and carry out attacks on a massive scale.

Unfortunately, when trying to evaluate the effectiveness of strategies put into place in order to prevent terrorist travel, there is no way to accurately measure success, only failure. For the most part, there are only data available on those individuals who have been identified as carrying out an activity relating to terrorism successfully. Those individuals who were encountered and prevented from carrying out their activity would not be included in the data if the true intentions of their actions were not uncovered. One instance of when a terrorist was successfully denied entry into the United States but his true intentions was not known until after an attack is the case of Mohamed al Kahtani.

Kahtani, who is frequently referred to as the 20th September 11 hijacker, attempted to enter the United States through Orlando International Airport on August 4,

2001. Kahtani was refused admission into the United States because his initial behavior raised suspicions of the immigration officers at the port of entry. He subsequently became hostile and refused to answer questioned regarding his trip to the United States. When Kahtani was refused admission, his photograph and fingerprints were taken as a routine part of the processing of his refusal. Kahtani was later captured in Afghanistan following the U.S. invasion and a check of his fingerprints linked him to the August 4 refusal. Further investigation into Kahtani's attempted entry into the United States revealed that Mohammed Atta was waiting for him at the airport on August 4, linking him directly to the September 11 attacks (9-11 Commission 2004a: 29-30).

Kahtani's inability to enter the United States stands as one example of U.S. officials successfully preventing a terrorist from entering its territory. Kahtani's case also highlights the difficulty in uncovering examples of border security strategy successes. The significance of Kahtani's entry refusal only came to light after the September 11 attacks were successfully carried out. In addition, if he was not subsequently captured in Afghanistan, his connection to the attacks may never have been known. There is no telling how many other Mohamed al Kahtanis were refused entry into the United States or other target countries. Unfortunately, the available data are significantly greater for those individuals who successfully gained entry into a target state such as those individuals discussed in great detail in Chapter 3, highlighting border security strategies' failures rather than successes.

Establishing a Frame for Research

As discussed in previous chapters, one of the strategies adopted in an attempt to prevent terrorists from crossing borders has been to assign immigration officers to work

in another jurisdiction with their foreign counterparts. While trying to determine the success of this strategy would be a noble pursuit, there is no way to accurately quantify and scientifically measure any potential success. First, as explained above, gathering data on terrorist border crossings is skewed, as it highlights failures and not successes. Second, any attempt to conclude scientifically how successful a particular strategy to prevent terrorist travel has been would require quantitative research methods and considerable statistical analysis. The number of immigration officers assigned to work in foreign jurisdictions is relatively small and obtaining results that could be considered statistically significant within an acceptable level would require nearly 100% participation of the total population examined. Achieving this level of participation when participation in the research is voluntary is highly unlikely, and such a research project utilizing quantitative research methods on these immigration officers is not practical.

The use of quantitative research methods in order to determine if the strategy of assigning immigration officers from one country to work with foreign counterparts in order to prevent terrorists from crossing borders is useful is not realistic endeavor. For this reason, this paper sought to explore only how immigration officers assigned overseas operate in furtherance of this strategy to prevent terrorist travel, not whether this strategy is actually successful. In order to answer this research question, the qualitative research method of a case study was employed in order to determine how attachés from U.S. Immigration and Customs Enforcement specifically operate within foreign jurisdictions to prevent terrorists from crossing borders to support, finance and carry out operations.

The decision to utilize a case analysis approach in an attempt to answer the research question was not arbitrary. The literature on both transnational advocacy

networks (TANs) and transgovernmental networks suggest that these two network types

operate in a similar fashion in order to accomplish their goals. Given that *Activists*

Beyond Borders by Margaret E. Keck and Kathryn Sikkink is regarded as a pioneer work

in the field of transnational activist networks (Brenner 1998:189), it would seem wise to

look to it for inspiration for conducting research on transgovernmental networks. When

Keck and Sikkink began their research on TANs, there had been little in the way of either

theoretical or empirical research of these networks types. Keck and Sikkink were entering

uncharted territory, and so their goal was to discover new theories and patterns relating to

the activities of TANs rather than hypothesis testing. In order to accomplish this goal,

they employed a qualitative research method known as grounded theory (Keck and

Sikkink 1998: 5).

Unlike quantitative research, which is usually concerned with future events and

behavior, qualitative research seeks an understanding of social interaction and processes

in an organization. Qualitative research is said to be more generalizable and study results

can be applied to other situations (McNabb 2004: 343), which makes it a valuable tool

when trying to explain or interpret why a particular situation exists or a social interaction

occurs. The grounded theory approach to qualitative research methods, which was

utilized by Keck and Sikkink, is primarily concerned with developing theories from

gathered data rather than testing predetermined theories. Data are collected, analyzed and

interpreted by the researcher for commonalities and differences, who then uses this

analysis and interpretation to develop theories about situations studied (McNabb 2004:

352). It is by analyzing the data of various social movements in different historical eras,

including three modern social movements, that Keck and Sikkink (1998) were able to

develop their theories that TANs are brought together because of shared values, a common discourse and a dense exchange of information and services (1-2); are characterized by their voluntary, reciprocal and horizontal patterns of communication between committed and knowledgeable actors working in a specific issue area (8); work to create categories or "frames" to generate and organize information on which they base their campaigns (10); and the belief by network members that networking will further their mission, consequently establishing international contacts in order to form networks (12).

Operationalizing and Conceptualizing Research

The literature relating to transgovernmental networks today is richer than the literature relating to TANs that existed when Keck and Sikkink began their initial research. As such, numerous theories have developed about how transgovernmental networks develop and operate (Keohane and Nye 1974, Slaughter 2004, Hajer and Versteeg 2005 and Slaughter and Zaring 2007). As such, the research in this paper does not attempt to add to the theoretical framework relating the overall topic of transgovernmental networks, but rather uses these existing theories to investigate how a transgovernmental network comprised of immigration officers assigned to foreign jurisdictions operate in order to prevent terrorist travel. The limited scope of this research does not lend itself to the ground theory approach utilized Keck and Sikkink, though the theories developed by Keck and Sikkink, as well as the theories found in the existing literature, are of great importance to hypothesis development. The work of Keck and Sikkink, as well as the existing literature on transgovernmental networks, suggests numerous similarities in the way TANs and transgovernmental networks operate to

achieve their goals. These similarities seem to indicate that the anticipated answer to the research question would be that *immigration officers assigned to foreign jurisdictions operate and interact with one another in an attempt to prevent terrorist travel in much the same way that members of transnational advocacy networks interact and operate in order to address their target problem.*

In order to answer the research question and test this hypothesis, a case analysis approach was used. A case study was conducted regarding how attachés from U.S. Immigration and Customs Enforcement specifically operate within foreign jurisdictions to prevent terrorists from crossing borders to support, finance and carry out operations. This approach focuses on agencies, organizations, a person or a group rather than dealing with variables. The objective of this approach was to serve as the "defining description of the organization" and serve as an example of similar groups (McNabb 2004: 352). The purpose of using the case analysis approach is to study a case because it provides insight into a particular issue, characteristic, problem or phenomenon not of interest in the specific case being studied (McNabb 2004: 358). Case studies are particularly appropriate when the researcher wants to establish a theory, test theories that already exist, identify conditions that lead to or contribute to a phenomenon, establish the relative importance of those contributing conditions and establish the relative importance of the case as it relates to other potential examples (McNabb 2004: 359). Given the criteria, a case analysis approach appeared to be an appropriate method for exploring the larger question of how transgovernmental networks are utilized to combat crime that is international in scope.

Units of Analysis

A case study is not intended to provide results that are representative of the entire world. Rather, the results simply represent the specific case or cases (McNabb 2004: 359). In order to answer the researcher question of how transgovernmental networks are used to combat crime that is international in nature, a single case study design was utilized. This study proposed to explore the ways in which one type of transgovernmental network comprised of law enforcement officers assigned in foreign jurisdictions is utilized in combating a particular activity of international criminal. More specifically, how attachés from U.S. Immigration and Customs Enforcement assigned to foreign countries operate in order to combat terrorist travel. A "unit of analysis" refers to individuals, groups, processes or organizations that are examined in a case study (McNabb 2004: 364). In this case study, ICE attachés were the units of analysis studied in order to answer the research question.

The results of this research cannot be universally applied to all transgovernmental networks or even all transgovernmental networks comprised of law enforcement officers, nor does it intend to. The selection of ICE attachés as the unit of analysis were an attempt at narrowing down the relevant data in order better manage the research. The goal of this study is to understand this particular strategy to combat terrorist travel and to provide greater insight into transgovernmental networks as a whole that may lay the foundation for further research into this emerging phenomenon in global governance.

Subject Recruitment and Data Collection

The recruitment of individuals to participate in this research presented several challenges. The most common methods for data collection in a case study are interviews,

observations and document analysis. Given that the units of analysis are individuals —

ICE attachés — interviews appeared to be the best data collection method. Interviews

usually occur as a conversation between the researcher and the research subjects. These

interviews can occur where the interview has a basic conversation guide or an idea of

what topics should be covered, allowing the respondent to freely provide answers that

come to mind. An interview may also be more structured, where respondent is asked to

reply to specific open-ended questions. However, in this research, the characteristics of

the units of analysis did not allow for recruitment and interviewing techniques using the

standard methods found in more traditional case studies.

ICE attachés are assigned to scores of different countries around the globe.

Distances between ICE attachés made in-person interviews impossible and the variety of

time zones in which ICE attachés are assigned made telephonic interviews impractical.

These same difficulties existed in the initial recruitment of research subjects and are

compounded by the nature of the ICE attaché position. While the existence, duties, roles

and responsibilities of these positions are not secret, there are no databases readily

available to the general public that list the contact information for ICE attachés

throughout the world. Even if such a database did exist, it is unlikely that these attachés

would voluntarily consent to participate in the research without first obtaining approval

from their agency. For these reasons, assistance for this research was requested directly

from U.S. Immigration and Customs Enforcement in the recruitment and questioning of

subjects.

The ICE attaché positions are the responsibility of the Office of International

Affairs component of U.S. Immigration and Customs Enforcement. In order to obtain the

agency's assistance in the research a request was sent to the Director of the Office of International Affairs outlining the research project and requesting his assistance in the recruitment of research subjects, as well as the delivery of the request for participation. The Director was asked to forward the researcher's letter requesting participation in the research to all ICE attachés throughout the world along with his approval for them to participate in the research. The letter was sent to the attachés via the agency's internal e-mail system and was accompanied by an e-mail from the Director granting his permission for participation in the study while advising that their participation in the research was purely voluntary. It is important to note that the dissemination of the request letter to the attachés and the granting of permission to participate in the research is the extent of U.S. Immigration and Customs Enforcement's involvement in this research project. The agency in no way supported this research, nor was it involved in the research design. However, this research project could not have been undertaken without the assistance of the Director of the Office of International Affairs, for which the researcher is extremely grateful.

As stated above, the fact that ICE attachés are scattered across the globe made conducting face-to-face or telephone interviews either impossible or impractical. In addition, in an attempt to maximize the number of responses, participating in this research project needed to be as effortless and undemanding as possible. For these reasons, as well as to assist in the organization of responses, the data collection method of questionnaires, which are often used in quantitative research methods, was utilized in lieu of interview types traditionally found in qualitative research methods. The benefit of questionnaires is that they are flexible, can be custom-designed to meet the objective of

almost any type or research project and can be designed to gather information from any group of respondents (McNabb 2004: 364).

The questionnaires were designed to: 1) Help better understand the respondent's organization and working environment; 2) Understand how the respondent in his or her official capacity attempts to curtail, combat or prevent criminals, smuggled or trafficked people, terrorists and other individuals crossing international borders in violation of the laws of any nation-state; 3) Get the respondent's opinion on how, in his or her official capacity, they are being utilized to attempt to curtail, combat or prevent criminals, smuggled or trafficked people, terrorists and other individuals crossing international borders, as well as what steps can and should be taken in order to be more successful in these areas. The majority of the questions on the questionnaire were of close-ended, structured or scale-type varieties, including attitude, importance and rating scales. The reasoning behind using these types of questions was for better organization and analysis of the data. However, recognizing the value of open-ended questions, each question provided the respondent the opportunity to qualify the answers provided, provide additional information they felt may have been missed in the structure of the question or provided any other information or comments they deemed necessary. Using this type of question structure allowed for the organizational benefits of structured close-ended questions while also preserving the free flow of information and ideas that are characteristic of open-ended interview questions.

The questionnaire was created, posted on the Internet and the responses stored using Questionpro.com, a website that allows for questionnaires to be constructed completed and securely stored, accessible only by the researcher. The questionnaire, once

created, could be accessed by the respondents by typing the questionnaire's internet

address into any web browser or clicking on a hyperlink that linked to the questionnaire.

This link was placed in a letter requesting participation in the research project, while also

outlining the purpose and goals of the research project and describing what their

participation required. If the attaché consented to participate in the research, he or she

could simply click on the hyperlink and begin the questionnaire.

Questionnaire Design and Analyzing Data

An added benefit of using a questionnaire for data collection is that responses that

are more uniform in language and meaning allow easier analysis of the data through basic

statistical analysis. Given that this research project employed a single case study design

that does not claim to representative of a population, the detailed and complex statistical

analysis utilized in quantitative research was not be employed. The goal of this research

project was not to achieve a statistically significant test of the hypothesis. Rather, it only

seeks to give insight into the research questions, test the general theory asserted in the

hypothesis and serve as a foundation for future research into the phenomenon that is

studied. To achieve this objective, data collected from the questionnaires were measured

for frequency and basic central tendencies of responses when appropriate. The measure

for determining central tendencies for responses to specific questions varied depending

on the specific data each particular question were attempting to collect.

The questionnaire was divided into three sections. The first section attempted to

gather characteristics of the respondents and their work environment. The first two

question in this section (Questions 1 and 2) seek to confirm the agency for which the

respondent is employed and their job title. This step was taken as a precaution, given the

means by which the request for participation was disseminated. As the request was sent via e-mail, it could easily be forwarded to unintentional recipients who could then use the hyperlink to access and complete the questionnaire. Nowhere in the letter requesting participation was the title of the respondents or the agency for which they worked stated, therefore if a respondent was unable to answer this questions correctly it could concluded that he or she was not an intended recipient of the request and the responses could be excluded.

The remaining questions in this section attempted to determine the characteristics of the respondents. This portion of the questionnaire was limited to three questions because the research required a degree on anonymity on the part of the respondent. Given that the population was relatively small, the inclusion of additional questions might have lead to the respondent's identity being revealed even if a large response rate to the questionnaire was obtained. These descriptive questions were limited to: total years of experience as an immigration, intelligence and/or law enforcement officer (Question 3), geographical area of responsibility (Question 4), and office location where the respondent usual reports on a daily basis (Question 5).

Question 3 was a rating scale question that will determine the total years of experience the respondent has as an immigration, intelligence and/or law enforcement officer. The respondent could choose from the follow categories: less than 5 years experience, 5 to 10 years experience, 10 to 15 years experience, 15 to 20 years of experience, and more than 20 years experience. The answers would be analyzed in an attempt to obtain the arithmetic mean of the number of years of experience of the respondents. In order to calculate the arithmetic mean, each possible response was

assigned a value between 1 and five with 1 as the value for less than 5 years experience

and 5 as the value for more than 20 years experience. The total number of answers for

that category was then multiplied by the value assigned to that category in order to get a

category score. The score for each category was added and the sum of the category scores

was divided by the total number of responses in order to obtain the arithmetic mean of the

number of years of experience of the respondents.

The symbols below are used to signify the variables in the calculation described

to determine the arithmetic mean:

N = total number of respondents
n = number of responses for that category
V = value assigned to the category
X = arithmetic mean

The formula used for calculating the arithmetic mean was:

$$[(n^1 * V^1) + (n^2 * V^2) + (n^3 * V^3) + (n^4 * V^4) + (n^5 * V^5)] \div N = X$$

Additional attitude, importance and rating scale questions were used throughout the

questionnaire. When the responses to these scale questions were analyzed in order to

determine the arithmetic mean, a similar formula was utilized. Once the arithmetic mean

was determined it was plotted on a line graph representation of the scale. Using the

question regarding years or experience as an example, if the arithmetic mean was

calculated as 3.6 then the arithmetic mean would plot between 10 to 15 years and 15 to

20 years on the line graph representation of the rating scale of experience.

Questions 4 and 5 were related to the physical location of the respondent's duty

location. As this research is trying to determine if the ICE attachés form the basis for a

global network, it is important to understand how these officers are dispersed around the

world and what type of environment they work in on a day-to-day basis. The respondents

were first asked to describe their geographical area of responsibility. They were asked to put their area of responsibility into one of eight geographical categories. These categories were: North America, Latin America and the Caribbean, Western Europe, Eastern Europe, Middle East and North Africa, Sub-Sahara Africa, Central or South Asia, East Asia, and Southeast Asia or Oceania. The respondents were next asked to select a category that best describes their office location, such as embassy or consulate, port of entry or local law enforcement agencies office. Given the wide variety of possible answers to this question, the respondent was provided with seven broad categories to describe their office location and could have also select "other" and provide their own description.

Both of these questions were descriptive in nature. Since the collected data are descriptive, there was no measure for central tendencies. The only statistics of interest for these questions were the frequency of particular responses. When reporting frequency of responses for the question regarding office locations, each different answer reported in the "other" category would be reported as if it were its own category rather than simply reporting the frequency with which the respondents reported "other".

The second section of the questionnaire attempted to understand how the respondents, in their official capacity as an ICE attaché, work to curtail, combat or prevent criminals, smuggled or trafficked people, terrorists and other individuals from crossing international borders in violations of the laws of any nation. In order to understand how the respondents accomplish this goal, they were first questioned about how much time they dedicate to this mission, how much time they dedicate to other duties and the amount of time dedicated specifically to trying to prevent terrorist travel.

Next they were questioned about specific activities related to curtailing, combating or preventing individuals from clandestinely crossing borders, what other agencies they work with and how they interact with these agencies.

The first question of the second section (Question 6) was a rating scale that asked the respondent to rate to what extent they agree with the statement: "Curtailing, combating or preventing criminals, smuggled or trafficked people, terrorists and other individuals from crossing international borders in violations of the laws of any nation is the primary job responsibility as an officer assigned overseas." The rating scale for this question was an attitude scale consisting of five choices that range from strong agreement to strong disagreement. The question also gave the respondents the option to answer that they "do not know." The answers were then analyzed in an attempt to obtain the arithmetic mean in a similar way as the arithmetic means was obtained for the number of years of experience of the respondents. Where this formula differed from the one used for years of experience was that the value assigned to "I do not know" or "I choose not answer" were zero and the number of people who selected one of these two categories were excluded from the total number of respondents when calculating the arithmetic mean. The formula used for calculating the arithmetic mean was:

$$\frac{[(n^1 * V^1) + (n^2 * V^2) + (n^3 * V^3) + (n^4 * V^4) + (n^5 * V^5) + (n^6 * V^6) + (n^7 * V^7)]}{(N - n^6 n^{7)}} = X$$

Once the arithmetic mean was determined it was plotted on a line graph representation of the respondents' attitude towards the questions.

The next two questions in the second section (Questions 7 and 8) were closely related to Question 6. Question 7 was an open-ended question that asked the respondent to list other job responsibilities besides "curtailing, combating or preventing criminals, smuggled or trafficked people, terrorists and other individuals from crossing international borders in violations of the laws of any nation." Question 8 was a rating scale that asked the respondent to rate to what extent they agreed with the statement: "The duties listed in Question 7 are my primary job responsibility as an officer assigned overseas." The Data collected in Question 7 were analyzed in order to determine the frequency that specific "other job responsibilities" were reported by the respondents in an attempt to gain a snap-shot of what those "other job responsibilities" may be. The rating scale and formula for calculating the arithmetic mean was identical to those employed for analyzing the responses to Question 6. This allowed for easier comparison between the respondents' attitudes to the two questions and the respondents' attitudes about what they perceived as their primary job responsibilities.

The primary objective of this questionnaire was to get a better understating of how the ICE attachés work to prevent terrorist travel. While the job responsibilities discussed in Questions 6 and 7 have an impact on an attaché's ability to prevent terrorist travel, these responsibilities are not exclusively to prevent terrorist travel. Question 9 asked the respondent to rate to what extent their official duties are "dedicated specifically to combating terrorist travel." The respondent was asked to select on of seven categories that best describe the amount of time spent combating terrorist travel ranging from "none" to "this is my only responsibility." The five categories between the two ends of the range let the respondent select from 20 percent increments, e.g. "1-20%" or "21-

40%." The answers were analyzed in an attempt to obtain the arithmetic mean in the same way the number of years of experience respondents have in Question 3 was calculated. Each possible response was be assigned a value between 0 and 6, with 0 as the value for "None" and 6 as the value for "This is my only responsibility." Once the arithmetic mean was determined it was be plotted on a line graph representation of the scale.

The five remaining questions of the second section of the questionnaire, with the exception of question 12, used a modified Likert scale to measure how the respondent rates certain items. The Likert scale, which is by far the most favored attitude measuring scale used in social science research today, asks the respondent to express his or her opinion regarding a pool of items (McNabb 2004: 161). Traditionally, when using a Likert scale, the respondent is asked to rate the extent with which he or she is in agreement with each item on the list. The extent of agreement is measured on a five point scale ranging from strongly agree to strongly disagree, with each response assigned a value between one and five.

The remaining questions in the second section were not seeking to determine the extent to which the respondent agreed with particular items, but were asking for various items in the question to be rated on a consistent scale. While not its traditional use, the Likert scale can be modified to rate items in a consistent scale beyond degrees of agreement with a particular statement. Using a consistent scale, the respondent were asked to rate various items related to how they are involved in "curtailing, combating or preventing criminals, smuggled or trafficked people, terrorists and other individuals from crossing international borders in violations of the laws of any nation." The items and rate

scale differed from question to question in an attempt at obtaining a larger picture of the respondent's work towards achieving this goal. The frequency of the ratings and the arithmetic mean for each item were reported to allow for comparison to the other items listed in the question. The formula for determining the arithmetic mean for each item in these questions was the same formula used in Question 6.

The first question (Question 10) utilizing the modified Likert scale asked the respondent to rate his or her level of responsibility in dealing with issues specifically or directly related to "curtailing, combating or preventing criminals, smuggled or trafficked people, terrorists and other individuals from crossing international borders in violations of the laws of any nation." The items for the question related directly to the numerous entry methods used by terrorists to cross international borders as described in great detail in Chapter 3. This question contained nine items such as "monitoring methods of illegal entry into the host country" or "working with host countries to monitor suspicious travel of its citizens." The respondents rated each item on a six point scale ranging from "this is my primary responsibility" to "I never deal with this issue," with each possible response being assigned a value between five and zero. The respondents were also given the opportunity not to answer a particular item. This question, along with all the remaining questions in section 2 allowed the respondents to provide additional items not already covered in the questions.

The next question (Question 11) attempted to determine who the respondents interact with on a regular basis as part of a possible larger transnational network to terrorist travel. The respondents were asked to indicate the frequency of their interaction and contact with others who may be responsible for "curtailing, combating or preventing

criminals, smuggled or trafficked people, terrorists and other individuals from crossing international borders in violations of the laws of any nation." The items included in this question include other agencies within the respondent's government, the immigration agency of the host country, other law enforcement and intelligence agencies, foreign ministries, international or regional organizations and private stakeholders such as NGOs of airlines. The respondents were asked to rate each item based on a five point scale ranging from primary contact to no contact.

The next question (Question 12) was concerned with how interaction occurs between the respondents and the items listed in the previous question. The item list was identical to that of the previous question and the respondents were asked to describe how the interaction occurs. The possible responses included electronic communication, dissemination of official reports, through secure communications, unofficial meetings, official meetings and no contact. While the modified Likert scale model provided the format for this question, the data were not be analyzed in the same way as the other questions in this section that used the modified Likert scale. The reason for this was that the respondents were not asked to rank the type of contact, only to describe it. Therefore, the data analysis was only concern itself with the frequency of responses.

Question 13 attempted to use the modified Likert scale to measure the frequency of specific activities undertaken by the respondents to further "curtailing, combating or preventing criminals, smuggled or trafficked people, terrorists and other individuals from crossing international borders in violations of the laws of any nation." The respondents were asked to rank each item on a five point scale ranging from "Primary Means" to "Never." The items in this question included such activities as investigation

coordination, intelligence and information sharing and providing training or advice. The next question (Question 14) then asked the respondents to indicate the level of authorization needed to conduct these specific activities addressed in the previous question. This question attempted to measure the level of independence granted to the respondents to carry out these activities. The literature on transgovernmental networks states that the benefit of these types of networks is their fluidity and ability to respond to situations quickly. The fewer restraints placed on network members the more fluid the network becomes. The respondents were asked to rate the level of authorization needed to conduct each item on a five point scale ranging from "little or no previous authorization" to that the activity is "never conducted."

The final question in this section (Question 15) asked the respondents to indicate "any activities, methods and responsibilities as an officer assigned overseas that were not already covered in this section." The questionnaire, while trying to keep some characteristics of open-ended, face-to-face-interview style questions, was comprised primarily of close-ended structured questions out of necessity. Question 15 was designed to allow the respondents to fill in the blanks of the questionnaire and provide additional data they felt were important. As exploratory qualitative research, any additional information that the respondents supplied was useful, especially if a pattern develops when compared with other responses. In an attempt to determine if such patterns existed, the responses provided were analyzed to determine frequency of responses provided. This analysis allowed for the uncovering of any significant gaps in the questionnaire's data while also providing a catalyst for further research.

The third and final section of the questionnaire seek to obtain the respondent's opinion regarding how, as an officer assigned overseas, he or she is being used to further the goal of "curtailing, combating or preventing criminals, smuggled or trafficked people, terrorists or other individuals from crossing international borders in violations of the laws of any nation." It was the hope that this section would, with the help of the respondents who are the frontline personnel responsible for the day-to-day operations of their agencies' mission, identify gaps between what is being done to combat terrorist travel and what should be done. Often, when an organization is tasked with a specific mission, there remain numerous bureaucratic impediments to accomplishing the organization's goals and often there are disparities between what is being done and what needs to be done. It was hoped that this section would not only point out these impediments and disparities but also identify the best practices that could be shared with other organizations that are attempting to achieve similar goals or face similar challenges.

The first question of the third section (Question 16) asks the respondents their opinion as to the amount of time in their official capacity they should dedicate specifically to "curtailing, combating or preventing criminals, smuggled or trafficked people, terrorists and other individuals from crossing international borders in violations of the laws of any nation." The respondents were asked to rate how much time they should dedicate to this mission based on an attitude scale consisting of six choices that range from "this should be my only responsibility" to "this should not be my responsibility." The question also gave the respondents the option not to answer by selecting the response "choose not to answer."

Question 17 asked the respondents to rate the amount of time that should be dedicated to responsibilities not related to "curtailing, combating or preventing criminals, smuggled or trafficked people, terrorists and other individuals from crossing international borders in violations of the laws of any nation." The respondents were asked to rate how much time should be dedicated to these other responsibilities based on an attitude scale consisting of five choices that range from "I should have no other responsibility" to "no time should be dedicated to these issues." The question also gave the respondents the option not to answer by stating "choose not to answer." The next question (Question 18) asked the respondents to rate to what extent of their official duties should be "dedicated specifically to combating terrorist travel?" The respondents were asked to select one of seven categories that best describe the amount of time spent combating terrorist travel ranging from "none" to "this is my only responsibility." The five categories between the two ends of the range will let the respondent select options in 20 percent increments, e.g. "1-20%" or "21-40%."

The formulas used to evaluate data gathered in Questions 16, 17 and 18 was the same formula used to evaluate data gathered in Questions 6, 8 and 9. The consistency in the formulas used to evaluate data captured in these various questions allowed for better comparison of data between these questions. While Questions 6, 8 and 9 asked the respondents to provide an impression about how much time is dedicated to "curtailing, combating or preventing criminals, smuggled or trafficked people, terrorists and other individuals from crossing international borders in violations of the laws of any nation," to other responsibilities besides those dedicated to these areas and those areas dedicated specifically to preventing terrorist travels. Questions 16, 17 and 18 asked how much time

should be dedicated to these activities. Using similar formulas for evaluating the responses to these questions allowed for improved comparison between how the respondents felt they are actually working to prevent terrorist and how they should be working to prevent terrorist travel.

The next question (Question 19) asked the respondents to use a Likert scale to rate the importance of various characteristics of the individuals with whom they deal with as part of their regular course of duties. This question contained sixteen items, including such characteristics as citizenship, education level, profession and previous relationships. The respondents were asked to rate the level of importance of each item on a five point scale ranging from "Extremely Important" to "Not important at all." The respondents could also choose not to answer for any of the items. The aim of this question was to identify those characteristics that were perceived as most significant when network members interact with one another.

The remaining questions of the questionnaire seek to identify possible impediments that could prevent the respondents from effectively achieving their goals while also identifying the best practice for overcoming these challenges. Given the nature of the questions, the variety of possible answers and the hope of obtaining as much useful data as possible, most of the remaining question were open-ended. This allowed the respondents to provide as much or as little information as he or she wished. The information provided was analyzed to determine if patterns developed among the responses.

The respondents were first asked to describe additional factors or resources not already covered in the questionnaire that assist them in "curtailing, combating or

preventing criminals, smuggled or trafficked people, terrorists and other individuals from

crossing international borders in violations of the laws of any nation" (Question 20).

They were then asked to describe additional situations or factors that make it more

difficult to achieve these goals. (Question 21) The respondents were next asked to rate

their current work environment, ranging from excellent to very poor, and then provide

information on how that work environment can be improved (Questions 22 and 23).

Next, the respondents were asked to rate overall job satisfaction, ranging from excellent

to very poor, and then provide information on how job satisfaction can be improved

(Questions 24 and 25).

Finally, the respondents were given the opportunity to provide any additional

information regarding his or her role as an officer assigned overseas or any concerns or

comments about the questionnaire. This gave the respondents the ability to fill in any

gaps and provide important information that may have been missed by the other

questions. It was the questionnaire's goal that this, along with the other questions, would

provide a comprehensive picture of how one type of transgovernmental network

functions in order to deal with one type of transnational problem. It is the hope that by

understanding how ICE attachés and their transgovernmental network work to combat

terrorist travel, valuable insight was obtained into how transgovernmental networks

behave and provided a platform for further research into this type of global governance.

Hypothesis Test

As stated earlier in this chapter, the existing literature on transnational advocacy

networks and transgovernmental networks suggests numerous similarities in the way

these two types of networks operate to achieve their goals. These similarities have led to

the development of a hypothesis that states that immigration officers assigned to foreign

jurisdictions operate and interact with one another in an attempt to prevent terrorist travel

in much the same way that members of transnational advocacy networks interact and

operate in order to address their target problem. The methods employed to examine how

these particular officers operate and interact with others was exploratory qualitative

research rather than quantitative methods which uses complex statistical analysis in order

to prove a hypothesis that can be universally applied. This research only looked to see if

the hypothesis appears correct when dealing specifically with ICE attachés.

      The existing literature on TANs claims that these networks have taken advantage

of advancements in communication to quickly organize, mobilize and share information

and services around the globe for the benefit of their expressed goals or concerns. They

brought together shared values, a common discourse and a dense exchange of

information and services. Network members often identify themselves more by their

cause and membership in the TAN than their own nationality, ethnic group or culture.

They often act independently with little centralized control. While the network members

usually belong to a larger hierarchical organization that frames issues or set priorities,

they usually share information and services, and coordinate activities horizontally with

other network members along regular, informal patterns. These characteristics appear to

exist regardless of whether the networks are honorable, such as a human rights network,

or dubious, such as a criminal or terrorist network.

      Transgovernmental networks also share many of these same characteristics with

TANs. Members of these networks communicate and interact amongst themselves in

order to share information, collect and disseminate best practices and provide technical

assistance and training to those officials who have less experience in specific areas than their network colleagues. Communication and interaction occurs between network members of various governments horizontally, with little control or guidance by the leadership of their agency or the chief executives of those governments other than "framing" the issues to be dealt with through their policies. As interaction with other network members becomes more regular and frequent, bonds and a sense of mutual trust develop, which leads to an environment in which individuals may even begin to define themselves as part of this professional group, rather than in purely national terms. This interaction becomes more frequent and easier with advancements in communication and allows for the network to expand further and quicker.

Both TANs and transgovernmental networks are horizontal networks that share information and services in pursuit of a common goal among network members. Advancements in communication have allowed this interaction between members to occur with more frequency and with little interference from a larger hierarchical organization. The frequency of this interaction has resulted in the development of bonds and a collective identity around a particular cause or identity and an environment that allows for the network to expend quickly. If these same characteristics exist in the methods utilized by ICE attachés in "curtailing, combating or preventing criminals, smuggled or trafficked people, terrorists and other individuals from crossing international borders in violations of the laws of any nation," then the hypothesis that immigrations officers assigned to foreign jurisdictions operate and interact with one another in an attempt to prevent terrorist travel in much the same way that members of transnational advocacy networks interact and operate in order to address their target problem would

appear to be true. In order to determine if these characteristics exist, the responses give to

several of the questions in the questionnaire was analyzed using the following matrix:

Characteristics	Question	Expected Results for Hypothesis
Mean of Interaction	Question 12	Frequency of electronic communication and unofficial meetings should be more frequent than other means of interaction.
Type of interaction	Question 13	Rating for information-sharing should be higher than more formal interaction.
Level or Authorization	Question 14	Ranking of the level of authorization interaction should be low.
Common Identity	Question 20	Profession and previous interaction should be viewed as more important than nationality or agency.

If the respondents answered the questions listed above as anticipated then it would appear

that the hypothesis is correct. If questionnaire responses are not as expected then the

hypothesis would appear incorrect and a network of immigrations officers assigned

overseas would not function in the same way as transnational advocacy networks, and

only share some similar characteristics.

Regardless of whether the hypothesis is true, the questionnaire provided valuable

date on how ICE attachés operate overseas to prevent terrorist travel while providing a

picture of how immigrations officers assigned overseas work to achieve their goals. It is

the hope that this research provided the foundation for further exploration into the

phenomenon of transgovernmental networking. If the hypothesis does appear true, it

would suggest the transgovernmental networks may be one model for a counterterrorism

strategy of confronting "networks of terror with networks against terror."

**CHAPTER FIVE: RESEARCH RESULTS-HOW ICE ATTACHÉS OPERATE**

The questionnaire's design combined close-ended and open-ended questions in order to: 1) Help better understand the respondent's organization and working environment; 2) Understand how the respondent in his or her official capacity attempts to curtail, combat or prevent criminals, smuggled or trafficked people, terrorists, and other individuals crossing international borders in violation of the laws of any nation-state; 3) Get the respondent's opinion on how, in his or her official capacity, they are being utilized, as well as what steps can and should be taken in order to be more successful in these areas. It was effective. The information from the respondents provided valuable insight into not just how ICE Attachés work to "curtail, combat or prevent criminals, smuggled or trafficked people, terrorists and other individuals crossing international borders in violation of the laws of any nation-state," but also provided valuable data on other duties and responsibilities. A total of 33 ICE attachés participated in this research project, and 24 completed the entire questionnaire.

Who are ICE Attachés?

As stated in the last chapter, the goal of the first sections of the questionnaire was to determine the characteristics of the respondents in relation to their position as ICE attachés. This section was comprised of descriptive questions to determine their number of years of experience as immigration, intelligence, and/or law enforcement officers, their

geographical area of responsibility, and the office location of the respondents. What the

data revealed were that the majority of the respondents had between 10 and 20 years of

experience as immigration, intelligence, and/or law enforcement officers, the respondents

are stationed throughout the globe, and they overwhelmingly work within a consulate or

embassy of the United States.

The following chart is a representation of how the respondents answered the

question regarding their experience as immigration, intelligence, and/or law enforcement
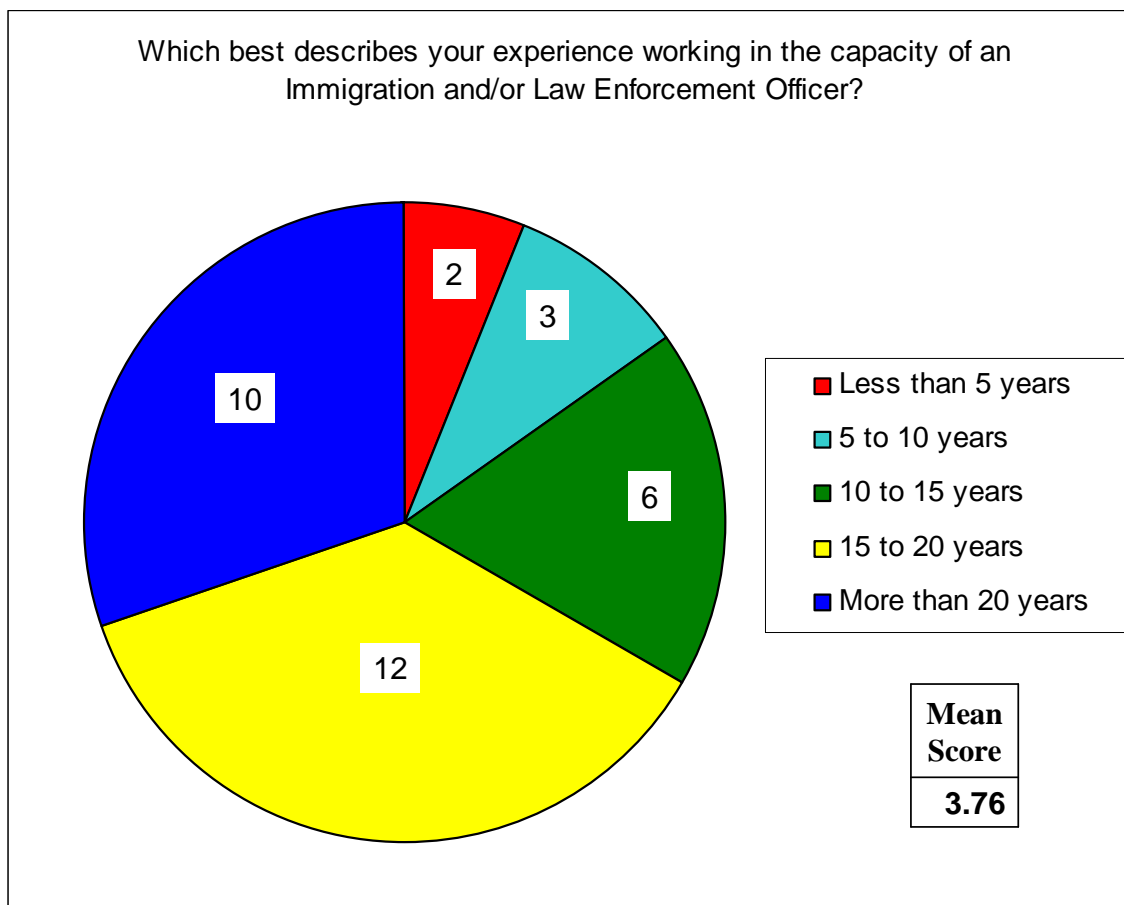
officers:

As the chart clearly illustrates, over one-third of the 33 respondents had between 15 and

20 years of experience as immigration, intelligence, and/or law enforcement officers.
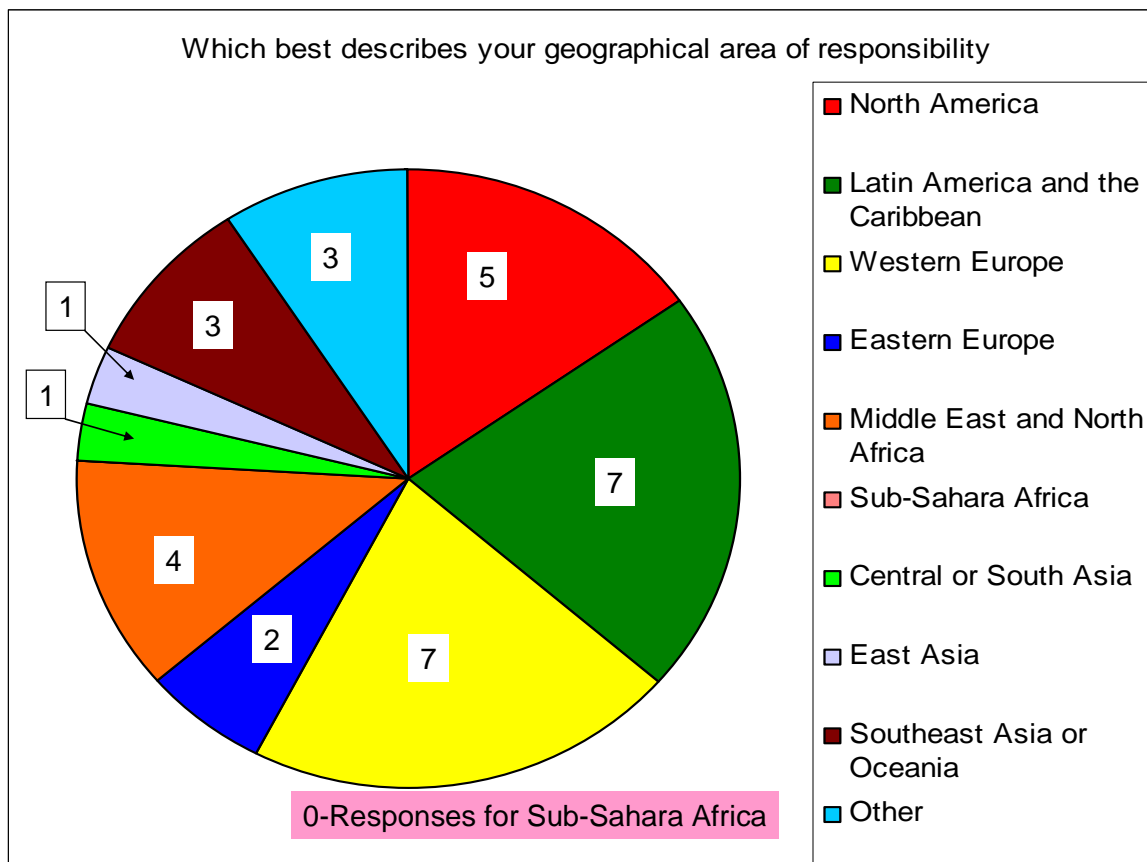
When a value between one and five is assigned to each category, with one as the value for less than five years experience, and five as the value for more than 20 years experience, the mean score for the value of the responses is 3.76. As illustrated by the line graph below, this would put the average number of years of experience firmly between 10 to 15 and 15 to 20 years of experience. This shows that ICE attachés have a significant amount of

Average Number of Years of Experience of ICE Attachés

Less than 5 years	5 to 10 years	10 to 15 years	15 to 20 years	More than 20 years
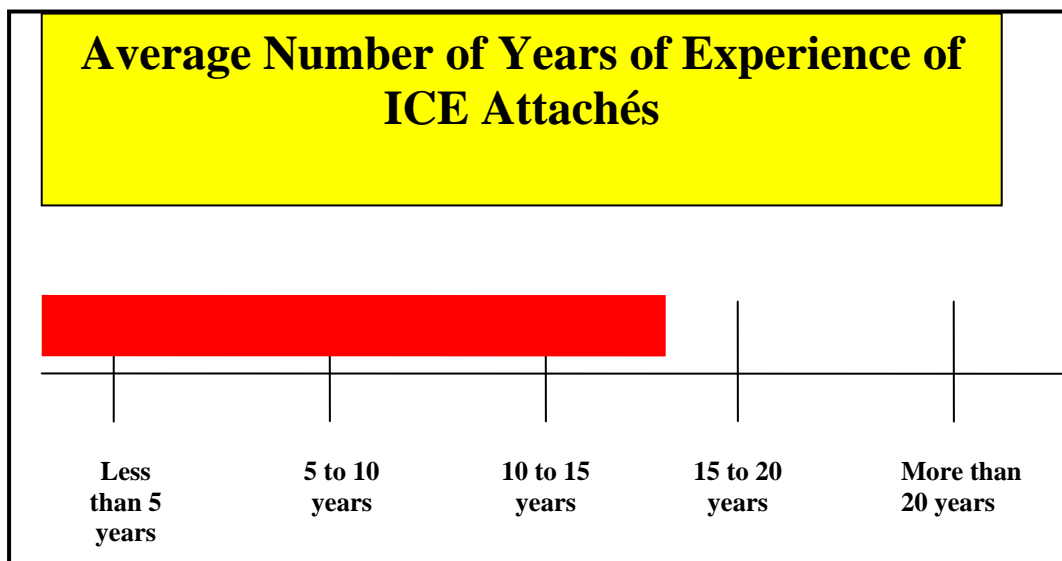
experience as immigration, intelligence and/or law enforcement officers.

As graphed below, answers collected from the questionnaire show that ICE attachés are dispersed around the world to a variety of regions.

Fourteen of the 31 respondents came from either Western Europe or Latin America and the Caribbean (seven each). There were multiple respondents for the remaining geographical areas, with the exceptions of East Asia and Central or South Asia, with one each, and no selections for Sub-Sahara Africa. Three respondents selected "Other," with one describing his area of responsibility as "West Africa." The other two respondents who selected "Other" did not clarify their answer. When asked to select the category

Which best describes your geographical area of responsibility

Legend:
- North America
- Latin America and the Caribbean
- Western Europe
- Eastern Europe
- Middle East and North Africa
- Sub-Sahara Africa
- Central or South Asia
- East Asia
- Southeast Asia or Oceania
- Other

Values shown in chart: 5, 7, 7, 2, 4, 1, 1, 3, 3

0-Responses for Sub-Sahara Africa

that best describes the office location to which they report, the respondents

overwhelmingly selected "Consulate or Embassy of your country." Twenty-six of the 33

respondents selected this category to describe their office location. Of the remaining

seven respondents, two chose "Offices of your agency located in the country to which

you are assigned," two chose "Offices of a local agency of the country to which you are

assigned," and three chose "Other." One of the respondents who selected "Other"

described his office location as "U.S. Special Operations Command Headquarters, Tampa

FL," while the other two respondents who selected "Other" did not clarify their answers.

What this section shows is that ICE attachés are experienced as immigration,

intelligence, and/or law enforcement officers. They are primarily located at U.S

Embassies and Consulates abroad, and their area of responsibilities covers every

geographical location in the world. Given the characteristics that the questionnaire

revealed about ICE attachés, it appears that these officers would provide a strong

foundation for a global network aimed at preventing terrorist travel.

**How do ICE Attachés Work to Combat Terrorist Travel?**

In the second section of the questionnaire, the respondents described how, in their

official capacity of an ICE Attaché, they work to curtail, combat, or prevent criminals,

smuggled or trafficked people, terrorists, or other individuals from crossing international

borders in violations of the laws of any nation. The respondents were asked to what

extent they agreed with the following statements: "Curtailing, combating, or preventing

criminals; smuggled or trafficked people; terrorists; or other individuals crossing

international borders in violation of the laws of any nations-state is the primary job

responsibility as an immigration officer assigned overseas." As you can see from the

graph below, the overwhelming majority of the 28 respondents who answered this

question either strongly agreed or agreed with this statement. Twenty-three of the 28

respondents selected either "Strongly Agree" or "Agree," which comprises 82% of all

respondents. Only two of the respondents indicated that they disagreed with the

statement. Given these responses, it should not be surprising that when a rate scale is

applied, with "Strongly Agree" assigned the value of five, that the arithmetic mean for

this question is a rating 4.29. This indicates that the level of agreement to the statement

by the respondents is extremely high.
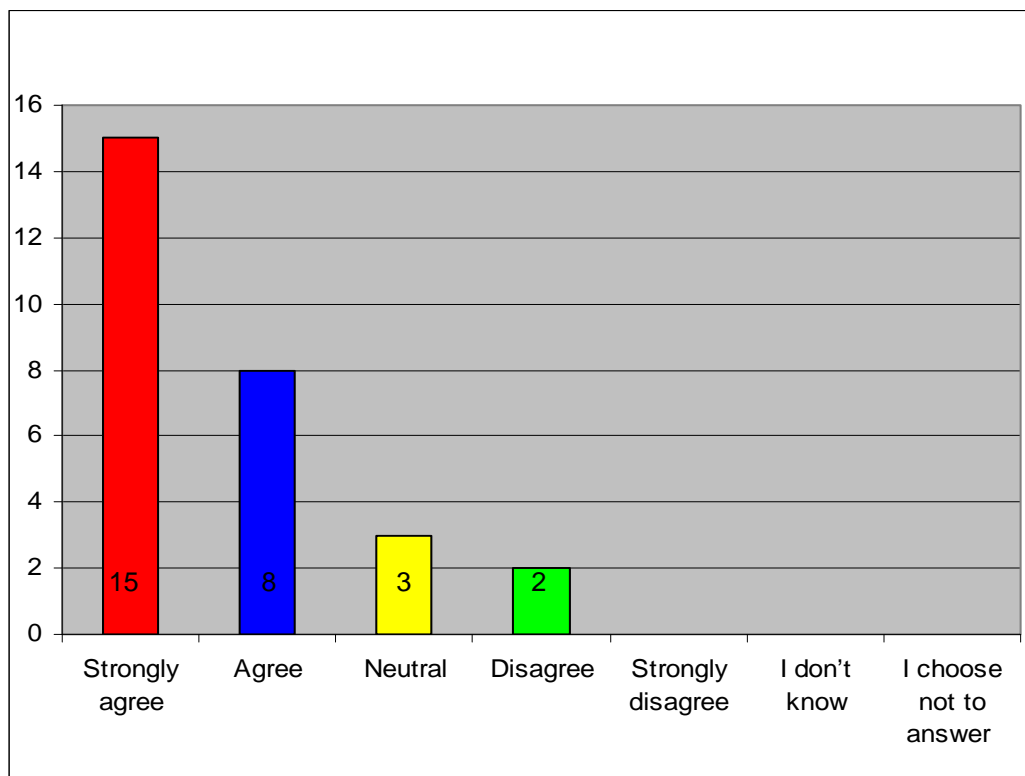
In Question 7, the respondents were asked to list their other job responsibilities as an Immigration Officer assigned overseas, besides: "Curtailing, combating, or preventing criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders in violation of the laws of any nations-state," which produced a number of different responsibilities. Many respondents list various crimes not directly related to curtailing, combating, or preventing criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders. These crimes included: money laundering, child pornography, counterfeit goods, narcotic smuggling, counterfeit pharmaceuticals and trade fraud. Other respondents simply answered enforcement of customs laws and regulations, which are violated when these listed crimes are committed.

These responses were not unexpected. As stated in Chapter Three, U.S. Immigration and Customs Enforcement was created from various components of the former U.S Customs Service and U.S. Immigration and Naturalization Service. Its primary mission is to protect United States national security by enforcing national customs and immigration laws. Given this mission, it seemed likely that when asked to report other job responsibilities as an Immigration Officer assigned overseas besides curtailing, combating, or preventing criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders, which is primarily an immigration-related matter, that the respondents would list responsibilities directly related to the enforcement of customs laws and regulations. It is interesting to note how the respondents rated their perception of how the customs responsibilities related to those immigration duties.

The respondents were asked to rate the level of agreement to the statement that "The job responsibilities listed in response to Question 7 are my primary job responsibilities as an Immigration Officer assigned overseas." As shown in the graph below, only 54% of the respondents strongly agreed or agreed with this statement. When a rate scale is applied, with "Strongly Agree" assigned the value of five, the arithmetic mean for this question is a rating 3.21. This is a full rating level lower than the responses provide for the responsibilities related to those duties besides curtailing, combating, or preventing criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders. In addition, three people chose not to answer the question; the reason for this response is not known.
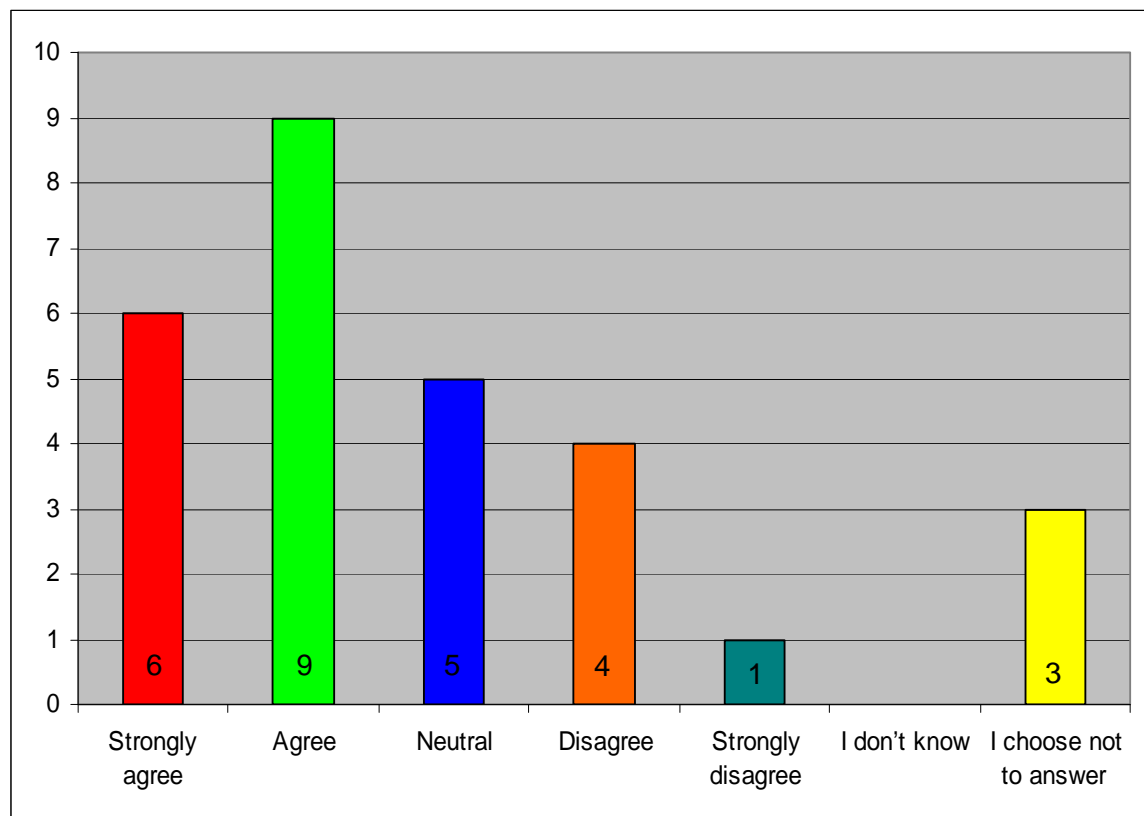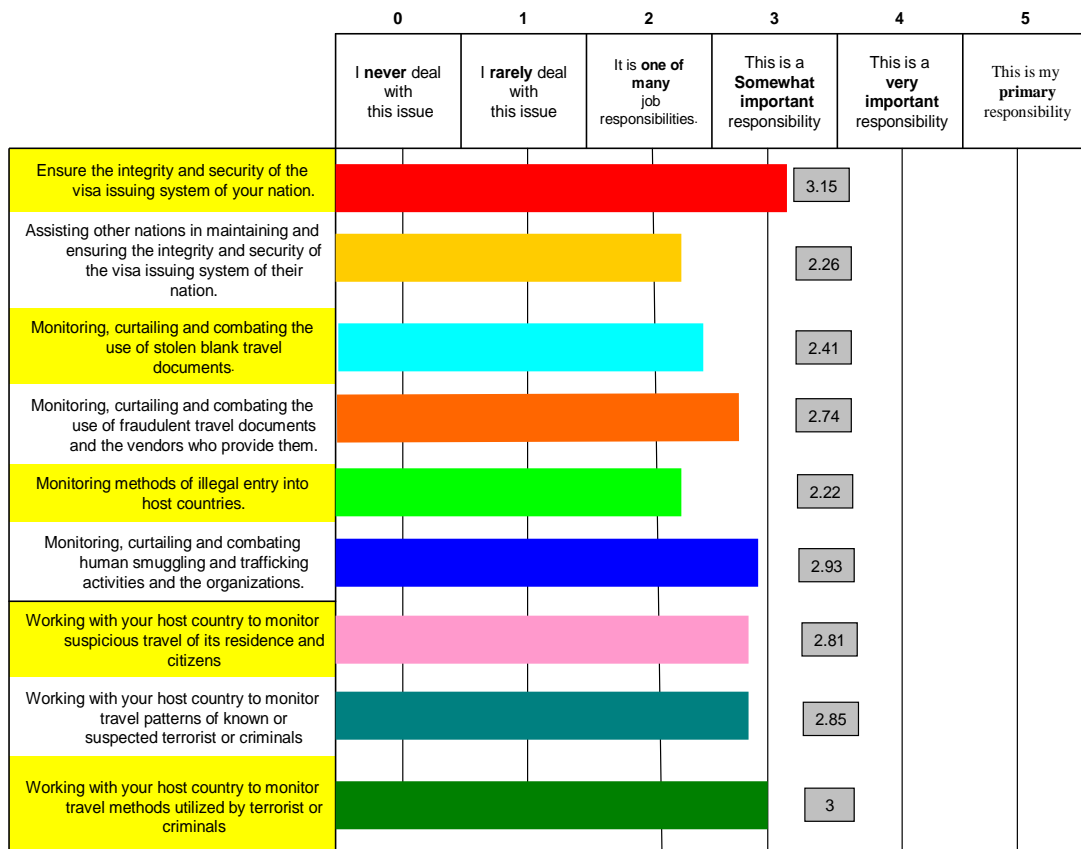
While both the job responsibilities related to immigration and customs matters will have an impact on an Attaché's ability to prevent terrorist travel, they are not carried out exclusively in order to prevent terrorist travel. When the respondents were asked how much time of their official duties are dedicated specifically to combating terrorist travel, they indicated relatively little time was dedicated to this mission. The must frequently selected response was "1-20%," and 68% of the respondents indicated that less than 40% of their time was dedicated to specifically combating terrorist travel. When an arithmetic mean is determined by assigning each possible response a value between zero and six, with zero as the value for "None," and six as the value for "This is my only responsibility," the calculated arithmetic mean for this question is 2.25. This would place the arithmetic mean slightly above 40%, even though

68% of the respondents indicated that they dedicated less than 40% of their time to combating terrorist travel. This reason for this skew is because the significant number of respondents, 22%, indicated they spent greater than 80% of their time dedicated to combating terrorist travel. There was only one respondent that chose the midpoint answer, while the other respondents answered by selecting rankings at either end of the spectrum. It cannot be determined why this disparity between responses exists; however, it does pose a question for further examination.
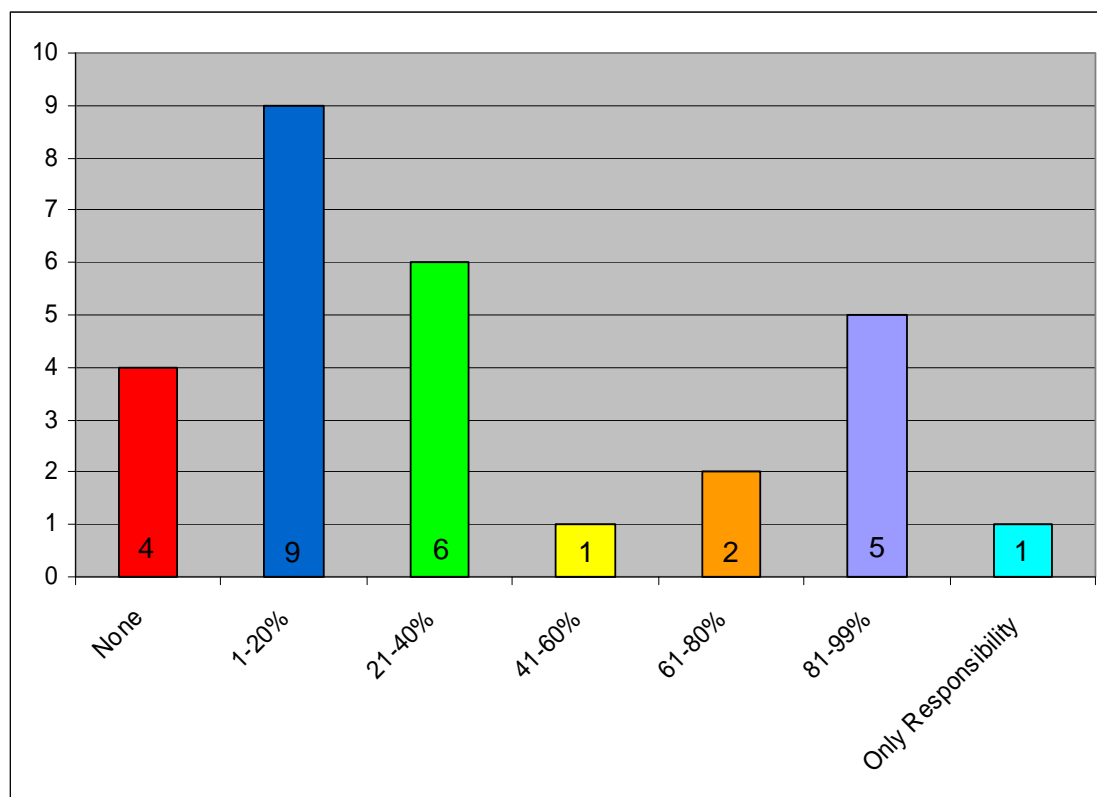
While the respondents differ greatly on the amount of time that they perceive they dedicate specifically to combating terrorist travel, they next rate their level of responsibility for dealing with issues specifically or directly related to, "curtailing, combating, or preventing criminals, smuggled or trafficked people, terrorists or other individuals from crossing international borders in violations of the laws of any nation."

The responsibilities listed in the question directly relate to the numerous entry methods

utilized by terrorist to cross international borders as described in great detail in Chapter

Three, and therefore terrorist travel. The respondents rated each item on a six-point scale,

ranging from, "This is my primary responsibility," to "I never deal with this issue," with

each possible response assigned a value between five and zero. To indicate the average

level of job responsibility the respondents had for each item, the arithmetic mean for the

responses for each item was calculated and then plotted on a bar graph.

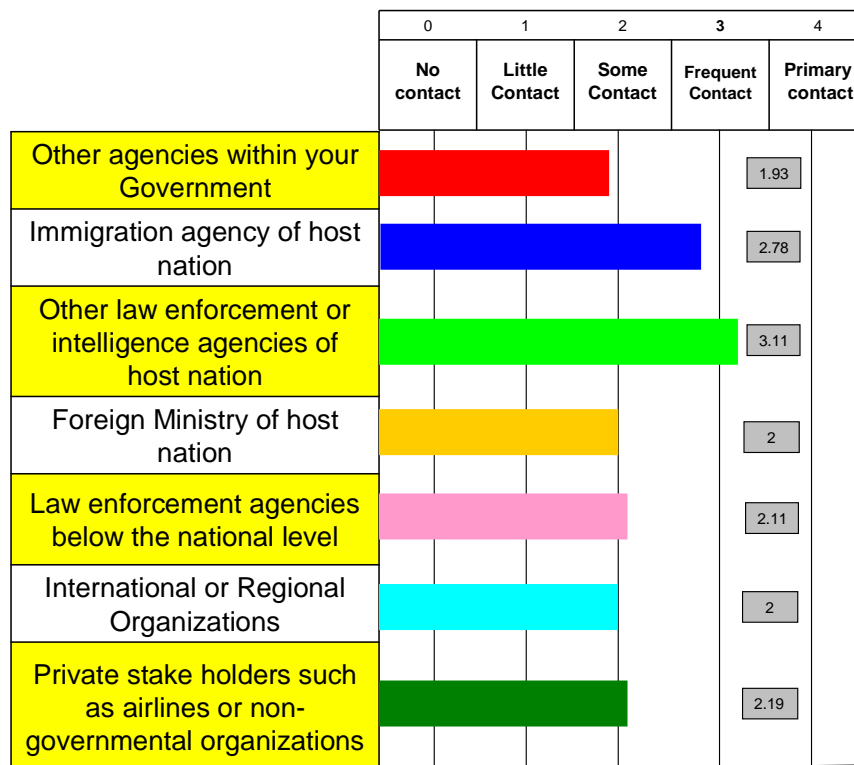|	0	1	2	3	4	5
	I **never** deal with this issue	I **rarely** deal with this issue	It is **one of many** job responsibilities.	This is a **Somewhat important** responsibility	This is a **very important** responsibility	This is my **primary** responsibility
Ensure the integrity and security of the visa issuing system of your nation.				3.15		
Assisting other nations in maintaining and ensuring the integrity and security of the visa issuing system of their nation.			2.26			
Monitoring, curtailing and combating the use of stolen blank travel documents.			2.41			
Monitoring, curtailing and combating the use of fraudulent travel documents and the vendors who provide them.			2.74			
Monitoring methods of illegal entry into host countries.			2.22			
Monitoring, curtailing and combating human smuggling and trafficking activities and the organizations.			2.93			
Working with your host country to monitor suspicious travel of its residence and citizens			2.81			
Working with your host country to monitor travel patterns of known or suspected terrorist or criminals			2.85			
Working with your host country to monitor travel methods utilized by terrorist or criminals			3			

As shown from the bar graph above, the respondent ranked each item with a

similar level of importance, in that the arithmetic mean for each item is ranked within one

point of each other, between 2.22 rating and a 3.15 rating. When plotted on a bar graph,

each item except for one falls firmly between "…one of many job responsibilities," and

"…somewhat important job responsibilities." The arithmetic mean for "Ensure the integrity of the visa issuing system of your nation," was rated slightly higher than somewhat important.

Another interesting aspect of the respondents' answers to this question is that all these items, which are related to curtailing, combating, or preventing criminals, smuggled or trafficked people, terrorists or other individuals from crossing international borders and terrorist travel methods, all but one of the responsibilities' scores fell between "one of many responsibilities" and "a somewhat important responsibility". When asked earlier to what extent they agreed with the statement: "Curtailing, combating or preventing; criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders in violation of the laws of any nations-state is the primary job responsibility as an Immigration Officer assigned overseas," 82% of all respondents either strongly agreed with or agreed with the statement. When asked specifically about terrorist travel, 68% of the respondents indicated that less than 40% of their time was dedicated to specifically combating terrorist travel. The reason for disparity between these three questions is not known. However, one possible reason is that the respondents view these various items as part of a greater mission of curtailing, combating, or preventing criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders; a mission that is not limited to terrorists, but all clandestine transnational actors who attempt to cross international borders in violation of the laws of any nation-state.

Next, the respondents provided information on whom they interact with on a regular basis as part of a possible larger transnational network to prevent terrorist travel

by indicating the frequency of their interaction and contact with others who may be responsible for "curtailing, combating or preventing criminals, smuggled or trafficked people, terrorists or other individuals from crossing international borders in violations of the laws of any nation-state." The following graph presents the arithmetic mean rating for each item of the question, indicating the average level of contact. The rating is based on a four-point scale ranging from 'Primary Contact" with a rating of four points, to "No contact," with a rating of zero points. As shown in the graph, there is a wide range of disparity in the levels of contact with the various items listed in the question:

	0	1	2	3	4
	No contact	Little Contact	Some Contact	Frequent Contact	Primary contact
Other agencies within your Government				1.93	
Immigration agency of host nation				2.78	
Other law enforcement or intelligence agencies of host nation				3.11	
Foreign Ministry of host nation				2	
Law enforcement agencies below the national level				2.11	
International or Regional Organizations				2	
Private stake holders such as airlines or non-governmental organizations				2.19	

While the arithmetic mean for each item on the list indicated that the respondents has some contact with each item in the question, it was the immigration agencies and other law enforcement and intelligence agencies of the host nation that received the highest rating. "Immigration agencies of host nation" received a rating of 2.78, while

"Other law enforcement and intelligence agencies of host nation" received a score of 3.11, meaning the respondents had frequent contact with these two categories. Interestingly, it was other agencies within the respondents' own government that received the lowest rating, with a mean score of 1.93. This shows that the respondents have significantly greater contact with foreign agencies then with other agencies within their own government. One respondent selected "Some contact" with "Other," indicating a category not included in the question, but did not provide a description for "Other" in the space provided.

In the next question, the respondents described the type of contact that they have with the items above. This question is of particular importance, in that it is the first in which the respondents' answers will be used to test this project's hypothesis. At first glance, it appears that the respondents indicated that their interaction with others who are responsible for "curtailing, combating, or preventing criminals, smuggled or trafficked people, terrorists or other individuals from crossing international borders in violations of the laws of any nation," overwhelmingly occurs in the form of official in-person meetings, briefings, or conferences. The average number of responses per item for this type of interaction was 10.14, almost twice as many as another category. When the two categories of unofficial interaction, electronic communication and unofficial in person meetings, are viewed together however, the average number of responses for these two types of interaction totals 10.85, which is a slightly higher average than official interaction. When the totals from the two types of interaction that occur most frequently are isolated, immigration agencies, and other law enforcement and intelligence agencies of the host nation, the scores for unofficial interaction are higher than the rate of all the

categories. The total number of responses for unofficial interaction with officers of the

immigration agency of the host nation was 14, versus 11 respondents who indicated that

official meetings were the most common type of interaction. When the same number was

isolated for other law enforcement and intelligence agencies of the host nation, it showed

that the respondents indicated unofficial interaction was the most common type of
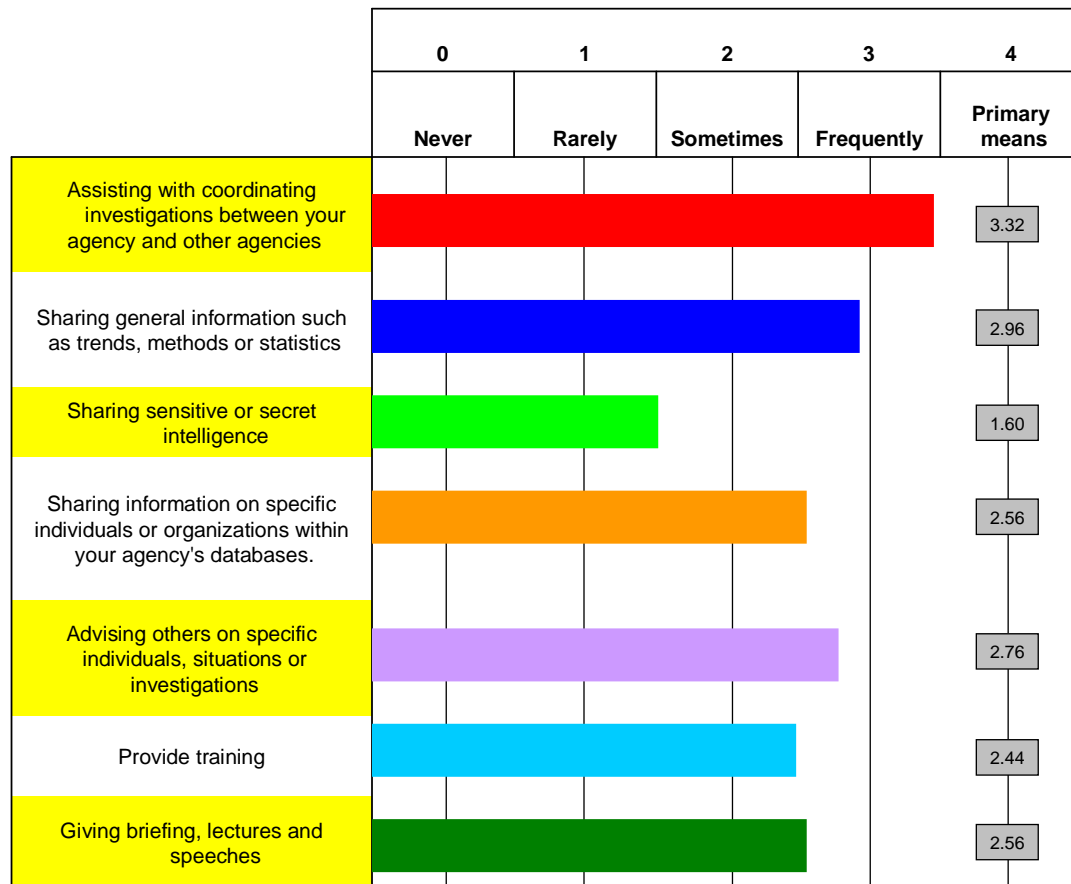
interaction 12 times, as opposed to 10 times for official interaction.

	Through regular electronic communication such as telephone fax or e-mails	Dissemination of intelligence reports, trend analysis or bulletins	Through secure communication methods such as secure phone and fax lines, or telex	Unofficial in person meetings, briefings or conferences or at social situations such as receptions or dinners	Official in person meetings, briefings or conferences	No Contact
Other agencies within your Government	11	3	1	4	7	0
Immigration agency of host nation	8	3	0	5	9	1
Other law enforcement or intelligence agencies of host nation	8	2	1	4	10	1
Foreign Ministry of host nation	3	3	1	2	13	4
Law enforcement agencies below the national level	5	1	0	7	9	4
International or Regional Organizations	2	2	1	5	12	4
Private stake holders such as airlines or non-governmental organizations	3	0	1	9	11	12
Average Number of responses per Item	5.71	2	0.71	5.14	10.14	3.71

In addition to the items listed in the question, several respondents indicated that

they frequently interact with their counterparts from a third country (British counterparts,

Canadian counterparts, etc.) that is located in or covering the same country in their area

of responsibility, via electronic communication. These numbers seem to indicate that the

respondents interact with individuals who may be part of a possible larger, transnational network to combat terrorist travel unofficially more frequently than officially.
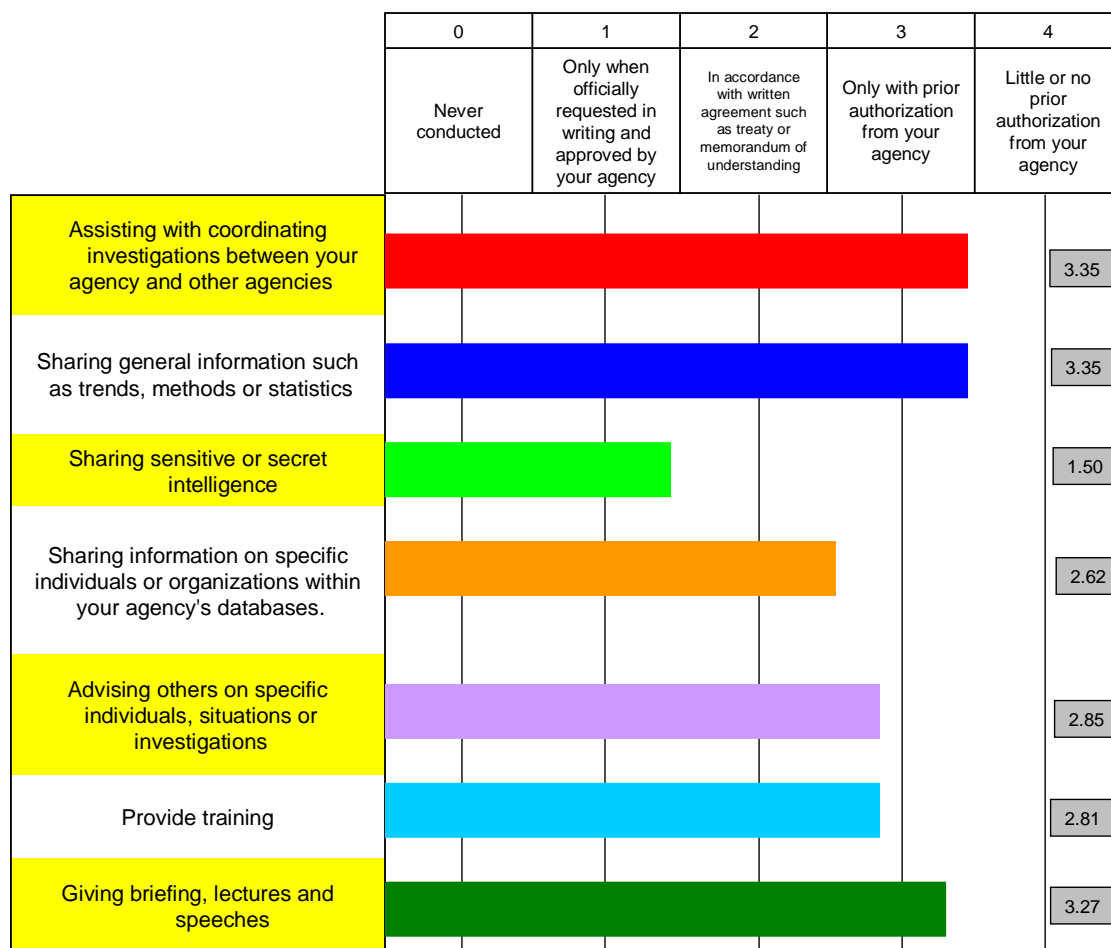
In the next question the respondents describe specific activities undertaken in the process of "curtailing, combating, or preventing criminals, smuggled or trafficked people, terrorists, and other individuals from crossing international borders in violations of the laws of any nation-state." This is the second question in which the respondents' answers will be used to test this project's hypothesis.

As the graph below indicates, all the activities carried out by the respondents but two received a ranking which fell between two and three. Two responses fell outside this range: investigation coordination, which received the highest score of 3.32, and the sharing of sensitive or secret intelligence, which received the lowest score of 1.60, and both could be considered more formal activities than just simple information sharing. While general information sharing received the second highest ranking, with a score of 2.96, it cannot be concluded from the data that information sharing occurs more frequently than more formal methods. The other possible methods of interaction addressed within the question, consisting of both formal interaction, such as providing training, and informal methods, such as sharing database information, receive a ranking score within .32 points of each other. This seems to indicate that the respondents utilize both formal and informal methods of interaction in order to aid in the curtailing, combating, or preventing criminals, smuggled or trafficked people, terrorists, and other individuals from crossing international borders at near equal rates.

	0	1	2	3	4
	Never	Rarely	Sometimes	Frequently	Primary means
Assisting with coordinating investigations between your agency and other agencies					3.32
Sharing general information such as trends, methods or statistics					2.96
Sharing sensitive or secret intelligence					1.60
Sharing information on specific individuals or organizations within your agency's databases.					2.56
Advising others on specific individuals, situations or investigations					2.76
Provide training					2.44
Giving briefing, lectures and speeches					2.56

Next, the respondents provided information on the level of authorization from

their agency that is needed to conduct the specific activities addressed in the previous

question. This is one of the most important questions, relating testing of the hypothesis

of this research project and the strongest indicator of the ICE Attaché network's ability to

act as an effective transgovernmental network to prevent terrorist travel. The literature

about transnational advocacy networks and transgovernmental networks suggests that the

key characteristics they both possess that leads to their effectiveness in dealing with

global problems is that they are light on their feet, and able to share information and carry

out other activities with their international partners with little or no centralized control.

Given these features of effective global networks, if a network of ICE attachés is part of

an effective transgovernmental network, the network's nodes should be able to carry out its normal activities and interact with other nodes within the network with little or no interference from a central control. This means that the individual attachés should be able to interact with their international partners with little or no prior authorization.

	0	1	2	3	4
	Never conducted	Only when officially requested in writing and approved by your agency	In accordance with written agreement such as treaty or memorandum of understanding	Only with prior authorization from your agency	Little or no prior authorization from your agency
Assisting with coordinating investigations between your agency and other agencies					3.35
Sharing general information such as trends, methods or statistics					3.35
Sharing sensitive or secret intelligence					1.50
Sharing information on specific individuals or organizations within your agency's databases.					2.62
Advising others on specific individuals, situations or investigations					2.85
Provide training					2.81
Giving briefing, lectures and speeches					3.27

The graph above indicates that the level of authorization required varies depending upon the type of interaction. Interestingly, with the exception of "Giving briefings, lectures and speeches," this chart appears almost identical to the previous chart depicting the frequency of interaction. This seems to indicate that the more frequently an action occurs, the less authorization is needed for the action to occur. For example, sharing sensitive or secret information ranked the lowest on both graphs, while

coordinating investigations and general information sharing were ranked the highest on both charts.   In fact, the ranking score for general information sharing was identical to that of investigation coordination as far as the level of authorization (3.35 out of 4). This suggests that relatively little prior authorization is needed for general information sharing, and that the respondents are part of a network that shares this characteristic with transgovernmental networks and transnational advocacy networks, even though the combined average score for all types of interaction is significantly lower (2.82 out of 4). This argument is strengthened when one looks past the mean ranking scores.

When the total numbers of responses for each level of authorization are calculated, regardless of the type of interactions, the choice most often selected by the respondents was little or no authorization (66 times). As the graph below shows, the respondents chose one of the lower two ranked choices on relatively few occasions (23 times total). While "Little or no prior authorization…" was selected the most often, the average mean ranking was brought down lower by the number respondents who selected the next two lower ranked categories. This makes it appear that on most occasions some level of prior authorization is need prior to the respondents' interaction with their foreign partners; thus, they are not behaving in a way consistent with the idea that transgovernmental networks are light on their feet and can share information and act quickly with little prior authorization. This may not be the case.
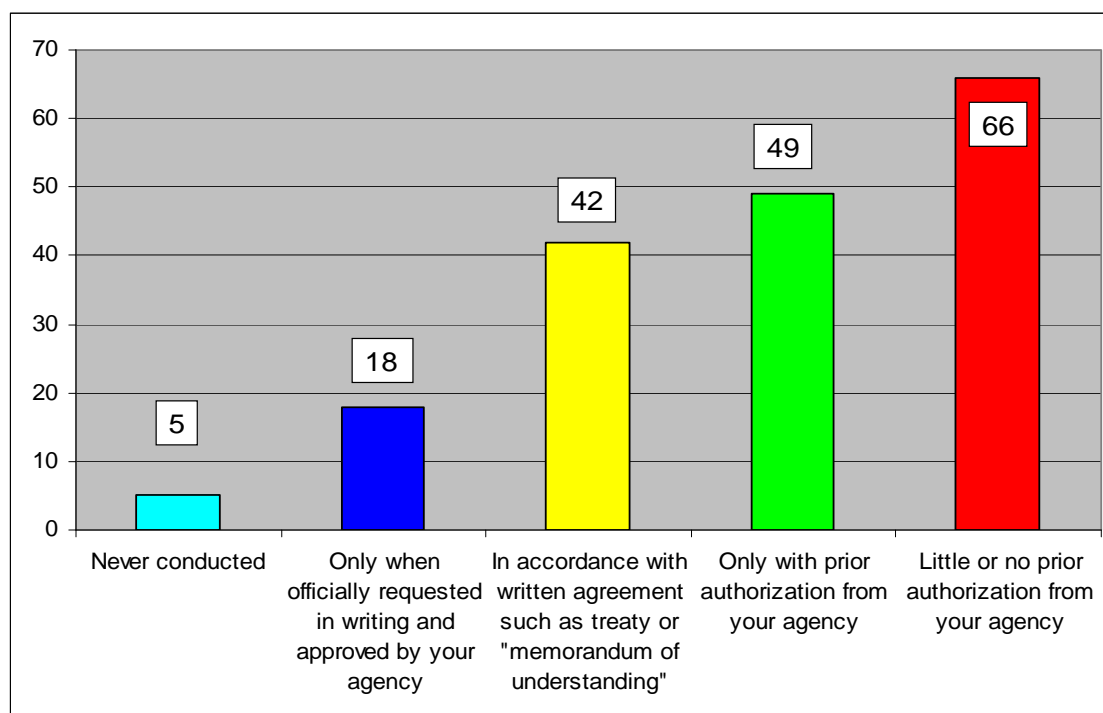
The fact the respondents selected, "In accordance with written agreement such as treaty or 'memorandum of understanding,'" on 42 occasions is a strong indication that the respondents are acting in a way consistent with transgovernmental networks. As discussed in Chapter Two, "memorandums of understanding" and similar agreements are actual an important component or many transgovernmental networks. These types of agreements, and even less formal initiatives, allow networks to respond to needs and coordinate activities quickly, as opposed to the lethargic pace of traditional treaties, and do not require the time consuming process of legislative approval to act. "The Statement of Mutual Understanding of Information Sharing," between the United States and Canada is one such agreement, and goes beyond simple information sharing with the other officers within its jurisdiction. A similar agreement between the United States and Canada in the months following September 11, 2001, the 30 Point Smart Border Action

Plan, identified the strategy of deploying "…immigration officers overseas to deal with document fraud, liaison with airlines and local authorities, and work with other countries to interrupt the flow of illegal migrants to North America," in order to improve border security (DHS 2002).

Using a ranking scale as an attempt to measure the level of authorization needed to interact with the respondents' foreign partners appears to be an error on the part of the researcher. The choice "…written agreement such as treaty or 'memorandum of understanding'" was only assigned a value of two; however, the literature suggests that they are a very important characteristic of transgovernmental networks. That the respondents selected "…written agreement such as treaty or 'memorandum of understanding'," or "Little or no prior authorization from your agency," indicates that the respondents do act in a way consistent with the idea that they are part of a transgovernmental network that is light on its feet and can share information and coordinate their activities quickly. This argument is strengthened when one considers the possibility that some the respondents interpreted "Only with prior authorization from your agency," as through informal agreements or less formal initiatives, as outlined in the literature of the subject. However, there is no way to know if the respondents did interpret these choices in that manner.

The final question of the second section was open-ended, which allowed the respondents to fill in the blanks of the questionnaire and provide additional data they felt were important to this section. They were asked to indicate "any activities, methods and responsibilities as an officer assigned overseas that were not already covered in this section." Many of the respondents took the opportunity to provide additional

information, though the information they provided was also given in earlier questions which provided the respondents an opportunity to provide additional information and clarification of answers.

What Should be Done: How ICE Attachés should Work to Combat Terrorist Travel

While the previous section asked the respondents how they acted in the official capacity to combat terrorist travel, the third and final section of the questionnaire asked their opinions on how they are being utilized to combat terrorist travel and what steps could and should be taken for them to be more successful in these areas. In the first question of this section, the respondents provide their opinion on the amount of time that should be dedicated to "Curtailing, combating, or preventing criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders in violation of the laws of any nations-state." As the graph below indicates, all the respondents but one felt that they are either dedicating sufficient time to these activities, or that more time should be dedicated. The one who did not respond did not feel that less time should be dedicated to these activities; rather, he chose not to answer. When calculated, the arithmetic mean found that the average rating of the respondents' view as to how much time should be dedicated to these activities is 2.96. If plotted on a line graph, the average rating would fall almost exactly on the point indicating that more time should be dedicated to these issues.
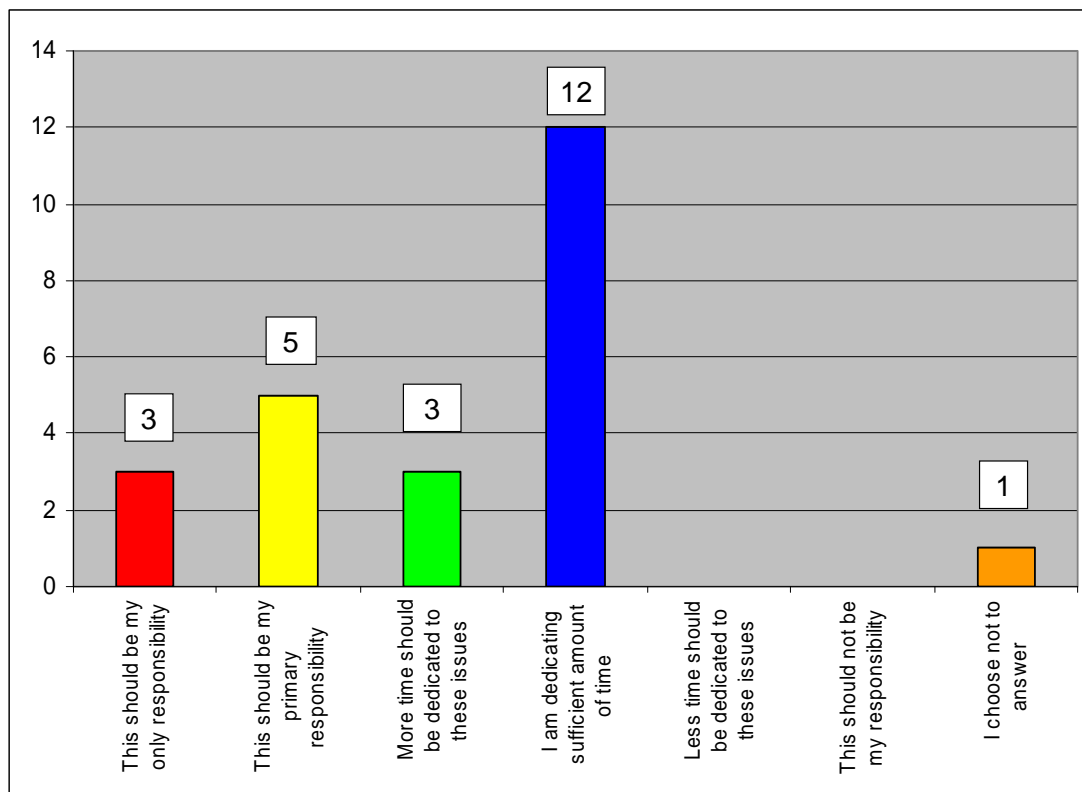
As the next chart illustrates, when asked about the amount of time that should be dedicated to responsibilities other than those related to "Curtailing, combating, or preventing criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders in violation of the laws of any nation-state," the most frequent answer given was that they were dedicating sufficient time to these activities. Unlike the previous question, this was not the answer given by the majority of the respondents. Also unlike the previous question, the respondents selected ratings on either side of the rating for dedicating sufficient time. As a result of this variety in responses, the calculated arithmetic mean gave an average rating score of 2.08, nearly a full point lower than the average rating score of the previous question. If plotted on a line graph, the average rating would fall almost exactly on the point indicating sufficient time is being dedicated to these activities, however, every respondent to the previous question

answered that either sufficient time is dedicated to, or more time should be dedicated to

"Curtailing, combating or preventing; criminals; smuggled or trafficked people; terrorists;

or other individuals crossing international borders in violation of the laws of any nation-

state."
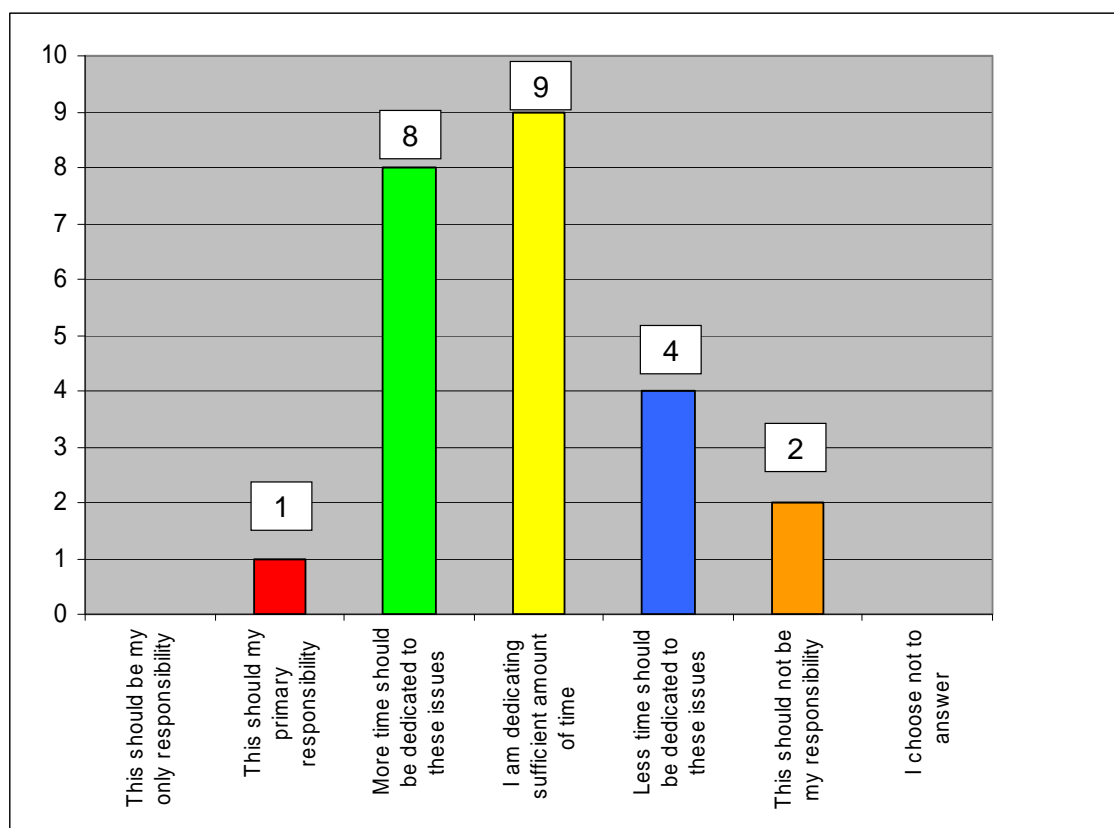
When the respondents were asked how much of their official duties should be dedicated

specifically to preventing terrorist travel, the most frequent answer given was 81-99%.

Nine of the 24 respondents (39%) felt that 81-99% of their duties should be dedicated

specifically to combating terrorist travel. What is interesting about these responses, is the

answers given by the respondents earlier in the questionnaire, when they were asked how

much of their duties were actually being dedicated to specifically to preventing terrorist

travel. Only 17% of the respondents indicated 81-99%. In fact, when asked how much

of their duties were actually dedicated specifically to preventing terrorist travel, only 29%

of the respondents indicated more than 60%, while 68% of the respondents indicated that

less than 40% of their duties were actually dedicated specifically to this mission. When

asked how much time should be dedicated to this mission, the respondents were split

right down the middle, with 42% indicating less than 40% of their duties, and 42%

selecting more than 60%. Four respondents selected 40-60%. These results suggest a

significant difference between the amounts of their duties that the respondents are

actually dedicating to combating terrorist travel.
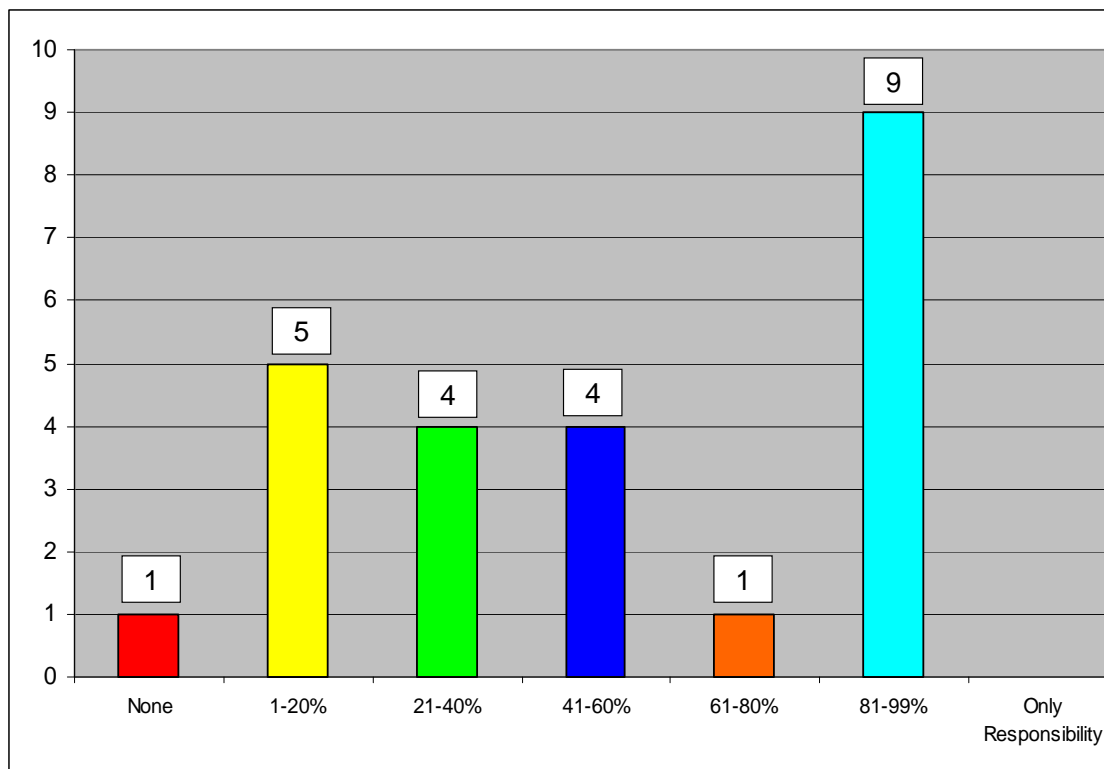
In the next question, the respondents used a Likert Scale to rate the importance of

various characteristics of the individuals with whom they deal as part of their regular

course of duties. This is the most important question of the third section of the

questionnaire, because it is the only one in this section that will be used in the hypothesis

testing. Based on the answers the respondents provided, it appears that the impression of a common identity based on profession, between the respondents and those they interact with in the course of their duties, is indeed important to the respondents. When the arithmetic mean is calculated for the level of importance of each characteristic to the respondents, those items related to profession and previous interaction received higher scores than those related to other characteristics, such as nationality. As the graph below illustrates, common identities related to professional identity, such as government employee, being an immigration officer, being a law enforcement or intelligence officer, and professional experience all received rating above three, meaning they ranked above "Somewhat important." Those related to other characteristics of individuals, such as citizenship, education level, and membership in professional organizations all received ratings below three, meaning they ranked below "Somewhat important." Education level, and membership in professional organizations actually rated closer to "Neutral" than "Somewhat important."

A similar pattern developed when the arithmetic mean was calculated for the respondents' rating of the level of importance of each item related to the manner of interaction between them and other individuals, as part of their regular duties. Type of interaction and frequency of interaction received ratings below three, meaning they ranked below "Somewhat important."   Quality of interaction, previous interaction, and profession relationship all received ratings above three, meaning they ranked above "Somewhat important." One item, "perceived 'trustworthiness,'" was rated 3.7 from the respondents, meaning this item actually rated closer to "Extremely important" than "Somewhat important."

	0	1	2	3	4	
	Not at all Important	Not Very Important	Neutral	Somewhat Important	Extremely Important	
The citizenship of the individual						2.85
The individual is a government employee						3.2
The individual is a government employee of your nation						3.3
The individual is a government employee of any nation.						2.95
The individual is an employee is an employee of your agency						3.35
The individual is an immigration officer						3.2
The individual is a law enforcement or intelligence officer						3.4
Education level						2.45
Professional experience						3
Membership in professional organizations						2
Previous interaction						3.1
Type of interaction						2.8
Frequency of interaction						2.95
Previous professional relationship						3.15
Perceived "trustworthiness"						3.7
Frequency and quality of previous assistance given						3.35

Given the literature on transgovernmental networks and transnational advocacy networks, these results should be expected if ICE attachés are part of a transgovernmental network to prevent terrorist travel. Valuable exchanges of ideas, techniques, and experiences result in a sort of collective memory, bonds, and identity over time (Keohane and Nye 1974 and Slaughter 2004). The conditions governing their behavior are the joint experience of collaboration, and the shared knowledge, trust, and reciprocal environment in which the various networks operate (Hajer and Versteeg 2005: 342). These conditions would explain why "Frequency and quality of previous assistance given," and "Perceived 'trustworthiness'," received the highest rating from the respondents of any of the items in the question.

In the next two questions, the respondents provided information on other resources or factors that assist in their ability to "Curtail, combat, or prevent criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders in violation of the laws of any nation-state," and they were asked to describe situations, working environment, or other factors that make it more difficult and impede or prevent their ability to achieve these missions. Of those respondents who provided other resources to assist them in their missions, the most common suggestions given were greater information and intelligence sharing from both the host country and other agencies within their own government. The areas in which the respondents were seeking additional information from host nations were: intelligence of known smuggling routes, including human, narcotic and weapons, identified patterns and trends, and access to airline passenger name records. The respondents also indicated that additional information and intelligence from their own government would be beneficial. Several respondents expressed particular frustration with the Department of State in obtaining passports and visa applications for review.

In response to the question of factors that make it more difficult impede or prevent their ability to achieve these missions, the overwhelming complaint from the respondents was that too much time was being dedicated to administrative functions and cutting through red tape. The respondents felt these tasks took significant time away from their law enforcement function. Other recurring themes from the respondents were difficulty with the host governments because of significant cultural differences, immigration viewed as an administrative not law enforcement function, and lack of entry and exit controls. Two other issues that were mentioned by more than one respondent

was infighting with other U.S. law enforcement agencies over territory or turf, and immigration issues not viewed a priority by ICE leadership.

When the respondents were asked to rate their current work environment, the most common rating given, 45% of all respondents who answered the question, rated their currents working environment as "very good." In fact, 60% of all the responses rated the current working environments either "excellent" of "very good". Of the remain 40% of respondents who answered the question, 20% gave their current working environment a rating of "good," while 20% gave a rating of "poor" or "very poor." Not a single respondent gave a rating of "neutral."

Given the high rating the "current working environment" received from the respondents, it is not surprising that few responded when asked how their work environment could be improved. Of those who did respond, the recurring theme was inadequate office space and resources. The responses regarding resources seem to be directed at inadequate access to certain computer systems, and again the Department of State was criticized for withholding information and resources. Several respondents also criticized the individuals they worked with on a regular basis from their own agency. They seem to suggest that those individuals were not qualified for the positions they held. The suggested that managers need to carefully select the individuals assigned overseas based on experience, job skills, and personality, and that personality has particular importance, as not only does the office environment suffer, but the image of the agency suffers as well.

When the respondents were asked to rate their current overall job satisfaction, the most frequent responses were "Very satisfied" or "Satisfied," with each rating selected by

the respondents 37% of the time. In fact, 79% of all the respondents rated their job

somewhat satisfied or better. Only 21% of the respondents stated they were dissatisfied

or very dissatisfied with their current job. Given these results, it is not surprising that few

respondents provided information on how their job satisfaction could be improved. Of

those that did respond, their answers focused again on the amount of time dedicated to

administrative responsibilities and frustration related to infighting with other U.S. law

enforcement agencies over territory or turf, especially in issues related to terrorism and

national security.

In the final question, the respondents provided any additional information

regarding their position or any other issues they felt were missed in the study.

Surprisingly, the responses to this open-ended question were similar in nature. The

respondents wanted it known to this author that their position's primary duty was not to

prevent terrorist travel, nor was it to "Curtail, combat or prevent criminals; smuggled or

trafficked people; terrorists; or other individuals crossing international borders in

violation of the laws of any nation-state." The respondents stated that they were involved

in a wide variety of issues related to both traditional immigration and customs matters.

These issues and crimes include: human smuggling and trafficking, child exploitation,

drug smuggling, money laundering/financial crimes, extraditions, violation of intellectual

property rights and cyber crimes.

Summary of Results

What the data revealed are that ICE attachés, with an average of 10 to 15 years of

law enforcement experience, are stationed around the world giving U.S. Immigration and

Customs Enforcement a global reach. According the respondents, ICE attachés dedicate

only a small portion of their official duties specifically to combating terrorist travel, with

68% of respondents indicating they dedicate less than 40% of their duties to this mission.

When it came to those issues closely related to combating terrorist travel, particularly :

"Curtailing, combating or preventing; criminals; smuggled or trafficked people; terrorists;

or other individuals crossing international borders in violation of the laws of any nation-

state," 82 % either "agreed" or "strongly agreed" that this was a primary function of their

position. The data provided by respondents showed that these were far from their only

duties.

When asked the level of agreement with the statement that job responsibilities

besides those job responsibilities related to: "Curtailing, combating or preventing;

criminals; smuggled or trafficked people; terrorists; or other individuals crossing

international borders in violation of the laws of any nations-state," 54% of the

respondents either "strongly agreed" or "agreed" with this statement. When asked to

describe these duties, the respondent listed preventing a wide variety of violations and

crimes including: money laundering, child pornography, counterfeit goods, narcotic

smuggling, counterfeit pharmaceuticals, and trade fraud. These are primarily customs

related crimes, and it should come as no surprise that were listed as other duties, given

the mission of U.S Immigration & Customs Enforcement.

Not surprisingly, when the respondents were asked with whom they had the most

interaction in order to "Curtailing, combating or preventing; criminals; smuggled or

trafficked people; terrorists; or other individuals crossing international borders in

violation of the laws of any nations-state," the highest-rated responses were received by

law enforcement or intelligence officers of the host nation, and the immigration agency of

the host nation. Perhaps more importantly, several respondents also indicated that they

frequently interact with their counterparts from third country located in or covering the

same country in their area of responsibility. What makes this information so important is

that it suggests that ICE attachés work not only with their foreign counterparts from the

host country, but also with individuals from other countries who are serving in similar

positions. This contact gives the ICE attachés access to even more resources and expands

a possible global network outward even further. The most common types of contact

between ICE attachés and those they interact with on a regular basis occur in the form of

official meetings, unofficial, less formal meetings, such as professional social gatherings,

and through normal electronic communications.

The respondents indicated that most frequently the activities they undertake in

order to better "Curtail, combat or prevent criminals; smuggled or trafficked people;

terrorists; or other individuals crossing international borders in violation of the laws of

any nations-state," were assisting with coordinating investigations, and sharing general

information, such as trends, methods or statistics. These two items also received the

highest rating from the respondents for the least amount or prior authorization needed to

carry out these activities. However, it is important to note that throughout the

questionnaire, when given the opportunity to provide additional information through

open-ended questions, the respondents stressed the importance of information sharing as

well as their frustration with obtaining information and intelligence from other agencies

within their own government.

The questionnaire not only collected valuable data into how respondents work to

prevent terrorist travel, but their opinion as to how much time should be dedicated to this

mission, the importance of various characteristics of individuals they deal with as a part of their regular duty and their interaction with those individuals, and what they perceive hampers their ability to prevent terrorist travel. All the respondents felt that either sufficient time or more time should be dedicated to "Curtailing, combating or preventing; criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders in violation of the laws of any nation-state." The majority of the respondents, 63%, felt less time should be dedicated to other activities not related to this mission. When asked specifically about preventing terrorist travel, the respondents indicated that more time should be dedicated to the combating this problem. Of the respondents, 38% indicated that over 80% of their time should be dedicated specifically to preventing terrorist travel, while previously in the questionnaire only 21 % indicated this amount of time was dedicated specifically to this area.

When the respondents were asked about the importance of various characteristics of individuals they deal with as a part of their regular duty and their interaction with those individuals, it was clear that perceived common identity and quality of previous interactions were important. Those items related to common professional identity received the highest ratings as to the importance to the respondents. Likewise, significantly higher ratings were given to the existence of previous relationships, such as the quality of previous interaction by the respondents. Perceived "trustworthiness" was the overwhelmingly the most important characteristic to the respondents when interacting with others to accomplish their mission.

While the respondents overwhelmingly were satisfied with the work environment and their level of job satisfaction, they did point to several issues that had an effect on

their ability to accomplish their missions. The most common complaint among the respondents was the amount of time being spent on administrative work, which they felt took significant time away from their primary missions. The respondents also stated there was need for greater information sharing and access to intelligence. The experience concern over the accessibility to information they perceived necessary to their job. Ironically, this complaint was not aimed toward their foreign partners but towards other agencies within their own government. They also complained that infighting often occurred with these same agencies over turf or territory during investigations or other operations, especially in areas related to terrorism or national security.

What the data obtained from the respondents suggests are that the ICE attachés serve as a foundation for a transgovernmental network that works not just to prevent terrorist travel, but to combat a variety of immigration and customs violations and crimes. These attachés interact with immigration, law enforcement, and intelligence officers not just from their host countries, but also from other nations, who hold similar positions and have a shared area of responsibility. Through these interactions, the network expands outward resulting in a coordination of activities and a sharing of information with officers from a variety of nations with greater ease than they often experience with other agencies within their own nation's government.

This network appears to share many of the characteristics that appear in the literature on transgovernmental networks and transnational advocacy networks; however, a key question in determining whether this network is a transgovernmental network is if it behaves in the way the literature suggests it should. Making this determination will require the hypothesis to be tested. The results of this test are important because if the

expected results are achieved, not only will they indicate how this transgovernmental

networks behaves, but will also provide insight into how, using the model of

transnational advocacy networks, this network can operate more effectively in achieving

its missions. This will be the focus of the following chapter.

CHAPTER SIX: DATA ANALYSIS

The goal of this research was to explore how immigration officers assigned overseas attempt to prevent terrorist travel. In order to accomplish this goal, his research used a questionnaire to determine how officers from U.S. Immigration and Customs Enforcement specifically operate within foreign jurisdictions to prevent terrorists from crossing borders to support, finance, and carry out operations. The data collected from these questionnaires have clearly provided a better understanding of how ICE attachés work to accomplish this mission. The existing literature on transgovernmental networks and transnational advocacy networks (TANs) suggests numerous similarities in the way TANs and transgovernmental networks operate to achieve their goals. These similarities seem to indicate that the anticipated answer to the research question will be that immigrations officers assigned to foreign jurisdictions operate and interact with one another in an attempt to prevent terrorist travel in much the same way that members of transnational advocacy networks interact and operate in order to address their target problem.

If ICE attachés are part of a transgovernmental network, they should operate in a similar way to TANs. If this is the case, when the ICE attachés interact with their foreign counterpart this interaction should be informal, consist primarily of information sharing, and occur with little interference from their agency's hierarchy. This interaction should be facilitated by a shared feeling of common identity based on profession rather than

nationality. Based on the data collected from the questionnaires, this appears to be the case.

Hypothesis Test

In Question 12, the respondents were asked to describe the means by which they interact with their foreign counterparts. If the hypothesis was correct, the frequency of electronic communication and unofficial meetings should be more frequent than other means of interaction. The average number of responses for each item listed in this question indicates that interaction occurs in the form of official in-person meetings, briefings or conference 10.14 times for each mode of interaction. This is higher than any other another category. However, when the two categories of unofficial interaction, electronic communication and unofficial in-person meetings, are viewed together, the average number of responses for these two types of interaction totals 10.85, which is a slightly higher average than official interaction. Perhaps more importantly, when the two totals from Question 11 regarding with whom the respondents interact with on a regular basis that occurred most frequently are isolated, immigration agencies, and other law enforcement and intelligence agencies of the host nation, the scores for unofficial interaction are even higher than the rate of all other categories. The total number of responses for unofficial interaction with officers of the host nation's immigration agency was 14, compared to the 11 respondents who indicated that official meetings were the most common type of interaction. When the same number was isolated for other law enforcement and intelligence agencies of the host nation, it shows that respondents indicated unofficial interaction was the most common type of interaction 12 times, compared to 10 times for official interaction. Therefore, the assumption of the hypothesis

that members of a transgovernmental network of immigration, law enforcement, and intelligence officers interact more frequently through informal means than formal means appears correct.

In Question 13, the respondents were asked to describe types of interaction with their foreign counterparts. If the hypothesis was correct, the ratings given by the respondents for information sharing should be higher than for formal interaction. The two types of interaction with the highest rating were assisting with coordinating investigations and sharing general information such as trends, methods, or statistics. Assisting with coordinating investigations received a higher rating than information sharing, which appears to be a more formal activity than simple information sharing. This would initially seem to indicate that this assumption of the hypothesis is incorrect. However, the literature on transgovernmental networks states that enforcement networks, such as those found among officers in law enforcement and intelligence agencies, go beyond the general exchange of information found in information networks to actionable intelligence (Slaughter 2004:55). Assisting with coordinating investigations would seem to fall into this category, and therefore the high ratings it received would be an indication that the behavior of ICE attachés in this area of hypothesis testing is consistent with the behavior found in transgovernmental networks.

In Question 14, the respondents were asked to describe the level of authorization to interact with their foreign counterparts. If the hypothesis was correct, the respondents should have indicated that they can interact with their foreign counterparts with little interference from the hierarchy of their agency. The data indicated that the more frequently a particular type of interaction occurred, the less authorization was needed for

the action to occur. Coordinating investigations and general information sharing, the two most common types of interaction, received identical scores for the level of authorization required (3.35 out of 4), indicating that these types of interactions occur with the least amount of prior authorizations. In addition, when the total numbers of responses for each level of authorization are calculated, regardless of the type of interactions, the choice most often selected by the respondents was little or no authorization (66 times).

The respondents also selected, "In accordance with written agreements such as treaty or 'memorandum of understanding,'" on 42 occasions. As discussed earlier, "memorandums of understanding" and similar agreements are an important component of many transgovernmental networks. There is also no way of knowing if some of the respondents who said that interaction can occur only with prior authorization from their agency were answering in regards to interaction on formal agreements or through less formal initiatives as outlined in the literature of the subject. All these facts seem to indicate that ICE attachés are part of a transgovernmental network that is light on its feet and can share information and coordinate its activities quickly, and that the behavior in this area of hypothesis testing is consistent with behavior found in transgovernmental networks.

The final assumption of the hypothesis to be tested is that the respondents share a common identity with those they interact with on a regular basis as part of their official duties, which is based on profession, quality of previous interaction, and trust. When dealing with these individuals, these factors are more important factors than nationality or other characteristics not directly related to their official duties. This shared identity helps facilitate more effective interaction between these partners who have the common goal of

preventing terrorist travel. To test this assumption, the data collected from the

respondents in Question 20 of the questionnaire were examined. When asked about the

importance of an individual's characteristics, the fact that the individual was an

immigration, law enforcement, or intelligence officer received higher ratings than those

related to nationality or other identifying characteristics. Significantly higher ratings were

given by the respondents to the existence of previous relationships and the quality of

previous interaction by the respondents. The highest ratings were given to perceived

"trustworthiness." These results show that profession, and frequency and quality of

previous interaction, are more important than nationality, education, or other

characteristics. Given these results, the final assumption of the hypothesis appears

correct: a common professional identity and the quality and frequency of previous

interactions are viewed as more important than other characteristics to members of a

transgovernmental network of immigration, law enforcement, and intelligence officers.

As stated in the previous chapters, if the hypothesis that immigration officers

assigned to foreign jurisdictions operate and interact with one another in an attempt to

prevent terrorist travel in much the same way that members of transnational advocacy

networks interact and operate in order to address their target problem is true, the four

assumptions of the hypothesis must be true. The respondents indicated that ICE attachés

interact with their foreign partners more frequently through informal means than formal

means. When examining the assumptions about type of interaction, the respondents

indicated that coordinating investigations and information sharing are the most common

types of interaction, and these activities require minimal prior authorization from their

agency or through information-sharing agreements such as "memorandums of

understanding." Finally, the perception the respondents have of other agents they interact with on a common basis is strengthened by sharing a common identity based on profession and by the frequency and quality of the interaction. Given these results, it appears that the hypothesis is correct.

The data collected from this questionnaire show that immigrations officers assigned to foreign jurisdictions, or at least ICE attachés, operate and interact with one another in an attempt to prevent terrorist travel in much the same way that members of transnational advocacy networks interact and operate in order to address their target problem. Given these results, and the other data collected from the respondents, it is concluded that ICE attachés are part of a transgovernmental network that works to combat not just terrorist travel but various other immigration and customs-related crimes and violations through the coordination of activities and the sharing of information and intelligence. This network is comprised not just of ICE attachés, and immigration, law enforcement, and intelligence officers of the host nation, but officers from other nations who hold similar positions and have a shared area of responsibility. This network expands outward and strengthens as interaction becomes more frequent and productive, and bonds of trust develop between the network members. The key to the success of this network is the ability of its members to freely exchange information and intelligence. By maximizing this ability, they can truly create a network to fight against terror.

Fighting "Networks of Terror with Networks against Terror"

As discussed in great detail in previous chapters, a strategy that has emerged to address the threat to global security presented by non-state actors is the idea of confronting networks of terror with networks against terror. This is a strategy that can be

used against criminal networks as well. The data collected from this questionnaire show that transgovernmental networks mirror terrorist and criminal network characteristics, networks of committed actors built on trust that allow primarily domestic actors to operate internationality and that are fluid in nature with the ability to adapt to changing circumstances and solve unforeseen obstacles in execution. The data also suggest that these networks also mirror one another in structure.

As described in Chapter One, the global Salafi jihad movement is made up of horizontal small world networks of nodes, links and hubs with an ability to adapt to changing circumstances and solve unforeseen obstacles in execution general plans. The movement maintains a vertical hierarchical network component in the form of al-Qaeda and its leadership which has reconstituted itself and found a new safe haven in the Northwest Frontier Provinces of Pakistan and other areas along its border with Afghanistan. This leadership exerts control and gives direction to the organization's horizontal network through hubs. The hubs are at the bottom of the vertical hierarchical network comprised of al-Qaeda's leadership; and also part of the organization's horizontal network. The leadership, through hubs transmits its desires to its various networks hubs overseas that finance, plan, and carry out the movement's agenda. This dual network design has allowed the global Salafi movement to maintain centralized vertical hierarchical organization while enjoying the benefits of the interconnectiveness of its horizontal network established following the September 11th attacks. The date collected from this research suggests that a global network of ICE attachés operate in much the same fashion. The leadership within ICE headquarters is a centralized vertical hierarchical network exerts control and direction to the horizontal

network through hubs. The hubs, individual attaché offices, are at the bottom of the vertical hierarchical network also part of a global horizontal network of law enforcement and intelligence officers. The hubs reach out to their foreign partners in the network, the nodes, to share information and coordinate investigations. Given the similarity in the structure of these two network types, a global ICE attaché network that combats terrorist travel appears to be an excellent model for the strategy of confronting networks of terror with networks against terror. A transgovernmental network of ICE attachés, however, has distinct advantages over the global Salafi jihad movement's network. The terror network cannot expand outward without opening itself up to increased security risks. A transgovernmental network to prevent terrorist travel can freely expand outward, and as it does so it acquires the knowledge and resources of the added network members. As exchanges with new network members become more frequent, greater levels of trust are built and the network becomes more robust. The ability of terrorist networks, such as those associated with the global Salafi jihad movement, to finance, plan, and carry out the movement's agenda is hampered by their need to operate clandestinely.

Transgovernmental networks do not face similar constraints. While the information exchanged within this network may be secret, its existence is not. In fact, transgovernmental networks are often the subject of press releases, such as those that publicize a new memorandum of understanding between two partners, in order to assure the citizenry of a nation that their government is taking steps to protect them. It is the transgovernmental network's ability to exchange information that is the key component to the network's success.

Information and Intelligence Sharing

Information binds network members together and is essential for network efficiency (Keck and Sikkink 1998: 18). This is true whether the network is a transnational advocacy network or a transgovernmental network. A transgovernmental network tasked with the mission of combating terrorist travel is no exception. France, Britain, Italy and Spain have a history of sharing intelligence on "radical Islamists" suspected of attending training camps (Rees 2006: 59). As those responsible for the 2005 and 2006 British terror plots have shown, monitoring the travel of individuals suspected of radicalization is important, even when these suspects are citizens of one's own country. The "far enemy" of the global Salafi jihad movement consists of other countries beyond these four and therefore this information needs to be shared with other international partners who are also targets of this movement. A transgovernmental network to combat terrorist travel may be just the way to share this type of information quickly and efficiently between members from like-minded countries.

Timely and accurate information and intelligence is a vital ingredient in fighting terrorism and, for it to be effective, it must be pooled (Rees 2006: 90). The ICE attachés who participated in the questionnaire confirmed the importance of intelligence and information sharing to achieving their mission. When the respondents were asked to rank specific activities undertaken in the process of "curtailing, combating, or preventing criminals, smuggled or trafficked people, terrorists, and other individuals from crossing international borders in violations of the laws of any nation-state," investigation coordination and general information sharing received the two highest scores. When they were later asked to indicate other resources that would assist them in their missions, the

most common suggestions given were greater information and intelligence sharing from both the host country and other agencies within their own government. Unfortunately, recognizing the importance and the need for information and intelligence sharing does not mean that greater sharing will occur.

There are many impediments to effective information and intelligence sharing. Valuable, actionable intelligence is difficult to obtain, making it a valuable commodity. Possession of this commodity gives power and prestige to the country or agency that holds it. The sensitive nature of the information makes it vulnerable to compromise as more people become aware of it. This means that it is shared with the greatest reluctance. When intelligence is shared, it is usually done so bilaterally and is not for dissemination to a wider audience (Rees 2006: 90-1). In their responses, ICE attachés echo the difficulties in obtaining valuable, actionable intelligence in order to accomplish their mission.

When asked what factors make it more difficult, impede or prevent their ability to achieve their missions, many respondents felt particular frustration with their access to additional information and intelligence from other agencies within their own government. More than one respondent felt this lack of cooperation was infighting with other agencies over territory or turf. Terrorism is a complex issue that crosses jurisdictions and combating it requires a variety of law enforcement and intelligence agencies. Terrorism has remained a high profile issue, so agencies hold onto their commodity of intelligence in hopes that they will be the ones to make the "big bust." Making the bust not only brings fame but also access to more resources. As a result of this environment, intelligence becomes increasingly valuable and important to an agency's ability to carry

out their mission. When intelligence is not accessible an agency must gather it itself. When it comes to gathering intelligence on terrorist travel, assets available to U.S. Immigration and Customs Enforcement puts the agency in a unique position to not only gather intelligence but also to put it to use. The global network of ICE attachés is an important component in the gathering, assessment and dissemination of this intelligence.

Information and Intelligence Gathering

Arbitrarily stopping a terrorist at a border will stop a terrorist from entering and operating within a country but will not necessarily stop a sophisticated plot. Mohamed al Kahtani, who is often referred to as the twentieth September 11 hijacker, was prevented from entering the United States on August 4, 2001. Even though Kahtani was successfully prevented from entering the United States, the September 11 attacks were still successfully carried out. Even if preventing a terrorist from entering a country also directly prevents an attack, the terrorist network he is a member of remains largely undisturbed (Sageman 2004: 140). In order for the prevention of a terrorist from crossing an international border to be fully beneficial, the individual must be identified as a terrorist, the means by which he was attempting to gain entry must be identified, and his arrest should lead to the identification of others in his network. Accomplishing these goals requires the gathering of intelligence at the time of the terrorist arrest.

Two of the recommendations of the 9/11 Commission were greater intelligence sharing between the United States and its allies and more resources invested in human intelligence sources. While a terrorist's failure to gain entry to a country may initially do little to disrupt his terrorist network, he is a valuable source of human intelligence on both the network that facilitated his travel and the larger terrorist network he belongs to.

Law enforcement officers have traditionally played the lead role in collecting and disseminating intelligence on transnational criminal activity. These officers are also responsible for finding, collecting, and delivering information and evidence to judicial authorities (Andreas and Nadelmann 2006: 60). The skill sets developed as a result of these duties make law enforcement officers uniquely qualified for exploiting human intelligence sources. As the primary law enforcement officers for investigating immigration violation of U.S. law, ICE officers appear to be the logical choice for collecting intelligence on terrorist travel.

U.S. Customs and Border Protection (CBP) is the agency tasked with screening individuals arriving at ports of entry and those individuals who attempt to cross into the United States between ports of entry. While CBP officers have a skill set that enables them to detect individuals attempting to enter the United States in violation of law, they lack specific training or experience in conducting long term criminal investigations or intelligence gathering, skills that translate better to intelligence collecting and analysis. ICE is also the agency tasked with detaining individuals who are refused entry into the United States. Collecting useable human intelligence often requires rapport with the source of intelligence that cannot be accomplished in a few hours at a port of entry. The detention of an individual while awaiting removal from a country provides a unique opportunity to collect intelligence from a human source. ICE already has in place a program to collect and disseminate intelligence obtained from human sources within its detention population. Finally, ICE attaché offices give the agency a global reach to both collect and disseminate intelligence and share information with their foreign partners.

A terrorist stopped from entering and operating within a country will not necessarily destroy the network he belongs to; he may, however, hold valuable information that can assist in accomplishing this mission. He may be a node who can provide a link to and help in identifying a network hub. It is these hubs where the network is vulnerable to attack. If enough hubs are destroyed, the network breaks down and the various nodes become isolated. Hubs are vulnerable because most communication goes through them. Through good police work and intelligence gathering, these hubs can be identified and arrested (Sageman 2004: 140-1). Because these hubs are scattered throughout the global and in a variety of jurisdictions, a transgovernmental information and intelligence sharing network is a necessary tool to accomplishing this mission.

ICE attachés and other members of a transgovernmental network that combats terrorist travel are somewhat unique in that they collect, analyze and disseminate intelligence. They collect data from their foreign partners and disseminate them to their own agency. They also collect data from their own agency and share the information with their foreign partners. When the data are collected, the attachés analyze the data to determine the meaning, importance, who will benefit from the information, and disseminate it accordingly. The ICE attachés have a particular characteristic that assists them in this process: their experience. The data collected by the questionnaire show that ICE attachés have an average of between 10 and 15 years of experience as immigration, intelligence, and/or law enforcement officers. The value of this experience cannot be overestimated.

When intelligence and information is collected, it is only beneficial if it ends up in the hands of those who need it most. Using the example above of a terrorist stopped at a border who then identifies a hub, the information obtained may have implications beyond combating terrorist travel, implications for areas beyond the jurisdiction of U.S. Immigration and Customs Enforcement. When this occurs, the information must not be held onto like a commodity, but rather disseminated by those who would benefit from it. Obviously, when information or intelligence is classified or secretive in nature, there are specific guidelines established for this information being shared and disseminated, especially with foreign partners. Where transgovernmental networks are beneficial is in the sharing of general information and intelligence in a quick and efficient manner to respond to specific situation. This environment of cooperation is stronger when a sense of trust exists within a transgovernmental network.

Building a Robust Network on a Foundation of Trust

The literature on transnational social movement organizations and networks describes how these organizations build on trust and cohesion in an attempt to serve as a structure for cooperation beyond political, social and cultural boundaries (Keck and Sikkink 1998, Falk 1999, Kaldor et al 2003). This idea of a network built on trust is also echoed in the literature on transgovernmental networks (Slaughter 2004, Hajer and Versteeg 2005, Pawlak 2007). The high importance of trust in governing interaction between network members was also reflected by the data collected from the ICE attachés. When they were asked to rate the importance of various characteristics of the individuals with whom they deal as part of their regular course of duties, "perceived trustworthiness" received a significantly higher score than any other characteristic.

Trust in networks is built on a foundation of a common professional identity and shared experiences. Trust strengthens as information is exchanged in a reciprocal environment, and grows outward to other members of the network. As a result, networks grow stronger over time. This phenomenon, however, provides certain challenges to transgovernmental networks comprised of officers assigned to foreign jurisdictions. These officers often live a transient life; they are not regularly assigned to one location for more than a few years and the relationships they build are only temporary. Although former network members may continue to communicate informally after their departure, their primary focus will usually have shifted elsewhere. The officer who replaces this network member must rebuild the foundation of trust that was established by his predecessor, which may not occur rapidly, especially given that the officer is also adjusting to life in a new country.

This process of membership change in a network may occur on a regular basis. The larger the number of people in the network, the more frequently this change occurs. Network change is not limited to those officers assigned to work in a foreign jurisdiction but officers from the host country as well. As the chart above shows, ICE attachés interacted with their foreign counterparts as well as with various agencies from their host country. Just as the foreign officers are rotated and re-assigned, officers from the host country's agencies that are part of the network are often reassigned to other units or cities. The result of these situations is a network that is in constant flux. One mechanism that could be employed to stabilize the network and help it work more efficiently is the foundation of working groups.

The use of network working groups is not new as a counter-terrorism strategy. In 1979, the United Kingdom established the Police Working Group on Terrorism. The aim of this group was to share operational knowledge among a variety of European police agencies. Cooperation in this working group emerged slowly at first, as there was an initial reluctance to share information. However, as a sense of mutual respect and an expectation of reciprocity increased, cooperation grew. The Police Working Group on Terrorism may be an appropriate model on which to build a transnational network to combat terrorist travel

One possible model for a working group to combat terrorist travel would be the establishment of a Migration and Border Security Working Groups. These working groups could be established in global cities such as New York, London, Dubai or Hong Kong, which are large hubs for the movement of goods and people. By having the group's focus on both immigration and border security issues, it can work to deter several non-terrorist crimes related to border security, like drug smuggling, money laundering and others listed by the respondents to the questionnaire. Structuring the working groups this way opens it up to other agencies with an interest in border security, and in doing so gives the group access to those agencies' resources as well.

Migration and Border Security Working Groups should not be viewed as international organizations or new multinational police organizations. It would be nothing more than a mechanism for members of a transgovernmental network assigned to a particular geographical area to gather together on a regular basis in order to share information, ideas and best practices and to a certain extent, bond. An agency responsible for border security from the host nation can organize monthly meetings where

representatives from agencies responsible for border security from like-minded countries are invited to attend. At these meetings the members of the network get to interact with one another face-to-face, giving the opportunity for new network members to be introduced to their colleagues from other agencies and nations. The working group is not designed to replace the regular interaction between individual network members, but rather is meant to help sustain the network and maintain trust through regular informal meetings.

The working group sustains the network by helping to maintain trust between existing members and helping new members develop trust within the network. Conditions may not require each network member to interact with every other member on a regular basis outside the working group's monthly meeting. The meeting provides a forum for individual network members to maintain a relationship in absence of regular interaction, so that when conditions require interaction between these network members, it occurs within an environment of trust. When a new officer is assigned to the area covered by the working group, the meetings provide a formal gateway into the network. If this new officer has the luxury of his assignment overlapping that of the officer he is replacing, the working group meetings provides the opportunity for the outgoing member to introduce his replacement. If the new officer does not have a transition period with the officer he is replacing, the working group provides the vehicle for integrating into the network rather than trying to develop relationships which each individual network member separately. The working group will also provide the new member with an introduction to the norms that govern the network's behavior, laying the foundation for a professional relationship based on trust.

The working group may also have the unintentional benefit or providing a social network for an officer recently assigned overseas. Moving from the comfort of one's native country to a foreign land where one is required to learn new customs, traditions and means of social interaction can be a stressful experience. This stressful situation is compounded when family is involved in the move. The working group meetings provide an immediate introduction to other individuals who have experienced similar situations, and the group can act as a support group for a new officer and as a source of social as well as professional interaction. These experiences unite network members beyond their professional identity of an immigration, law enforcement or intelligence officer. They also have shared life experiences that create an even stronger common identity that form the foundation of a relationship based on trust.

Transgovernmental Networks - The Future of Global Governance

The primary goal of the strategy of assigning law enforcement officers overseas to work directly with their foreign counterparts is to build a network of law enforcement officers as capable and as swift as the networks criminals and terrorist use (Rees 2006: 31). The data provided by the respondents seem to suggest that a global network comprised of ICE's attachés and their foreign partners is such a network. By mirroring the behavior of global social movement organizations such as transnational advocacy networks, they have created the foundation of global information sharing networks based on trust, shared experiences, and common identity, which grow outward to other members of the network. This network's structure mirrors that of the global Salafi jihad movement, the main threat presented by non-state actors to the United States and its Western allies, all of whom have been designated as the "far enemy" by the movement.

Both networks are comprised of a leadership that is vertical, and a hierarchical network that exerts control and directs a horizontal network of foot soldiers through various network hubs. The ICE's attachés' network has a distinct operational advantage over the global Salafi jihad movement's network in that they do not need to operate clandestinely and can interact with their fellow network members openly.

The key components of a transgovernmental network's success are the existence of trust between network members and the ability to share information quickly and effectively. In order for the network to remain robust, efficient information sharing and an environment of trust must be maintained. Given that information is often viewed as a commodity that is often horded, coupled with the transient nature of the network members, it is often difficult to maintain a robust network. The network itself can take steps in order to help ensure the network remains strong. If, as the respondents indicated, the agencies represented in the network have difficultly in obtaining information from other agencies within their own government, these agencies must put into place mechanisms for gathering and disseminating their own information and intelligence. The network, through the formation of Migration and Border Security Working Groups, can ensure that regular contact between network members occurs. This regular contact will help maintain an environment of trust between its members while helping new members integrate into the network. By taking these steps, the network can build upon the strong foundation that is already in place and expand the network further in order to help combat terrorist travel and other transnational crimes.

Transnational advocacy networks stress fluid and open relationships among committed and knowledgeable actors in specialized issue areas and operate through

global networks (Keck and Sikkink 1998: 8). Through their collective action, they have turned their attention to global problems and issues they feel need to be addressed. This approach has resulted in transnational advocacy networks having a greater impact on the world and having an increased role in global governance. Transgovernmental networks also have to deal with global problems that cannot be addressed unilaterally by domestic actors. Transgovernmental networks have given traditionally domestic agencies a global reach that provides the flexibility and efficiency to deal with crime and terrorism that is not found within traditional instruments of global governance such as regimes and international organizations. Moving forward into the second decade of the 21st century, transgovernmental networks appear to be the future of global governance in an increasingly shrinking world.

CONCLUSION:

The phenomenon of globalization has created a global interdependency where issues which were once purely domestic have become transnational. This situation has required both states and non-state actors to find new ways to operate in this new environment. Essentially, they needed to develop a new mechanism of global governance beyond international organizations and regimes. Global civil society, more specifically social movement organizations, quickly learned the benefits of establishing global networks to accomplishing the goals. States have begun to follow suit.

Summary:

States have begun developing relationships between similar agencies across governments, rather than dealing exclusively through foreign ministries. Officials from these agencies interact through transgovernmental networks comprised of government officials from various nations, forming both formal and informal global networks that reach out to their foreign counterparts. When the problem facing states is the threat to security from non-state actors such as criminal or terrorist organizations; transgovernmental networks of law enforcement and intelligence officers are often called upon to help combat this threat. It is the way in which these networks operate that this research sought to gain a better understanding.

In order to accomplish this goal, a qualitative case study approach was utilized to study how a transgovernmental network works to combat a particular activity of

international criminal and terrorist organizations. More specifically, how officers from U.S. Immigration and Customs Enforcement (ICE attachés) operate in foreign countries in order to combat terrorist travel. By studying these officers, the research sought to identify best practices that may be shared with others, identify ways in which this strategy may be improved to better combat terrorist travel, and determine if this strategy can be applied to combat other transnational crimes. Based on the existing literature on transitional advocacy networks and transgovernmental networks, a hypothesis was developed that asserted that these officers assigned to foreign jurisdictions operate and interact with one another in an attempt to prevent terrorist travel in much the same way that members of transnational advocacy networks interact and operate to address global issues and problems that they feel need attention.

What this research showed was that the hypothesis did in fact appear true. These officers are part of a transgovernmental network that works to combat terrorist travel; and this network operates and behaves in much the same way as transnational advocacy networks. These officers are hubs in a horizontal information sharing network built on trust and a common identity which strengthens as interaction becomes more frequent. This network consists not just of ICE attachés but also nodes made up of a variety of stakeholders with an interest in combating terrorist travel. These stakeholders include officers from the immigration agency of the host country, local and national law enforcement agencies of the host country, and their foreign counterparts assigned to the same host country by their agencies.

This transgovernmental network of officers not only shares characteristics with transnational advocacy networks but also mirrors the structure of the global Salafi jihad

movement's network, which is viewed as the greatest security threat posed by non-state actors to the United States and its western allies, what the movement labels the "far enemy." Both networks consist of leadership in the form of a vertical hierarchical network in a centralized location. This vertical network provides direction and guidance through a hub to a global horizontal network consisting of many nodes. It is the travel of these members of the global Salafi jihad movement's network that the transgovernmental network studied here is trying to prevent. It appears that this transgovernmental network has laid the foundation for "a network of law enforcement officers as capable and as swift as the networks criminals use (Rees 2006: 31)." By doing so, they have put into practice the counter-terrorism strategy of confronting "networks of terror with networks against terror (Bendiek 2006: 5)."

Another goal of this research was to identify best practices that could be adopted by other transgovernmental networks to assist them in accomplishing their missions. While specific best practices were not identified, what the data collected suggested were the transgovernmental network of which the ICE attachés are members could take steps to help them work more efficiently and assist the network in accomplishing their mission. The ability to share information and the existing trust between network members are crucial factors to the network's success. The respondents expressed frustration with their access to actionable information and intelligence, especially when held by other agencies within their own government. One step that can be taken to help address this problem is for those agencies represented in the network to develop their own mechanisms for gathering and developing information and intelligence regarding terrorist travel.

The transient nature of officers assigned overseas can make maintaining trust between network members over time a challenging endeavor. One possible solution to this situation is by providing a loose structure to the network through the formation of working groups. By organizing regular scheduled meetings, the working groups can help ensure continued contact between network members while assisting new members assimilate into the network. Through these steps, a robust and effective network to combat terrorist travel can be built on the existing foundation of the transgovernmental network of which the ICE attachés are members.

The final goal of this research project was to determine if this governance strategy of transgovernmental networks can be applied to combat other transnational crimes. What was learned was that this approach is already being applied to combat other types of transnational crimes. The respondents indicated that ICE attachés not only combat terrorist travel, but also a variety of immigration and customs violations and crimes committed by non-state actors. These crimes include human smuggling and trafficking, child exploitation, drug smuggling, money laundering/financial crimes, extraditions, violation of intellectual property rights, and cyber crimes. These results, however, lead to the development of a new research questions: Is this transgovernmental network approach utilized by ICE attachés to combat transnational crimes being utilized by other agencies tasked with combating threats that span across borders? This new research question, while suggesting further research in the topic of transgovernmental network, also identifies weaknesses in this research.

Weaknesses and Limitations:

Important data were gathered regarding the way in which ICE attachés operate within a transgovernmental network to combat terrorist travel and other transnational crime. These data, however, only encompasses the experiences of officers from one agency assigned to foreign jurisdiction in an attempt to combat transnational crime. Canada pioneered the practice of stationing immigration officers abroad in order to prevent dangerous or inadmissible travelers from reaching their territory (Rekai 2002: 20); and Australia, the United Kingdom and the Netherlands also have similar programs as well (Koslowski 2004b: 7). Other agencies within the United States government, such as The Federal Bureau of Investigations and the Drug Enforcement Administration, also assign their agents outside the U.S. to gather information and coordinate their agencies' operations beyond the territory of the United States (Rees 2006: 32). The experiences of ICE attachés might not mirror those experience of agents assigned overseas by other U.S. agencies or immigration officers from other countries.

The total number of possible respondents was relatively small given that there are only 52 ICE attaché offices. As a result of this small population, obtaining results that could be considered statistically significant within an acceptable level would require nearly 100% participation, meaning that this research could only be qualitative in nature not quantitative. Given that quantitative research methods were not employed, the results of this research cannot be universally applied to all transgovernmental networks of law enforcement officers assigned overseas to combat transnational crime, let alone all transgovernmental networks.

The questionnaire used to collect data from the respondents had one major omission, which if not addressed by the respondents in other areas, would have left an important characteristic regarding this transgovernmental network undiscovered. When the respondents were asked to describe the methods and frequency of interaction and contact with various stakeholders who also may be responsible for: "Curtailing, combating or preventing; criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders in violation of the laws of any nations-state," the list of stakeholders did not include their counterparts from third countries also located in or covering the same country in their area of responsibility. Many of the respondents viewed these foreign counterparts as an important component of this transgovernmental network in that they felt it necessary to mention them in the open-end question portions on the questionnaire. Fortunately, these respondents did feel these foreign counterparts' role in the network were important enough to mention, yet important data still may have been lost by not including them on the initial list of stakeholders.

Finally, collecting data on terrorism is obviously a difficult task given that terrorists, by necessity, operate clandestinely and are secretive about details of their operations (Leiken and Brooke 2006: 504). All of the background material in this research relating to terrorist networks, individual terrorists and their entry methods was gathered from open sources, including media accounts. Relying on journalistic accounts can be risky because there is significant misinformation in the press. Many journalists do not distinguish between sources that have access to information and those that don't (Sageman 2004: 66). As a result, accounts of terrorist activity that appear in open sources, particularly the media, can be as much rumor as fact. Likewise, government

agencies may be less than forthcoming about all their counterterrorism strategies and operations. While open sources will provide accounts of some government successes in combating terrorism, it will not include those most successful programs that continue to yield benefits for fear the utility of these programs would be compromised. Just as terrorists operate clandestinely, often so to do those government agencies task with combating terrorism.

Implications

Despite the weaknesses and limitations of this research, it has made a significant contribution to the body of work across various disciplines including, global governance, security studies, international criminal justice, and global affairs as a whole by its interdisciplinary approach to studying a problem which is global in nature. While the results of the survey cannot be universally applied, it certainly suggests the existing global governance literature description of transgovernmental networks as informal institutions built on trust and a common identity that links actors across national boundaries and allows them to carry out various aspects of global governance in new and informal ways (Slaughter 2004, Hajer and Versteeg 2005, Pawlak 2007, Slaughter and Zaring 2007). It has shown, through proving the project's hypothesis true, that members of this network interact with one another in much of the same way that members of transnational advocacy networks interact with each other.

Substantial contributions were also made in the area of security studies. It has shown how law enforcement officers operate overseas and interact with their foreign counterparts in order to combat transnational crime and threats to global security, such as terrorism travel. It also revealed that the structure of this particular network, shares

similar characteristics to the network whose travel they are trying to combat. In doing so, it has provided a potential blue print for the strategy of combating networks of non-state actors who provide a threat to security with networks of representatives from states task with combating these non-state actors' activities.

Beyond the contributions made to the existing global governance literature, the topic transgovernmental networks in particular, this research has also laid the foundation for further research in these areas. As discussed earlier, through its use of qualitative research methods, it has shown that many conclusions found in the existing literature regarding transgovernmental appear to be true. However, data were collected from a small specialized population all of whom shared a common nationality and were employed by the same agency. This narrow view of the topic means it cannot necessarily be universally applied to all transgovernmental networks. Ironically, these weaknesses in the scope and design of this research provide a guide for further research into the topic of transgovernmental networks as a tool for global governance.

A single case study design was employed in order to investigate how ICE attachés operate overseas in order to combat terrorist. While this design has yielded valuable data, it only applies experience of officers from one agency. As discussed earlier, the strategy of assigning officers overseas to combat unwanted arrivals at ones border has been used by numerous nations. The experiences of these immigration officers from other nations are not reflected in the data. One possible way to fill this research gap would be to use this research on ICE attachés and replicate it in the form of a multi-case study design to include a wide-sample of officers assigned overseas by a variety agencies charged with enforcing their countries' immigration laws. Replicating and adopting this model into a

multi-case study will allow this potential future research to build on the success and learn from the short comings of this research on ICE attachés.

Just as this exploration into the ICE attachés' transgovernmental network could be adapted into a multi-case study design to examine how immigration officers from other countries operate to accomplish their missions. It could also be used to examine the activities of officers from law enforcement agencies who are assigned to foreign jurisdiction to combat activities not directly related to terrorist travel or other types of border security issues or used to combat other types of criminal networks, such as organized crime groups or international street gangs like Mara Salvatrucha (MS-13). Just as the FBI and the DEA have assigned their agents outside the U.S. to gather information and coordinate their agencies' operations beyond the territory of the United States, so have many other domestic and foreign law enforcement agencies. The Royal Canadian Mounted Police, National Police Services Agency of the Netherland (KLPD), and even the New York Police Department are just a few of the many law enforcement agencies that have adopted the strategy of assigning officers to foreign jurisdictions to combat transnational crime as a counterterrorism strategy. Conducting a study into how these officers operate in foreign jurisdictions would require the data collection questions to be revised to better reflect general crime control efforts than specific questions relating to terrorist travel and border security strategies; however the general research design could remain mostly unchanged.

Horizontal information sharing networks comprised of law enforcement officer are by no means the only type of transgovernmental networks where government officials interact with their foreign counterparts to deal with problems which are global in scale.

Non-state actors are far from the only threat to global security. The financial crisis, environmental degradation and pandemic illness are all global problems that require collective action to confront. Regulators from finance ministries, environmental agencies and health ministries also work together in both horizontal and vertical networks in an attempt to address these global problems. But regulators from national government agencies are just one group that address problems through transgovernmental networks; so do members of the legislative and judiciary branches of national governments, and increasingly so do representatives from sub-national governments. Simple replication of this research into how ICE attachés operate would not likely be the best research method for further study in these larger groupings of transgovernmental networks. It may provide valuable insight and data collection techniques from a specialized population spread across the globe, while illustrating many of the benefits and pit falls of these collection methods.

The research methods used have significance beyond just the study of transgovernmental networks or even global governance. They have significance and value to all social sciences. Just as globalization has affected state and non-state actors' abilities to operate effectively, it has also impacted those who pursue academic research on a global scale. Like this exploration into the activities of ICE attachés, researchers are finding it necessary to gather data from across the global. Most research method texts however do not dedicate significant space to research design which is transnational in scope. Nor, do they explain how to adapt existing methods to meet these needs. The methods employed here do just that. The Internet was used extensively to recruit study subjects from a specific population, design and disseminate the data collection tool, and

collect the data for analysis. This was accomplished while remaining in compliance with

Rutgers University's regulations for conducting research on human subjects. As such,

these methods can serve as a prototype for others conducting social science research on a

global scale and are faced with similar challenges.

Perhaps the most significant contribution of this work is in the emerging field of

international criminal justice. Studies of criminal justice and criminology have long taken

an interdisciplinary approach to research, encompassing such fields as sociology,

psychology, law, public policy and administration, and even political science. As

international criminal justice continues to become an important sub-field within the

discipline, global governance literature and theories will play vital role in this sub-field.

This research into the way ICE attachés operate to prevent terrorist travel draws on

theories from the existing global governance literature and applies them to crime

prevention techniques utilized by law enforcement on a global scale. In doing so, it

shows the increasing interconnectivity between the subjects of global governance and

criminal justice, and the need for further cross-discipline research to the benefit of both

fields.

From a personal stand point, this was a very rewarding experience for me. As

discussed in the preface of this dissertation, my return to graduate school to work towards

my doctorate was driven in great part by the events of September 11, 2001. I wanted to

understand how I, as an officer charged with protecting the citizens of the United States,

failed to prevent the terrorists who carried out these attacks from entering the United

States and what could be done to prevent it in the future. Rather than satisfying this

desire, this dissertation has furthered my need to continue researching, not just terrorist

travel, but also the larger topics of transnational networks and transnational crime and crime controls.

Professionally, I was fortunate enough to be part of this transgovernmental network of officers working together to combat terrorist travel, although I did not understand at the time that this was a network or of my membership. I was not an officer assigned to foreign jurisdiction, rather an officer of the host country who worked directly with these officers assigned to foreign jurisdiction on a regular basis in order to support the border security of both nations. While an officer with U.S Customs and Border Protection and U.S. Immigration and Customs Enforcement, I interacted with immigration officers assigned to the United States from a variety of countries including Canada, the United Kingdom and Taiwan, as well as consular officers from a variety of nations tasked with dealing with immigration and border security matters. I have always been impressed with the professionalism and dedication of these officers. What this research has taught me is that the United States, and my agency in particular, has many officers who are equally as dedicated and working to provide, not just for the security of the United States but also, for the security of their international partners, as well. I feel that if the globalization of the world continues at a rapid pace, these officers, and other like them, will become an important feature of any strategy to combat transnational crime and terrorism.

Road Map for the Future:

As Anne-Marie Slaughter (2004) points out, transgovernmental networks have become a key feature of global governance in the 21st Century, but they remain under-appreciated, under-supported, and under-utilized. It is my hope that this work, by adding

to the existing literature on transgovernmental network, will help bridge this gap. This research has shown how one transgovernmental network, comprised of ICE attachés and other stakeholders in maintaining border security, work to combat terrorism travel and other transnational crime. It has offered valuable insight into how horizontal information sharing networks operate to address global problems, offered suggestions into how this network can function more effectively, and presented a potential roadmap for further research into transgovernmental networks.

By proving the hypothesis that members of transgovernmental network operate in much the same way as members of transnational advocacy networks, it will allow both networks to learn how to operate more effectively from each other. The results of the hypothesis test does not just provide benefit to governance practitioners, such as officials from agencies tasked with maintaining border security or members of global civil society, but also academics and others researching transgovernmental networks. Like this research, the similarities between the ways these two network types operate allows researchers investigating transgovernmental networks to draw on both the existing literature and research on transgovernmental networks and social movement organizations such transnational advocacy networks.

Anne-Marie Slaughter was correct with her claim that transgovernmental networks have become a key feature of global governance in the 21st Century. Their informal structure allows them to respond rapidly, and often in innovated ways, when new problems present themselves. Transgovernmental networks are uniquely capable of addressing global problems that flow from outside sources (Slaughter 2004: 170),

including problems perceived as a threat to global security such as transnational crime and international terrorism.

Criminals and terrorists are both opportunist. As globalization continues, criminals, terrorists, their organizations and networks will continue to take advantage of advancements in communication and transportation to further their objectives. In my opinion, this will increase the threat that transnational crime and terrorism poses to global security. Agencies tasked with border security and combating transnational crime, such as U.S. Immigration and Customs Enforcement, will need to dedicate more resources to their international operations. This increase in international operations does not just mean increasing assets overseas, but will require increasing resources domestically to allow for greater interaction and cooperation with foreign counterparts assigned within their jurisdictions. I believe that through this type of global partnership and collective actions, agencies tasks with combating transnational crime and terrorism can best work to combat these global security threats.

Transgovernmental networks should not be viewed as replacements to other institutions of global governance. Solving global problems still requires formal collective actions between states. International organizations, regimes and other formal governance institutions are not obsolete and will remain important components of any strategy to address problems on a global scale. Transgovernmental networks complement these more formal institutions. It is the fluidity of these networks that make them best suited to responded to rapidly changing situations or crises that need immediate and direct action or issues that require specific skills sets to combat effectively, such as preventing

terrorists from crossing international borders to train for, plan, finance and carry out attacks.

It is the growing threat to security from transnational non-state actors and the role of transgovernmental networks in combating these threats that show the true value and contribution of this work to the existing body of literature in both the fields of global governance and criminal justice. Further research into the security threat presented by non-state actors and transnational crime requires that theses two fields do not work independently of one other. They must each draw from the others body of work and take a cross-discipline approach when exploring transnational crime and terrorism. This research did just that. It pulled from the theories found in global governance literature and showed how they have been applied by criminal justice practitioners on a global scale. In doing so, this work has provided a road map in the form of its methods and design for further research in theses areas, while providing a strong foundation for building a greater body of literature across both disciplines.

Bibliography

Adamson, Fiona B. (2005) "Globalisation, Transnational Political Mobilisation, and Networks of Violence" *Cambridge Review of International Affairs,* Vol. 18, No. 1 April 2005

Al-Qaeda (unknown) *Declaration of Jihad Against the Country's Tyrants Military Series,* Seized from al-Qaeda member's home in Manchester England.

Andreas, Peter (2001) "The Transformation of Migrant Smuggling across the US-Mexican Border," in Kyle, David and Koslowski, Rey (ed.) *Global Human Smuggling: Comparative Perspectives,* Baltimore, The John Hopkins University Press

Andreas, Peter (2003) "Redrawing the Line: Borders and Security in the Twenty-first Century," *International Security,* Vol. 28, No. 2, pp. 78-11 (Fall 2003), MIT Press.

Andreas, Peter and Nadelmann, Ethan (2006) *Policing the Globe" Criminalization and Crime Control in International Relations,* Oxford University Press, New York

Arrillaga, Pauline, Rodriguez, Olga (2005) "The Terrorist Immigration Connection," Associated Press, July 3, 2005

Baker, Mark (2003) "Terrorist Mastermind Who Ran Out of Places to Hide," *The Sydney Morning Herald*, August 18, 2003

Ballard, Mark (2008) "Europlod plan to share DNA and biometric data comes under fire," *The Inquirer*, April 28, 2008, available at: http://www.theinquirer.net/inquirer/news/929/1028929/euro-dna-plan-slated

Bellanova, Rocco (2009) "Prüm: A Model 'Prêt-à-Exporter'? The 2008 German–US agreement on Data Exchange," *CEPS CHALLENGE programme,* March 2009 available at: **http://www.ceps.eu**

Bendiek, Annegret (2006) "Steps Toward a Coherent Network Policy." *EU Strategy on Counter-Terrorism,* German Institute for International and Security Affairs. November 2006.

Benjamin, Daniel, Simon, Steven (2002) *The Age of Sacred Terror,* Random House, New York.

Benner, Thorsten, 1998 "Book Review of Activist Beyond Borders, *Millennium: Journal of International Studies* 28 (1), pp. 188-190

Bernton, Hal, Carter, Mark, Heath, David Neff, (2002) "The Terrorist Within: The Story Behind One Man's Holy War Against America" *The Seattle Time,* June 23-July 7, 2002

Bertone, Andrea M. (2008) "Combating Human Smuggling: Transnational Advocacy Networks between Thailand and the United States," presented at the 49th Annual International Studies Association Convention, March 24-28, 2008

Camarota, Steven A. (2002) *The Open Door: How Militant Islamic Terrorists Entered and Remained in the United States, 1993-2001,* Center for Immigration Studies, Washington, D.C.

Canada Border Services Agency (2009a) "About CBSA" available at: http://www.cbsa-asfc.gc.ca/agency-agence/who-qui-eng.html

Canada Border Services Agency (2004) "Fact Sheet: Immigration Intelligence Overview," January 2004, available at: http://www.cbsa-asfc.gc.ca/media/facts-faits/031-eng.html

Citizenship and Immigration Canada (2003) "Statement of Mutual Understanding on Information-Sharing" *Policies and Regulations,* Citizenship and Immigration Canada available at: http://www.cic.gc.ca/english/policy/smu/

Cobain, Ian and Weaver, Matthew (2008) "Rashid Rauf, The Mysterious Adult Life of a Birmingham Baker's Boy Turned Alleged al-Qaida Terrorist." *The Guardian*,

Council of the European Union (2005) "The Prüm Convention" July 7, 2005, available at: http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf

Custom and Border Protection (2005a) "United States – Canada NEXUS Program" U.S. Customs and Border Protection. Department of Homeland Security, available at: http://www.customs.gov/xp/cgov/travel/frequent_traveler/nexus.xml

Custom and Border Protection (2005b) "United States – Canada NEXUS Air Program" U.S. Customs and Border Protection. Department of Homeland Security, available at: http://www.customs.gov/xp/cgov/travel/frequent_traveler/nexus_air.xml

Custom and Border Protection (2008a) "This Is CBP," December 11, 2008, available at: http://cbp.gov/xp/cgov/about/mission/cbp_is.xml

Custom and Border Protection (2008b) "Protecting our Borders against Terrorism," May 14, 2008, available at: http://cbp.gov/xp/cgov/about/mission/cbp.xml

Department of Homeland Security (2002) "*Summary of Smart Border Action Plan Status,"* September 9, 2002, available at: http://www.dhs.gov/xnews/releases/press_release_0024.shtm

Department of Homeland Security (2006) "The Visa Waiver Program," *Travel Guide for Travelers Visiting the United States,* August 2006, available at: www.dhs.gov

Department of Homeland Security (2008) "DHS and DOJ Sign Agreement on Enhancing Cooperation in Preventing and Combating Serious Crime with the Republic of Estonia," September 29, 2008, available at: http://www.dhs.gov/xnews/release/pr_1222715330518.shtn

Department of Immigration and Citizenship Australia (2007) *Strategic Plan for Identity Management 2007 – 2010* "Identity Matters," available at: http://www.immi.gov.au/managing-australias-borders/border-security/systems/identity.htm

Desai, Meghnad and Said, Yahia (2001) "The New Anti-Capitalist Movement: Money and Global Civil Society" *Global Civil Society 2000,* Oxford University Press, Oxford.

Falk, Richard (1999) *Predatory Globalization: A Critique,* Polity Press, Cambridge, UK

Fouda, Yosri, Fielding, Nick (2003) *Masterminds of Terror: The Truth Behind the Most Devastating Terrorist Attack the World Has Ever Seen,* Arcade Publishing, New York

Friedman, Thomas L. (2000) *The Lexus and the Olive Tree*, Updated and expanded Edition, Anchor, New York

FRONTEX (2009) "Mission Statement": available at: http://www.frontex.europa.eu/more_about_frontex/

Giddens, Anthony (1990) *The Consequences of Modernity,* Stanford University Press, Palo Alto, CA

Greenberg, Richard, Cruickshank, Paul and Hansen Chris (2008) "Inside the Terror Plot that 'Rivaled 9/11' What Really Happened in the Case that Led Airlines to Ban Liquids and Gels" *Dateline NBC,* September 16, 2008

Guild, Elspeth (2007) "Merging Security from the Two-Level Game: Inserting the Treaty of Prüm into EU Law," *Centre for European Policy Studies Policy Brief,* No. 124, March 2007. available at: http://ssrn.com/abstract+1334608

Hajer, Maarten, Versteeg, Wytske (2005) "Performing Governance Through Networks." *European Political Science,* European Consortium for Political Science Research, 2005 Issue 4. p 340-347)

Home Office (2007) *Securing the UK Border, Our Vision and Strategy for the Future* March 2007, available at: http://www.bia.homeoffice.gov.uk/managingborders/borders/

Home Office (2008) *How the Risk and Liaison Overseas Network can help you,* October 30, 2009, available at: http://www.ukba.homeoffice.gov.uk/aboutus/ workingwithus/transportindustry/rlon/howrloncanhelp/

Home Office (2009a) "About UK Border Agency," available at: http://www.bia.homeoffice.gov.uk/aboutus/

Home Office (2009b) *UK Border Agency Business Plan: April 2009-March 2012,* Available at: http://www.ukba.homeoffice.gov.uk/sitecontent/documents/aboutus/businessplan/

Hufbauer, Gary C. Schott, Jeffrey J. (2004) "The Prospect for Deeper North American Economic Integration: A U.S. Perspective" *The Border Papers,* C.D. Howe Institute, November 2002, Toronto, available at: http://www.iie.com/publications/papers/hufbauer0104.pdf

Immigration and Customs Enforcement (2009a) "About ICE," April 7, 2009, available at: http://www.ice.gov/about/index.htm

Immigration and Customs Enforcement (2009b) "Mission," *Office of International Affairs,"* February 20, 2009, available at: http://www.ice.gov/about/internationalaffairs/index.htm

Immigration and Customs Enforcement (2009c) "Attaché Offices," *Office of International   Affairs,"* March 19, 2009, available at: http://www.ice.gov/about/internationalaffairs/AttacheOffices.htm

International Civil Aviation Organization (2009) "Strategic Objectives for ICAO," available at: http://www.icao.int/icao/en/strategic_objectives.htm

International Organization for Migration (2003) , *International Terrorism and Migration,* available at*:* www.iom.int/en/PDF_Files/tcm/Int_terrorism_migration.pdf

International Organization for Migration (2009) "About the IOM," available at: http://www.iom.int/jahia/Jahia/about-iom/lang/en

INTERPOL Media Release (2007) "INTERPOL warns of Terrorists Using Stolen Travel
        Documents to Evade Detection," May 2, 2007, available at:
        http://www.interpol.int/public/ICPO/PressReleases/PR2007/PR200715.asp

Jennings, Peter (2004) "US Concerned About Possible Terrorist Use of Stolen Passports"
        ABC World News Tonight, April 26, 2004, story 9

Kaldor, Mary, Anheier Helmut, Glasius, Marlies (2003) "Global Civil Society in an Era
        of Regressive Globalisation" *Global Civil Society 2000,* Oxford University Press,
        Oxford.

Kean, Thomas H. Hamilton, Lee H. (2005) " 9/11 Public Discourse Project Ceases
        Operations," *9-11 Public Discourse Porjec,* December 31, 2005 availible at:
        http://www.9-11pdp.org/press/2005-12-31_statement.pdf

Keck, Margaret E. Sikkink, Katheryn (1998) *Activists Beyond Borders,* Cornell
        University Press, 1998

Keohane, Daniel (2005) "One Step Forward, Two Steps Back," *E!Sharp,* November-
        December 2005, available at:
        http://www.cer.org.uk/pdf/article_keohane_esharp_nov05.pdf

Keohane, Robert O. Nye, Joseph S. (1974) "Transgovernmental Relations and
        International Organizations" *World Politics*, Vol. 27, No. 1, pp. 39-62,
        The John Hopkins University Press.

Kirby, Aidan (2007) "The London Bombers as 'Self-Starters': A Case Study in
        Indigenous Radicalization and the Emergence of Autonomous Cliques" *Studies in
        Conflict and Terrorism,* Volume 30 p. 415-428, Routledge.

Koslowski, Rey (2004a) "International Cooperation on Electronic Advanced Passenger
        Information Transfer and Passport Biometrics" Presentation at the International
        Studies Association Meeting, Montreal, March 17-20, 2004

Koslowski, Rey (2004b) "Possible Steps Toward an International Regime for Mobility",
        Migration Perspectives, No 8 (October 2004), The Research Paper Series of the
        Global Commission on International Migration: at:
        http://www.gcim.org/en/ir_gmp.html

Koslowski, Rey (2008) "Global Mobility and the Quest for an International Migration
        Regime," Presentation at Conference on International Migration and
        Development: Continuing the Dialogue – Legal and Policy Perspectives, the
        Center for Migration Studies (CMS) and the International Organization for
        Migration (IOM), New York, New York, January 17-18, 2008, Revised April
        2008.

Kyle, David and Koslowski, Rey (2001) "Introduction" for *Global Human Smuggling: Comparative Perspectives,* Baltimore, The John Hopkins University Press

Langhorne, Richard (2001) *The Coming of Globalization,* St. Martin Press, New York

Langhorne, Richard (2006) chapter on "Global Civil Society," *The Essentials of Global Politics,* Hodder Arnold, London

Leiken, Robert S. (2004a) *Bearers of Global Jihad? Immigration and National Security After 9/11,* The Nixon Center, Washington D.C.

Leiken, Robert S. Brooke, Steven (2004b) "Who is Abu Zarqawi." *The Weekly Standard,* May, 24, 2004 Volume 9 Issue 35

Leiken, Robert S. Brooke, Steven (2006) "The Quantitative Analysis of Terrorism and Immigration: An Initial Exploration," *Terrorism and Political Violence,* No 18: 503-512

Letzing, John (2005) "Cross-Border Security: the Visa Loophole," *Al-Qaeda's New Front,* Frontline, Public Broadcasting System,

Levine, Samantha (2004) "Terror's Best Friend" *U.S. News and World Report* December 6, 2004

Lewis, Aidan, (2005) "Bombing Suspect Used Fake Name to Enter UK." Associated Press, August 1, 2005

Luif, Paul. (2007) "The Treaty of Prüm: A Replay of Schengen?," *European Union Studies Association Biennial Conference,* May 17-19, 2007, Montreal, Canada.

McNabb, David E. (2004) *Research Methods for Political Science, Quantitative and Qualitative Methods,* M.E Sharpe, Armonk, NY

Miller, John, Stone, Michael (2002) *The Cell: Inside the 9/11Plot, and Why the FBI and CIA Failed to Stop It.* Hyperion Books, New York

Mittelman, James H. (2000) *The Globalization Syndrome, Transformation and Resistance,* Princeton University Press, Princeton NJ

Naim, Moises (2003) "Five Wars of Globalization: The illegal trade in drugs, arms, intellectual property, people, and money is booming," *Foreign Policy,* issue No. 134, pages 28-37, Washington

National Counterterrorism Center (2006) *National Strategy to Combat Terrorist Travel* May 2, 2006. available at:
http://www.nctc.gov/docs/u_terrorist_travel_book_may2_2006.pdf

9-11 Commission (2004a) *9-11 Commission Staff Monograph on 9/11 and Terrorist Travel* New York: W.W. Norton 2004.

9-11 Commission (2004b) *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, New York: W.W. Norton 2004.

9-11 Commission (2004c) *About the Commission,* available at: http://govinfo.library.unt.edu/911/about/index.htm

9-11 Public Discourse Project (2005) "Final Report on 9/11 Commission Recommendations," December 5, 2005, Available at: http://www.9-11pdp.org/press/2005-12-05_report.pdf

Noble, John J. (2004) "Fortress America or Fortress North America" IRRP Conference on North American Integration: Migration, Trade and Security, April 2004 available at: http://www.irpp.org/events/archive/apr04/noble.pdf

Pawlak, Patryk (2007) "From Hierarchy to Networks: Transatlantic Governance of Homeland Security," *Journal of Global Change and Governance, Vol. 1 Issue 1, Winter 2007*

Powell, Bill (2008) "A Terrorist's Network" *Time Magazine,* August 20, 2008

Rapoport, David (2001) "The Fourth Wave: Sept. 11 in the History of Terrorism," *Current History*, Dec. 2001, pp. 419-424.

Rees, Wyn (2006) *Transatlantic-Counterterrorism Cooperation: The New Imperative,* Routledge, London, 2006

Reeve, Simon (1999) *The New Jackals: Ramzi Yousef, Osama Bin Laden and the Future of Terrorism,* Northeastern University Press, Boston

Rekai, Peter (2002) "US and Canada Immigration Policies, Marching Together to Different Tunes" *The Border Papers,* C.D. Howe Institute, November 2002, Toronto, available at: http://www.cdhowe.org/pdf/Rekai.pdf

Robertson, Roland (1992) *Globalization: Social Theory and Global Culture,* Sage Publications, London

Rosenau, James N (1995) "Governance in the Twenty-first Century," *Global Governance"* Vol. 1 1995

Sageman, Marc, (2004) *Understanding Terror Networks,* University of Pennsylvania Press, Philadelphia

Salter, Mark B. (2004) "Passports, Mobility and Security: How Smart Can the Border Be?" *International Studies Perspective,* Vol. 5 No. 1 Blackwell Publishing, Malden, MA

Sassen, Saskia (2000) "The Impact of the Internet on Sovereignty: Real and Unfounded Worries" presented at *The Internet and International Systems: Information Technology and American Foreign Policy Decision making*, December 10, 2000, San Francisco, CA.

Schock, Kurt (2005) *Unarmed Insurrections: People Power Movements in Nondemocracies,* University of Minnesota Press, Minneapolis

Shapiro, Jacob. (2005) "Organizing Terror: Hierarchy and Networks in Covert Organizations" *Paper presented at the annual meeting of the American Political Science Association,* Washington, DC, Sep 01, 2005

Slaughter, Anne-Marie (2004) *A New World Order,* Princeton, Princeton University Press, 2004

Takeyh, Ray and Gvosdev, Nikolas (2002) "Do Terrorist Networks Need a Home?" *The Washington Quarterly* Vol 25, No 3, pp 97-108, The Center for Strategic and International Studies and Massachusetts Institute of Technology

Tarrow, Sidney (2002) "The New Transnational Contention: Organization, Coalition. Mechanisms" Presentation at the Panel on "Social Movements and Transnational Social Movements" American Political Science Association Annual Metting, September 1, 2002, Chicago.

U.S. v. Kourani (2003) Indictment filed November 19, 2003, U.S. District Court Eastern District of Michigan , Southern Division.

Wapner, Paul (1995) "Politics Beyond the States: Environmental Activism and World Civic Politics" *World Politics,* Vol. 47 Issue 3 Apr. 1995, John Hopkins University Press.

Waters, Malcolm (1995) *Globalization,* Routledge Publishing, New York.

White House (2002) "U.S.-Canada Smart Border/30 Point Action Plan Update." *Office of the Press Secretary,* December 6, 2002, available at: http://www.whitehouse.gov/news/releases/2002/12/20021206-1.html

Winer, Jonathan M. (2004) "Cops Across Borders: The Evolution of Transatlantic Law Enforcement and Judicial Cooperation," Presentation at the Council on Foreign Relations, September 1, 2004

World News (2004) "Trial for Afghan Murder Suspects" *SBS-World News,* November, 29, 2004

Appendices

Appendix 1-Letter Request for Participation-ICE Office of International Affairs

Appendix 2-E-mailed Request for Participation to Potential Respondents

Appendix 3-Questionnaire

Appendix 4- Curriculum Vitae

Appendix 1

Raymond Parmer
Acting Director,
Office of International Affairs
U.S. Immigration and Customs Enforcement
801 "I" Street, NW, Room 800
Washington, DC 20536

Director Palmer,

My name is Keith Cozine and I am a PhD candidate at Rutgers University, Division of Global Affairs. I am requesting assistance and participation, from you and your agency, in a research project affiliated with my doctoral dissertation.

As you are well aware, the openness and interconnectivity resulting from globalization has created an environment that has allowed transnational crime to flourish. Advancements in technology and transportation that have facilitated trade and travel have not done so exclusively to the benefit of legitimate transnational actors, but also to international criminal and terrorist organizations. As a result, law enforcement and intelligence agencies tasked with combating these activities must find new and innovative ways to share information and intelligence, and coordinate investigations with their foreign counterparts. Assigning Immigration Officers from one country to work with their foreign counterparts within their jurisdiction is one of the strategies that have been adopted in an attempt to prevent criminals and terrorists from crossing borders.

My research will examine how Immigration Officers operate within foreign jurisdictions to prevent terrorists from crossing borders to support, finance, and carry out operations. I plan to include five agencies tasked with enforcing its nation's immigration laws in this study to determine whether this is an effective strategy in preventing terrorist travel and, whether this can be applied to other transnational crimes.

The amount of effort and resources needed from you for your agency to participate in this research project would be minimal. If your agency agrees to participate, at the start of the research project, which I anticipate to begin in September 2008, I will send you an e-mail requesting participation in my survey. I ask that you forward this request on to all your agency's officers assigned in foreign jurisdictions. This request contains a link to a survey to be completed by the Immigration Officers assigned overseas within your organization. The surveys contain 26 questions, many of which require multiple responses. It is anticipated that it will take no longer

than 30 minutes to complete. There will be no need for you to complete a survey as well as it is only for Immigration Officers assigned overseas.

The data collected as a result of these surveys will primarily be used for the completion of my doctoral dissertation. Following the dissertation submission and defense, a copy will be forwarded to your office to be used as you see fit. It is only requested that further use by you or your agency is credited properly. It is my belief that this research, through its qualitative exploration of transgovernmental interaction between enforcement agencies (specifically Immigration Officers assigned overseas), will be of significant benefit to your agency. It is my hope that this research will highlight issues and challenges faced by various officers in the course of their official duties, while also identifying various best practices that, through the dissemination of this dissertation, can be shared between the participating agencies.

Thank you in advance for considering this request, and I hope to hear from you soon that your agency will participate in this research project. I ask that you respond in writing via e-mail or regular mail that your agency will assist by forwarding the request to participate to your officers assigned overseas. I can be reached via e-mail at kcozine@pegasus.rutgers.edu, by mail at 21 Rolling Hills Road, Clifton NJ, USA 07110 or by telephone at 973-332-4683 to answer any questions you may have or to discuss this project further.

Best Regards
Keith Cozine
Ph.D. Candidate
Rutgers University

Enclosed:

Abstract
Participation Request

Appendix 2

Officer:

My name is Keith Cozine. I am a PhD Candidate at Rutgers University, Division of Global Affairs and employee of U.S. Immigration and Customs Enforcement. I am requesting your assistance and participation in a research project as part of my doctoral dissertation.

I am conducting a case study of how immigration officers operate within foreign jurisdictions to prevent terrorists from crossing borders to support, finance, and carry out operations. Through this research I hope to determine whether assigning immigration officers overseas is an effective strategy in preventing terrorist travel and whether this can be applied to other transnational crimes.

The amount of effort and resources need for your participation in research project is minimal. If you agree to participate, simply click on the internet addresses below and complete the survey. The surveys contain 26 questions, many of which require multiple responses. It is anticipated that it will take no longer than 30 minutes to complete.   The survey is anonymous and you will not be asked to provide any biographical data other than your agency, job title and general location of your duty station.

The data collected from this survey will be used for the completion of my doctoral dissertation. It is not being conducted or sponsored by yours or any other government agency. Your participation is purely voluntary; however your participation would be greatly appreciated and be considered a valuable contribution to this research project. I will gladly forward you a copy of the project upon completion if requested.

 It is my belief that this research, through its qualitative exploration of transgovernmental interaction between enforcement agencies, specifically immigration officers assigned overseas, will be of significant benefit to you and your agency. It is my hope that this research will identify various best practices that, through the dissemination of this dissertation, can be shared between the participating agencies.

I thank you in advance for considering this request and hope you agree to participate in this research project by clicking on the link below. I can be reached via e-mail at keithcozine@yahoo.com, by mail at 21 Rolling Hills Road, Clifton NJ, USA 07110 or by telephone at 973-332-4683 to answer any questions you may have or to discuss this project further.

If you have any questions about your rights as a research subject, you may contact the Sponsored Programs at Rutgers University at:

Rutgers University Institutional Review Board for the Protection of Human Subjects
Office of Research and Sponsored Programs
3 Rutgers Plaza
New Brunswick, NJ 08901-8559
Tel: 732-932-0150 ext. 2104
Email: humansubjects@orsp.rutgers.edu

Please click here to participate in this survey or cut and past this address into bar of your web browser:
http://www.questionpro.com/akira/TakeSurvey?id=1090568

Best Regards
Keith Cozine
Ph.D. Candidate
Rutgers University

Appendix 3

These questions are an attempt to understand your working environment:

1) Which of the following agencies are you currently assigned?

☐ U.S. Customs and Border Protection
☐ U.S. Immigration and Customs Enforcement
☐ Canadian Border Security Agency
☐ Taiwan National Immigration Agency
☐ United Kingdom's Border Control and Immigration Agency
☐ Other: _____

2) What is your official title?   _____

3) Which best describes your experience working in the capacity of an Immigration and/or Law Enforcement Officer?

☐ Less than 5 years experience.
☐ 5 to 10 years experience.
☐ 10 to 15 years experience.
☐ 15 to 20 years experience.
☐ More than 20 years experience.

4) Which best describes your geographical area of responsibility?

☐ North America
☐ Latin America and the Caribbean
☐ Western Europe
☐ Eastern Europe
☐ Middle East and North Africa
☐ Sub-Sahara Africa
☐ Central or South Asia
☐ East Asia
☐ Southeast Asia or Oceania

5) Which best describes your office location.

     ☐ Consulate/Embassy of your country
     ☐ Offices of your agency located in the country to which you are assigned
     ☐ Offices administrated by an International or Regional Organization
     ☐ Offices of the immigration agency of the country to which you are assigned
     ☐ Offices of a national police agency of the country to which you are assigned
     ☐ Offices of a local agency of the country to which you are assigned
     ☐ Port of entry/exit or other border crossing
     ☐ Other: _____

These questions are an attempt to understand how, in your official capacity as an Immigration Officer assigned overseas, you attempt to curtail, combat or prevent; criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders in violation of the laws of any nations-state.

6) To what extent do you agree with the flowing statements: "Curtailing, combating or preventing; criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders in violation of the laws of any nations-state is the primary job responsibility as an Immigration Officer assigned overseas."

     ☐ Strongly agree
     ☐ Agree
     ☐ Neutral
     ☐ Disagree
     ☐ Strongly disagree
     ☐ I don't know
     ☐ I choose not to answer

7) Please list your other job responsibilities as an Immigration Officer assigned overseas besides: "Curtailing, combating or preventing; criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders in violation of the laws of any nations-state."

8) To what extent do you agree with the flowing statements: The job responsibilities listed in response to Question 7 are my primary job responsibility as an Immigration Officer assigned overseas."

☐ Strongly agree
☐ Agree
☐ Neutral
☐ Disagree
☐ Strongly disagree
☐ I don't know
☐ I choose not to answer

9) Pleas indicate how much of your official duties as an Immigration Officer assigned overseas is dedicated specifically to combating terrorist travel.

☐ None
☐ 1-20%
☐ 21-40%
☐ 41-60%
☐ 61-80%
☐ 81-99%
☐ This is my only responsibility.

10) Please describe to what level you are responsible for dealing with these issues specifically or directly related to: "Curtailing, combating or preventing; criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders in violation of the laws of any nations-state."

Ensure the integrity and security of the visa issuing system of your

☐   ☐   ☐   ☐   ☐   ☐   ☐

nation.							
Assisting other nations in maintaining and ensuring the integrity and security of the visa issuing system of their nation.	☐	☐	☐	☐	☐	☐	☐
Monitoring, curtailing and combating the use of stolen blank travel documents.	☐	☐	☐	☐	☐	☐	☐
Monitoring, curtailing and combating the use of fraudulent travel documents and the vendors who provide them.	☐	☐	☐	☐	☐	☐	☐
Monitoring methods of illegal entry into host countries.	☐	☐	☐	☐	☐	☐	☐
Monitoring, curtailing and combating human smuggling and trafficking activities and the organizations.	☐	☐	☐	☐	☐	☐	☐
Working with your host country to monitor suspicious travel of its residence and citizens	☐	☐	☐	☐	☐	☐	☐
Working with your host country to monitor travel patterns of known or suspected terrorist or criminals	☐	☐	☐	☐	☐	☐	☐
Working with your host country to monitor travel methods utilized by terrorist or criminals	☐	☐	☐	☐	☐	☐	☐
Other (please specify in box below)	☐	☐	☐	☐	☐	☐	☐

11) Please indicate the frequency of your interaction and contact with various stakeholders who are also may be responsible for: "Curtailing, combating or preventing; criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders in violation of the laws of any nations-state."

	Primary contact	Frequent contact	Some contact	Little contact	No contact
Other agencies within your Government	☐	☐	☐	☐	☐
Immigration agency of host nation	☐	☐	☐	☐	☐
Other law enforcement or intelligence agencies of host nation	☐	☐	☐	☐	☐
Foreign Ministry of host nation	☐	☐	☐	☐	☐
Law enforcement agencies below the national level	☐	☐	☐	☐	☐
International or Regional Organizations	☐	☐	☐	☐	☐
Private stake holders such as airlines or non-governmental organizations	☐	☐	☐	☐	☐
Other (please specify in box below)	☐	☐	☐	☐	☐

12) Please indicate method of your interaction and contact with various stakeholders who are also responsible for: "Curtailing, combating or preventing; criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders in violation of the laws of any nations-state."

	Through regular electronic communications such as telephone fax or e-mails	Dissemination of intelligence reports, trend analysis or bulletins	Through secure communications methods such as secure phone and fax lines, or telex	Unofficial in person meetings, briefings or conferences or at social situations such as receptions or dinners	Official in person meetings, briefings or conferences	No Contact
Other agencies within your Government	☐	☐	☐	☐	☐	☐
Immigration agency of host nation	☐	☐	☐	☐	☐	☐
Other law enforcement or intelligence agencies of host nation	☐	☐	☐	☐	☐	☐
Foreign Ministry of host nation	☐	☐	☐	☐	☐	☐
Law enforcement agencies below the national level	☐	☐	☐	☐	☐	☐
International or Regional Organizations	☐	☐	☐	☐	☐	☐
Private stake holders such as airlines or non-governmental organizations	☐	☐	☐	☐	☐	☐
Other (please specify in box below)	☐	☐	☐	☐	☐	☐

13) Please indicate the frequency of the following activities you take in order to better: "Curtail, combat or prevent criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders in violation of the laws of any nations-state."

	Primary means	Frequently	Sometimes	Rarely	Never
Assisting with coordinating investigations between your agency and other agencies	☐	☐	☐	☐	☐
Sharing general information such as trends, methods or statistics	☐	☐	☐	☐	☐
Sharing sensitive or secret intelligence	☐	☐	☐	☐	☐
Sharing information on specific individuals or organizations within your agency's databases.	☐	☐	☐	☐	☐
Advising others on specific individuals, situations or investigations	☐	☐	☐	☐	☐
Provide training	☐	☐	☐	☐	☐
Giving briefing, lectures and speeches	☐	☐	☐	☐	☐
Other (please specify in box below)	☐	☐	☐	☐	☐

14) Indicate the level of authorization required in order for you to conduct the following activities in order to better: "Curtail, combat or prevent criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders in violation of the laws of any nations-state."

	Little or no prior authorization from your agency	Only with prior authorization from your agency	In accordance with written agreement such as treaty or "memorandum of understanding"	Only when officially requested in writing and approved by your agency	Never conducted
Assisting with coordinating investigations between your agency and other agencies	☐	☐	☐	☐	☐
Sharing general information such as trends, methods or statistics	☐	☐	☐	☐	☐
Sharing sensitive or secret intelligence	☐	☐	☐	☐	☐
Sharing information on specific individuals or organizations within your agency's databases.	☐	☐	☐	☐	☐
Advising others on specific individuals, situations or investigations	☐	☐	☐	☐	☐
Provide training	☐	☐	☐	☐	☐
Giving briefing, lectures and speeches	☐	☐	☐	☐	☐
Other (please specify in box below)	☐	☐	☐	☐	☐

15) Please use the space to bellow to indicate any activities, methods and responsibilities as an Immigration Officer assigned overseas that has not already covered in this section:

```



```

These questions in this section are an attempt to get your <u>opinion</u> how, in your official capacity as an Immigration Officer overseas, are you being utilized to: Curtail, combat or prevent; criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders in violation of the laws of any nations-state." And what steps can and should be taken in order for you to be more successful in these areas.

16) The amount or time I spend in my official capacity as an Immigration Officer assigned overseas dedicated to: "Curtailing, combating or preventing; criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders in violation of the laws of any nations-state."

- ☐ This is my only responsibility
- ☐ This should be my primary responsibility
- ☐ More time should be dedicated to these issues
- ☐ I am dedicating sufficient amount of time
- ☐ Less time should be dedicated to these issues
- ☐ This should not be my responsibility
- ☐ I choose not to answer

17) The amount or time I spend in my official capacity as an Immigration Officer assigned overseas dedicated to other responsibilities not related to: "Curtailing, combating or preventing; criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders in violation of the laws of any nations-state."

- ☐ I have no other responsibilities
- ☐ I should have no other responsibilities
- ☐ More time should be dedicated to other issues
- ☐ I am dedicating sufficient amount of time to other issues
- ☐ Less time should be dedicated to these other issues
- ☐ I choose not to answer

18) Pleas indicate how much of your official duties as an Immigration Officer assigned overseas should be dedicated specifically to combating terrorist travel.

- ☐ None
- ☐ 1-20%
- ☐ 21-40%
- ☐ 41-60%
- ☐ 61-80%
- ☐ 81-99%
- ☐ This is my only responsibility.

19) Please use the space bellow to describe other resources or factors that assist to in your ability to "Curtail, combat or prevent criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders in violation of the laws of any nations-state."

20) Please rate the following characteristics of individuals you interact with in the course of your duties as an Immigration Officer assigned overseas by their value in assisting you in accomplishing your mutual goals.

	Extremely Important	Somewhat Important	Neutral	Not Very Important	Not at all Important	I choose not to answer
The citizenship of the individual	☐	☐	☐	☐	☐	☐
The individual is a government employee	☐	☐	☐	☐	☐	☐
The individual is a government employee of your nation	☐	☐	☐	☐	☐	☐
The individual is a government employee of any nation.	☐	☐	☐	☐	☐	☐
The individual is an employee is an employee of your agency	☐	☐	☐	☐	☐	☐
The individual is an immigration officer	☐	☐	☐	☐	☐	☐
The individual is a law enforcement or intelligence officer	☐	☐	☐	☐	☐	☐
Education level	☐	☐	☐	☐	☐	☐
Professional experience	☐	☐	☐	☐	☐	☐
Membership in professional organizations	☐	☐	☐	☐	☐	☐
Previous interaction	☐	☐	☐	☐	☐	☐
Type of interaction	☐	☐	☐	☐	☐	☐
Frequency of interaction	☐	☐	☐	☐	☐	☐
Previous professional relationship	☐	☐	☐	☐	☐	☐
Perceived "trustworthiness"	☐	☐	☐	☐	☐	☐
Frequency and quality of previous assistance given	☐	☐	☐	☐	☐	☐
Other (please specify in box below)	☐	☐	☐	☐	☐	☐

21) Please use the space bellow to describe situations, working environment or other factors that make it more difficult impede or prevent your ability to: "Curtail, combat or prevent criminals; smuggled or trafficked people; terrorists; or other individuals crossing international borders in violation of the laws of any nations-state."

22) How would you rate your current working environment?
- ☐ Excellent
- ☐ Very good
- ☐ Good
- ☐ Neutral
- ☐ Poor
- ☐ Very Poor
- ☐ I choose not to answer

23) Please use the space below to describe how your work environment could be improved

24) How would you rate your current overall job satisfaction?
- ☐ Very satisfied
- ☐ Satisfied
- ☐ Somewhat satisfied
- ☐ Neutral
- ☐ Somewhat dissatisfied
- ☐ Dissatisfied
- ☐ Very dissatisfied
- ☐ I choose not to answer

25) Please use the space below to describe how your rate of overall job satisfaction could be improved.

26) Is there anything else regarding Immigration Officers overseas, their official interaction with others, work environment, other factors or concerns you would like to pass on to the study coordinator? Or any concern or comments about this study or survey. Please tell us as much as you like, as little as you like or nothing at all.

CURRICULUM VITAE

Name: Keith Cozine-Born September 3, 1972, Belleville NJ

Address: 21 Rolling Hills Road
Clifton, NJ 07013

E-Mail: **keithcozine@yahoo.com**

Education:

Ph.D., Rutgers University, The Division of Global Affairs, Newark, NJ
2004-2009. Global Affairs

M.A., Rutgers University, School of Criminal Justice, Newark, NJ
1995-1998. Criminal Justice

B.A., Ramapo College of New Jersey, Mahwah, NJ
1990-1994. Political Science

Work Experience:

2005- Deportation Officer (Field Intelligence Officer)
Department of Homeland Security, U.S. Immigration and Customs Enforcement
Detention and Removal Operation, Newark Field Office, Newark, NJ

2003-2005 CBP Officer (acting Operations Specialist for Border Security)
Department of Homeland Security, U.S. Customs and Border Protection
Office of Field Operations, NewYork, NY

1998-2003 Immigration Inspector
Department of Justice, U.S. Immigration and Naturalization Service
Newark District, Inspections Branch, Newark, NJ

Awards:

2007 Defense Intelligence Agency Award for Outstanding Contribution

2004 U.S. Customs and Border Protection Commissioner's "Anti-Terrorism Award"
U.S. Customs and Border Protection "Unifying Best Practice" Award

2002 U.S Immigration and Naturalization Service Meritorious Award

2000 U.S. Immigration and Nationalization Service Commissioner's Award for
"Excellence in a Group"