Methods and Motives:

Exploring Links between Transnational Organized Crime & International Terrorism

June 23, 2005

This project was supported by Grant No. 2003-IJ-CX-1019 awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. Points of view in this document are those of the authors and do not necessarily represent the official position or policies of the US Department of Justice.

Project Team

Dr. Louise I. Shelley, Principal Investigator
Transnational Crime and Corruption Center
American University
Washington, DC

John T. Picarelli
Transnational Crime and Corruption Center
American University
Washington, DC

Allison Irby
Transnational Crime and Corruption Center
American University
Washington, DC

Douglas M. Hart
Cyberneutics, Inc.
Arlington, VA

Patricia A. Craig-Hart
Cyberneutics, Inc.
Arlington, VA

Dr. Phil Williams
University of Pittsburgh
Pittsburgh, PA

Steven Simon
US National Security Council (1994-1999)
Washington, DC

Nabi Abdullaev
Moscow, Russia

Bartosz Stanislawski
Syracuse University
Syracuse, NY

Laura Covill
Arlington, VA

Acknowledgements

The authors would like to express their sincere gratitude to all of the scholars who helped shape this report. First and foremost is our heartfelt thanks to members of our advisory panel, Bruce Hoffman, Jonathan Winer, Rensselaer Lee III, Spike Bowman, Robert Perito and Todd Stewart. Their attention to detail and extensive feedback throughout the project, and in particular on the contents of this report, have helped the project team immensely. Second, the team would like to thank the two anonymous reviewers from the National Institute of Justice, who again helped the project team to clarify the final report. Third, the team would like to thank Kristen Kowalew of TraCCC for her timely contributions to the project. Finally, and certainly not least, the project team would like to thank NIJ, particularly Jay Albanese and Jennifer Hanley, for their guidance and assistance in seeing this project through to completion.

Abstract

The nexus with transnational organized crime is increasingly a focus for security planners in their analyses of terror groups. Their approach is best described by the phrase "methods, not motives." While the motives of terrorists and organized criminals remain divergent most often, our research indicates this is not always the case. For that reason, this report argues that such a general approach has become too restrictive and can be misleading since the interaction between terrorism and organized crime is growing deeper and more complex all the time. In short, the lines of separation are no longer unequivocal.

The report analyzes the relationship between international organized crime and terrorism in a systematic way in order to highlight the shortcomings of the "methods, not motives" argument. In so doing, the report considers the factors that most closely correspond to crime-terror interaction and identifies those regions of developed and developing states most likely to foster such interactions. Likewise, the paper will suggest an evolutionary spectrum of crime-terror interactions that serves as a common basis for discussion of such often-used terms as "nexus."

The centerpiece of the report is a groundbreaking methodology for analysts and investigators to overcome this growing complexity, identify crime-terror interactions more quickly and to assess their importance with confidence. The approach is derived from a standard intelligence analytical framework, and has already proven its utility in law enforcement investigations.

The report is the product of a recently concluded and peer-reviewed 18-month NIJ-sponsored research project, and includes empirical evidence drawn from numerous case studies developed in the course of the research program.

Executive Summary

Scholars of transnational organized crime view the events of September 11th and subsequent terrorist plots as confirmation that criminal groups have eclipsed state actors as the most malignant opponents of the nation state. In the 1990s, experts largely concurred that a convergence of international terrorism and transnational organized crime might take place. Shrewd investigators noted marked similarities in the behavioral and operational methods of both terrorists and organized criminals. Yet they saw no reason to change their long-held view that different goals – personal profit for criminals and political upheaval for terrorists – would keep the two types distinct. Both law enforcement and intelligence continued, therefore, to rely on the established maxim of examining 'methods, not motives' in attempts to observe and identify the two criminal types.

Research conducted by the authors of this report suggests that this is too narrow a view. We support the notion that terrorists and criminals often use the same methods, most often for divergent motives—but not always. Indeed, this report identifies and analyzes the points of convergence between organized criminals and terrorists to draw useful conclusions for investigators.

In some cases, the terrorists simply imitate the criminal behavior they see around them, borrowing techniques such as credit card fraud and extortion in a phenomenon we refer to as activity appropriation. This is a shared approach rather than true interaction, but it often leads to more intimate connections within a short time. This conclusion is not widely shared in the U.S. law enforcement and intelligence community: the National Intelligence Council found in its recent report that organized criminal groups are 'unlikely to form long-term strategic alliances with terrorists.'[1]

To understand what happens next, we point to the situation in regions of the world where combinations of poor governance, ethnic separatism and/or a tradition of criminal activity that are most likely to support crime-terror interactions—such as failed states, war regions, penal institutions and some neighborhoods of urban centers.

Once terrorists and other criminals begin to work together, they have moved beyond activity appropriation to a different, closer, form of interaction. We have devised an evolutionary system showing five different stages in the terror-crime relationship. This linear scale is termed the terror-crime interaction spectrum.

Starting by borrowing each other's methods (activity appropriation), terror and crime groups naturally begin to buy and sell services and goods from each other instead. Clearly, it is more efficient to outsource a service - such as passport forgery - to an established specialist than to try and master the necessary techniques yourself. These business relationships, which we term nexus, tend to be focused on individual

transactions and may not persist beyond the short term. The next stage of convergence is a natural progression from that point: the two groups begin working together more regularly and begin to share each other's goals as well as working methods. This stage is called a symbiotic relationship.

As we describe in detail in this report, regions such as Chechnya and the Tri-Border area of Paraguay, Brazil, and Argentina are so saturated with all kinds of organized crime as well as terrorist activity that it is often difficult, not to say meaningless, to draw a distinction between groups. Many individuals belong to both terror and organized crime groups, and conduct a variety of tasks for both. In those circumstances, the process of convergence continues until the two groups become one, which we refer to as a hybrid group. Organized crime and terrorism are more or less equally important to the group, which after all needs to commit fraud, extortion and other staple activities of organized crime in order to fund its terror operations. In a few cases, a hybrid group becomes fixated so keenly on one activity that it drops the other altogether. This process is called transformation. We emphasize, however, that while convergence is a dynamic process, many terror-crime links do not ever progress to close cooperation, let alone merger. Indeed, close proximity does not even guarantee that crime and terror groups with collaborate. The true utility of the terror-crime interaction spectrum is to suggest the possibilities to investigators and analysts and to ensure that they understand the use of terms like "nexus" and "hybrid" throughout the text of the report.

Using this basis, the next stage for investigators is to organize all available information and data about a crime or terrorist group. Acknowledging that almost all investigators have access to a mass of data, but lack effective means to analyze it, we propose a methodology that identifies and eliminates irrelevant avenues of enquiry. Drawing on a venerable military intelligence method called intelligence preparation of the battlefield (IPB), the proposed method, preparation of the investigation environment (PIE), allows investigators to identify the areas where terrorism and organized crime are most likely to interact. Such areas are expressed not only in geographic but notional terms as well. For example, the report identifies the way groups organize themselves, communicate, use technology, employ their members and share cultural affinities as loci of overlap. Within each of these areas, herein referred to as watch points, investigators can then identify specific indicators that suggest whether or not cooperation between known terrorists and a specific criminal group is actually taking place.

These new models have wholly practical objectives: to assist law enforcement and intelligence personnel in their constant struggle to make best use of the information available, and thus apprehend criminals as early as possible. This report contains three detailed case studies of regions that are hospitable to crime-terror interactions– Chechnya, the Black Sea region, and the Tri-Border Area mentioned above. We de-

scribe the environment that facilitates interaction between crime and terror, and then suggest indicators that help determine whether and how those links work in practice. The report also includes two examples of how TraCCC has implemented the PIE approach in its own research and analysis.

We conclude that the fight against terrorism is being undermined by a critical lack of awareness about terrorists' links with organized crime. Crime analysis must be central to understanding the patterns of terrorist behavior and cannot be viewed as a peripheral issue. Furthermore, resources taken away from the transnational and organized crime arena in the post 9/11 era are giving criminals a greater chance to operate and even provide services to terrorists.

Our central recommendation is therefore to incorporate crime analysis in the work of intelligence analysts and law enforcement officers addressing terrorism. A methodology such as PIE would be suitable for that purpose.

Other recommendations are that the business community should work more closely with law enforcement to detect patterns and methods of organized crime, since so many crimes fund terrorism. More detailed analysis of the operation of illicit activities around the world would help advance an understanding of terrorist financing. Corruption overseas, which is so often linked to facilitating organized crime and terrorism, should be elevated to a U.S. national security concern with an operational focus. A joint task force composed of analysts from the FBI, Department of Homeland Security and Federal intelligence agencies should be formed immediately to create an integrated system for data collection and analysis. Finally, a broader view of today's terrorist and criminal groups is needed, given that their methods and their motives are often shared. The ultimate test of this will be greater effectiveness in observing, detecting, and apprehending politically and economically motivated criminals that undermine the security of the United States and other nations.

Table of Contents

We expect that the relationship between terrorists and organized criminals will remain primarily a matter of business, i.e. that terrorists will turn to criminals who can provide forged documents, smuggled weapons, or clandestine travel assistance when the terrorists cannot procure these goods and services on their own. Organized criminal groups, however, are unlikely to form long-term strategic alliances with terrorists. --*Mapping the Global Structure*, Report of the National Intelligence Council's 2020 Project, National Intelligence Council, Washington, December 2004, p. 96

There is strong evidence of Al Qaeda's ties to the African diamond trade, despite the reluctance of some in the U.S. intelligence community to acknowledge the link. --Douglas Farah, author of *Blood from Stones: The Secret Financial Network of Terror*, testifying before the U.S. House Subcommittee on Oversight and Investigations, Committee on Financial Services, Hearing of Terrorist Financing, February 16, 2005

No responsibility of the United States Government is more urgent than combating the networks of Islamic extremists who have embraced terrorism as a weapon without limits against secular government. The country's ability to detect and deter acts of terror is a crucial policy concern to all Americans.

Despite the many successes in detecting terrorist activities, and even averting them at an early stage, U.S. intelligence and law enforcement are failing to make vital deductions. Although it is well known that terrorists have affiliations with organized crime, little attention has been given to those links. Their significance has been underestimated. Consequently, information that could lead to earlier detection of some terrorist groupings, plans, and operations, has been inadequately analyzed and integrated by counter-terrorist investigators. Better understanding of the links between the two groups, areas of overlapping activities, personnel, and service provides, could enhance current counter-terrorist efforts and facilitate earlier detection of a wider range of potential terrorist threats.

1. Introduction

> It was twilight on a cold day in mid-December 1999 as the Canadian ferry docked at Port Angeles, WA. The last vehicle to approach U.S. Customs Inspector Diana Dean was an unremarkable green Chrysler 300M. The fact that the male driver was alone raised a small question in her mind. And when her routine questions got some attitude from the French-speaking Canadian, Agent Dean sent the vehicle and driver into secondary inspection. A few minutes later, the man had made a run for it, pursued by three agents through this quiet border town some sixty miles west of the main highway between Seattle and Vancouver. The customs officials thought they were dealing with a drug smuggler. In fact, the car was carefully packed with explosives. Dean and her colleagues were about to uncover an Al Qaeda plot to bomb Los Angeles International Airport during America's millennium celebration. Ahmed Ressam and others he implicated were ultimately convicted of terrorist offenses, providing important information about other terrorist plots against America. The subsequent investigation revealed that warnings by European police, along with vital evidence about the perpetrators' involvement in organized crime, had been disregarded by law enforcement on this side of the Atlantic. Had the authorities made connections based on what they already knew about that criminal activity, this terrorist plot would never have progressed so far.

Like Diana Dean, any law enforcement officer might easily mistake one type of criminal for the other.

After all, there are striking similarities between terrorists and individuals engaged in organized crime. Both criminal types commit fraud, theft, forgery, and violent street crime. Both traffic in drugs and human beings. Both extort, intimidate, and bribe. Both do business in the legitimate economy, too. Both use subterfuge to conceal their real purpose. Granted, their motives appear different: organized crime focusing on making money and terrorism aiming to undermine political authority. But the perpetrators have similar profiles, and are often the same individuals.

Three years after the war on terror began, investigators are taking careful note of how terrorists use the resources and the methods of organized crime to prepare attacks. At a practical level, security planners are increasingly aware of the ways in which terrorists and organized crime cooperate, such as terrorists' involvement in money laundering and narcotics trafficking. But they fail to analyze that interaction in order to detect terrorists' planning.

Existing academic work has provided some foundation for further analysis of these links. During the 1990s, some scholars argued that a convergence between international terrorism and transnational organized crime would prove detrimental to national security and would require new techniques and tools to combat. What did not occur was any systematic study of the cooperative arrangements between those criminal and terrorist groups.

'Methods, not motives' has long been a maxim for analysts investigating links between organized crime and terrorism,[2] on the grounds that while terrorists might share the methods of other criminals, their

motives are quite different. We argue in this report that this general approach has become too restrictive and can be misleading.

The interaction between terrorism and organized crime is growing deeper and more complex all the time. First, transnational criminal groups are expanding, both through the addition of new groups and the growth of existing ones. Such growth led to more connections between these groups as well as with other shadowy actors like insurgents, arms proliferators and indeed terror cells. For example, as gangs have evolved into the newest transnational crime groups in North America,[3] stories have recently surfaced that an Al Qaeda operative made contact with members of one gang, Mara Salvatrucha or MS-13, in Honduras in 2004.[4] Terrorists in European prisons recruit criminals to their cause, allowing incarcerated individuals move between their identities as terrorists and criminals.[5]

Second, the dealings between terrorist and organized crime groups have long since ceased to be a matter of business alone; the two phenomena now intersect on many different levels. Many international terrorists sustain themselves only with the support of organized crime. That dependency, combined with the fact that terrorists commit a range of relatively minor crimes too, can be important keys to detecting and apprehending them.

With so many individuals active in both terrorism and organized crime, there now exists a merging and blurring of functions. Crucially, the distinctions between the two types are particularly unclear in developing countries, in prisons and conflict zones where there is no effective government.

Our research indicates that organized crime tends to flourish most when groups in society see their own interests as separate from that of the system of governance, and the norms promulgated from that system. They flourish where the standards of law enforcement are low and there is limited respect for the law and legal authority. They also flourish where local law enforcement, such as in many developed communities, cannot successfully police ethnic subcommunities within the larger community or ignore the relations that form in penal institutions. Thus, enclaves of homogeneous ethnic minority groups are commonly vulnerable to becoming a host for organized crime in democracies, and in less democratic countries, many other groups may see independent action as more in their self-interest than playing by the rules, and as morally justified due to what they see as lack of legitimacy in the rule class and institutions.[6] In conflict zones and certain urban areas, for example, criminals are less constrained by respect for the political system and the rule of law, less intimidated by regulation and law enforcement, and often motivated by a desire to subvert or disregard the established order. It comes as no surprise that the cooperation between crime and terror is growing rapidly in conflict zones where there is no effective governing state. But it is

also growing in the heart of many major cities or penal institutions in democratic societies where subgroups do not share the norms of the larger society.

Patterns of criminal behavior generated overseas are transferred to the U.S. through U.S.-based cells of foreign terror groups and tend to persist once transferred. For example, Hezbollah involvement in cigarette trafficking observed first in the tri-border area in Latin America was subsequently prosecuted in North Carolina. Chechen involvement in the sex industry in Russia has been noted by Los Angeles law enforcement.

In developing countries, criminals and terrorists tend to spawn more collaborative relationships that are closer knit, whereas in the developed world, organized crime is more likely to co-exist with terrorism through arm's length business transactions. Terrorists in developed countries may, however, use crime to support their activities.

Terrorism investigators at U.S. federal, state, and local agencies are naturally inclined to focus on evidence of possible attacks in the United States, or the activities of groups operating overseas that are known to be hostile to the U.S. Yet the evidence given above suggests that a study of the structure and nature of this cooperation overseas is no less relevant. Indeed, it may be more fruitful than avenues of investigation focused too narrowly on the United States.

This report analyzes the relationship between international organized crime and terrorism systematically in order to translate research into practice. While the report does not go so far as to state that terrorists and organized criminals share the same motives and methods and thus completely repudiate "methods, not motives," the report will demonstrate that the lines of separation are far from unequivocal. Indeed the dominant pattern remains—crime groups collaborating with terror groups in committing illicit activities without adopting the latter's objectives. However, the report does identify circumstances where this pattern does not hold true. Likewise, while profits from criminal activities remain predominantly a means for terror groups to accomplish their objectives, it has not limited terror groups from establishing or tapping cells that specialize in using organized crime to garner profits and provide logistical support.

As such, the report's focus on complexity should not be mistaken as jettisoning the basic truths of the "methods, not motives" argument. The report does not support broad statements such as "most organized criminals are becoming terrorists" or that terror groups and crime groups are fusing into a seamless web. Rather, this report is a clarion call for a new approach to coping with the complexities represented in the evolving relationships between organized crime and terrorism and their increasing intersection.

In translating this knowledge into praxis, we propose a methodology for evaluating crime-terror interaction both in terms of organizational structure and operations. Our aim is to offer practical tools and

recommendations for U.S. intelligence and law enforcement. The centerpiece of this report is a method that analysts and investigators can use, with or without information technology, both to shorten the efforts needed to locate crime-terror interactions and to assess their importance to the efforts to fight terrorism and organized crime.

The report is broken into several sections. The opening section is a discussion of the terms of reference for the report, the goals of the report and the methods by which we arose at our conclusions. The next section provides an overview of our approach to finding and assessing crime-terror interaction, dubbed Preparation of the Investigation Environment or PIE. Following that is a section that reviews the numerous approaches to the evolution of the crime-terror relationship to explain the meaning of our frequently used terms like "nexus" (i.e. an ontology). The remaining sections consider how PIE has led the authors to focus more attention on areas like conflict zones, penal institutions and certain urban areas. We also deconstruct the PIE approach into watch points and indicators of crime-terror interaction. Applying these PIE's watch points and indicators to three diverse case studies revealed a wealth of information concerning crime-terror interactions. The conclusion of the report considers the implications for the PIE approach for practitioners and policymakers alike.

2. Methodology

2.1. Terms of reference

It is easiest to think about terrorism and organized crime when they are personified by well-known groups: Al Qaeda and La Cosa Nostra; the IRA and the Yakuza. But a crucial argument underlying this study is that both categories of behavior are broader and less easy to classify than are these discrete groups. Terrorism and organized crime are also activities. These are labels for fraudulent or destructive criminal behavior by individuals who may otherwise use legitimate means to make a living and pursue their interests. Some terrorists are also legal employees of a corporation, many gangsters engage in legitimate businesses. Moreover some individuals engage in both terrorism and organized crime.

Distinguishing between organized criminal groups and organized crime has important implications. It means that an overlap in transnational organized crime and terrorism can occur without any cooperation between two groups. Some of the most serious terrorism cases detected have not involved organized crime groups at all – the terrorists have acted alone using the methods of organized crime. Similarly, a terror group may traffic drugs to fund its campaign of violence, but it remains first and foremost a terrorist organization. Involvement in the drug trade simply increases the group's operating risk and makes it more vulnerable to detection by law enforcement.

In preparation for the work on this report, we reviewed a significant body of academic research on the structure and behavior of organized crime and terrorist groups. By examining how other scholars have approached the issues of organized crime or terrorism, we were able to refine our methodology. This novel approach combines a framework drawn from intelligence analysis with the tenets of a methodological approach devised by the criminologist Donald Cressey, who uses the metaphor of an archeological dig to systematize a search for information on organized crime.[7] All the data and examples used to populate the model have been verified, and our findings have been validated through the rigorous application of case study methods.

While experts broadly accept no single definition of organized crime, a review of the numerous definitions offered identifies several central themes.[8] There is consensus that at least two perpetrators are involved, but there is a variety of views about the way organized crime is typically organized as a hierarchy or as a network.[9] Organized crime is a continuing enterprise, so does not include conspiracies that perpetrate single crimes and then go their separate ways. Furthermore, the overarching goals of organized crime groups are profit and power. Groups seek a balance between maximizing profits and minimizing their own risk, while striving for control by menacing certain businesses. Violence, or the threat of violence, is used to enforce obligations and maintain hegemony over rackets and enterprises such as extortion and narcotics

smuggling. Corruption is a means of reducing the criminals' own risk, maintaining control and making profits.

It is striking, however, that three significant aspects of organized crime in the 2000s are generally ignored in these definitions. Most writers focus on organized crime as a domestic entity with peripheral links to cross-border illicit transactions. They take a limited view of organized crime as an organization, such as the Genovese family of New York or Chinese Triads. In doing so they overlook the fact that organized crime is also an activity such as narcotics smuggling or extortion. Finally, few definitions challenge the common view of organized crime as a 'parallel government' that seeks power at the expense of the state but retains patriotic or nationalistic ties to the state. This report takes up that challenge by illustrating the rise of a new class of criminal groups with little or no national allegiance. These criminals are ready to provide services for terrorists as has been observed in European prisons.[10]

We prefer the definition offered by the UN Convention Against Transnational Organized Crime, which defines an organized crime group as "a structured group [that is not randomly formed for the immediate commission of an offense] of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences [punishable by a deprivation of liberty of at least four years] established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit."[11] This definition is precise and comprehensive. It implies that at least three people are involved in a criminal activity sustained and repeated over a period of time. The rationale of organized crime is to make profits. The definition covers transnational crime groups - which we define as criminal enterprises that extend across national borders - and is not limited to argument about 'parallel governments'. Finally, it also encompasses numerous forms of organized crime while excluding petty crime or one-time conspiracies from organized crime.

A related concept that features prominently in this report is the shadow economy, which has been defined as economic transactions outside the view of government regulators.[12] Obviously, illicit and criminal activities are included in this category, but the shadow economy is a broader term. Mark Galeotti, among others, shows how legitimate businesses and individuals can operate in the shadow economy, such as by evading taxes or making corrupt payments to secure business contracts.[13] Some scholars take the view that a global shadow economy already exists, but we prefer the notion of a number of shadow economies, in the same way that macroeconomists use the global economy, comprising markets, sectors and national economies, as their basic unit of reference.

As with organized crime, there is no consensus about the definition of terrorism. Alex Schmid and Walter Laqueur have both conducted detailed analyses of the various attempts to define terrorism, show-

ing how these definitions have evolved over time.[14] Drawing on these studies and others, the terrorism scholar Bruce Hoffman has offered a comprehensive and useful definition of terrorism as *the deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change.*[15] Hoffman's definition offers precise terms of reference while remaining comprehensive; he further notes that terrorism is 'political in aims and motives,' 'violent,' 'designed to have far-reaching psychological repercussions beyond the immediate victim or target,' and 'conducted by an organization with an identifiable chain of command or conspiratorial cell structure.' These elements include acts of terrorism by many different types of criminal groups, yet they clearly circumscribe the violent and other terrorist acts. Therefore the Hoffman definition can be applied to both groups and activities, a crucial distinction for this methodology we propose in this report.

The TraCCC team also recognized that examining all terror groups could lead to the production of conclusions that are not of utility for practitioners. As a number of terrorism experts conveyed to the team, circumscribing the universe of terror groups to those that threaten US interests and the US homeland aligns this study and its conclusions on the requirements and interests of our intended audience. While no list is likely ideal or perfect, the team found that the best expression of this pared list of groups is found in the US State Department's annual posting of Foreign Terrorist Organizations.[16] The list consists of terror groups that meet the criteria Hoffman lays out and, by definition, meet the criteria of threatening US homeland security.

2.2 Prior scholarly analysis of organized crime and terror

A number of academic scholars have engaged the topic of crime-terror cooperation. In constructing our model and approach, we chose to build on their valuable work, seeking to re-evaluate their findings while learning from their analysis.

By and large, the TraCCC team was able to loosely group these prior scholarly analyses of crime and terror interactions into several categories. There are historical studies that examine the links between terrorism and crime among the anarchists, the Bolsheviks and crime.[17] Next are those studies that focus on crime-terror interactions in the specific context of the international market for narcotics. Early identification of terror-crime cooperation occurred in the 1980s and focused naturally on narcoterrorism, a phrase coined by Peru's President Belaunde Terry to describe the terrorist attacks against anti-narcotics police in Peru. The criminologist Rachel Ehrenfeld advanced this theory significantly when she highlighted the growing connection between narcotics smuggling and terrorism. Her analysis showed why separate groups, motivated either by profit or by politics, might coalesce or cooperate.[18] More recently Ekaterina Stepanova,

a senior researcher at the Russian Academy of Sciences, completed a volume that explores the link between the illegal narcotics trade and terror groups in three different regions – Latin America, Central Asia, and the Golden Triangle.[19] Stepanova concludes that the links between narcotics trafficking and terror groups exist in many regions of the world but that it is difficult to make generalizations about the terror-crime nexus.

The extension of narcoterrorism studies may have inadvertently circumscribed analysis of crime-terror interaction. For example it is difficult to extend Stepanova's conclusions is outside the realm of narcotics since, as this report later demonstrates, terror groups interact or intersect with organized crime in other criminal enterprises that bear little resemblance to narcotics trafficking, such as document fraud. Likewise, Ehrenfeld's more recent publications reflect much the same limitations, positing that the only ties between terrorists and criminals are to be found in the drug trade and thus the main conduit of crime-terror interaction is financial in nature.

International relations theorists have also produced a group of scholarly works that examine organized crime and terrorism (i.e. agents or processes) as objects of investigation for their paradigms. While in some cases, the frames of reference international relations scholars employed proved too general for the purposes of this report, the team found that these works demonstrated more environmental or behavioral aspects of the interaction. That is, transnational crime and terrorism are malevolent non-state actors that exploit failures in a state-centric global system, such as the limitations of sovereignty, legal jurisdictional boundaries and the safe havens that failed or weak states represent. James Rosenau discusses crime-terror cooperation as an example of a changed world order, one in which non-state actors and individuals are of growing importance.[20] Maryann Cusimano-Love sees organized crime and terrorism as two examples of international problems that require public-private partnerships to solve.[21] Others including Manuel Castells as well as John Arquilla and David Ronfeldt examine the networked nature of organized crime and terrorism as a significant factor in their likelihood to cooperate.[22] Likewise, the international relations scholar Susan Strange defines zones of ungovernability as the 'retreat of the state' from both globalization and non-state actors. Strange devotes a chapter to the role of organized crime in the process, which she summarizes as when national governments are weak and criminals are rich, something close to civil war erupts.[23] Following on this theme, Erik Scott applies Mary Kaldor's conceptual framework of a globalized war economy to the Republic of Georgia in order to highlight how different types of malevolent non-state groups have coalesced in defined geo-economic regions (e.g. Ossetia) to further their interests.[24] Finally, works by Saskia Sassen, James Mittelman, and Moíses Naim each argue that the forces of globalization have empowered both organized crime and terrorism, which they call the 'dark side of globalization'.[25]

Finally, a number of scholars have set out to contribute insights into the nature of interactions between organized crime and terrorism. The works of Tamara Makarenko provide a linear model for different forms of crime-terror cooperation, offer reasons for each group to cooperate within each given form, and even introduce the notion of shifting between the different forms.[26] The work of R.T. Naylor has likewise suggested an evolutionary pattern between criminals and terrorists. Another important contribution comes from Chris Dishman, who outlines a process of transformation by which terror groups morph into entities that are 'political by day but criminal by night'.[27] Phil Williams conducted one of the more detailed analyses, focusing on three cooperative models of transnational criminal and terrorist groups. These are, first, convergence into a singular phenomenon, second, collusion with one another, and third, influence on an operational approach, such as when organized crime groups adopt terror-bombing campaigns to force concessions. Williams concludes that short-term convergent and divergent episodes between the two were more likely than a longer-term nexus or cooperative relationship.[28]

A theme that figures prominently into these and other examinations of the links between organized crime and terrorism is that these groups use similar methods for divergent motives. Naylor puts this phenomenon succinctly:

> A world of difference exists between the motives of insurgent versus criminal groups. Criminals commit economic crimes to make money. The buck, so to speak, stops there. But to an insurgent group, money is merely a tool—one that is necessary but not sufficient to achieve the group's goals.[29]

Shelley and Picarelli explored the implications of this 'methods not motives' argument, concluding that the framework is too general for investigators and analysts to employ in the construction and prosecution of cases.[30] Schmid's exhaustive criminological comparison of organized crime and terrorism used the lenses of organizational structure, modus operandi and risk assessment to arrive at much the same conclusion.[31] Furthermore, the framework overstates the complexity of crime-terror interactions, oftentimes limiting such interactions to the financial realm and dismissing evidence that the goals of crime and terror groups have coalesced in the past. While the argument was a good starting point, Shelley and Picarelli concluded that substantial research was required to reveal the numerous connections between crime and terrorism.

2.3 Data collection

Much of the information in the report that follows was taken from open sources, including government reports, private and academic journal articles, court documents and media accounts. Andrew Silke,[32] updating Schmid and Jongman's 1988 survey of data sources found in terrorism research,[33] notes that open

source documents remain the dominant form of data for scholars. We acknowledge Silke's two major concerns: that open sources, particularly media sources, may be inaccurate, and may contain bias of one form or another.

To ensure accuracy in the collection of data, we adopted standards and methods to form criteria for accepting data from open sources. In order to improve accuracy and reduce bias, we attempted to corroborate every piece of data collected from one secondary source with data from a further source that was independent of the original source — that is, the second source did not quote the first source. Second, particularly when using media sources, we checked subsequent reporting by the same publication to find out whether the subject was described in the same way as before. Third, we sought a more heterogeneous data set by examining foreign-language documents from non-U.S. sources. We also obtained primary-source materials such as declassified intelligence reports from the Republic of Georgia, that helped to clarify and confirm the data found in secondary sources.

The second source of data was interviews. We conducted dozens of interviews with government officials and private experts in the United States, Canada, the U.K., Ireland, the former Soviet Union and other countries to verify data discovered in secondary sources, obtain information relevant to the project goals, and to refine the recommendations we make based on the research. Since all these meetings were confidential, it was agreed in all cases that the information given was not for attribution by name.

Our final data source was ethnographic studies of crime-terror cooperation in three regions—the countries adjoining the Black Sea, the Russian Caucasus, and the Tri-Border Area bordering Paraguay, Brazil and Argentina. For each of these studies, researchers traveled to the regions a number of times to collect information. Their work was combined with relevant secondary sources to produce detailed case studies presented later in the report. The format of the case studies followed the tenets outlined by Robert Yin, who proposes that case studies offer an advantage to researchers who present data illustrating complex relationships – such as the link between organized crime and terror.[34] According to Yin, employing the case study method is most appropriate when the research question begins with how or why, when the study cannot control for behavioral events, and when the study focuses on contemporary events. Clearly, this study meets all three criteria, studying contemporary topics over which the team has no control while asking two central questions: why and how do crime and terror groups cooperate?

2.4. Research goals

This project aimed to discover whether terrorist and organized crime groups would borrow one another's methods, or cooperate, by what means, and how investigators and analysts could locate and assess crime-

terror interactions. This led to an examination of why this overlap or interaction takes place. Are the benefits merely logistical or do both sides derive some long-term gains such as undermining the capacity of the state to detect and curtail their activities?

In an attempt to identify how and why international criminal and terrorist groups cooperate, we devised a methodology to evaluate the forms this cooperation takes, both in terms of organizational structures and operating procedures. The TraCCC team arrived at our methodology, preparation of the investigative environment (PIE), by adapting a long-held military practice called intelligence preparation of the battlespace (IPB). The IPB method anticipates enemy locations and movements in order to obtain the best position for a commander's limited battlefield resources and troops. The goal of PIE is similar to that of IPB—to provide investigators and analysts a strategic and discursive analytical method to identify areas ripe for locating terror and crime interactions, confirm their existence and then assess the ramifications of these collaborations. The PIE approach provides twelve watch points within which investigators and analysts can identify those areas most likely to contain crime-terror interactions. Indicators within each watch point assist analysts to look for data that suggest tangible crime-terror interactions, such as communications between a known criminal and a known terrorist. As analysts and investigators undertake the construction of a case, they can use PIE to frame further investigation in a way that assesses the data—either confirming that collaboration exists or dismissing the initial data as idiosyncratic.

The PIE methodology was designed with the investigator and analyst in mind, and thus PIE demonstrates how to establish investigations in a way that expend resources most fruitfully. The PIE methodology shows how insights can be gained from analysts to help practitioners identify problems and organize their investigations more effectively. When coupled with the fact that there is an increasing volume of structured data on terrorist incidents, smuggling attempts, movement of persons and other attendant areas in both secure and open formats, the latter specifically in the large databases being constructed by the University of Maryland, the Monterey Institute of International Studies and the RAND Corporation among others, the project team found that this approach can be automated through the use of software for analysts and investigators. The Appendix discusses how analysts and investigators can deconstruct PIE into steps of analysis that available commercial semi-automated software tools can assist. The approach can also be adapted to meet the constantly changing nature of the two organizational types and their shared links. Ultimately, the methodology aims to provide practical tools and recommendations for U.S. law enforcement, homeland security, and intelligence at federal, state, and local level.

2.5. Research challenges

Our first challenge in investigating the links between organized crime and terrorism was to obtain enough data to provide an accurate portrayal of that relationship. Given the secrecy of all criminal organizations, many traditional methods of quantitative and qualitative research were not viable. Nonetheless we conducted numerous interviews, and obtained identified statements from investigators and policy officials. Records of legal proceedings, criminal records, and terrorist incident reports were also important data sources. As mentioned earlier, we also acquired further primary-source data--declassified specifically for our analysis--from law enforcement and intelligence in the United States, several South American countries, and the Republic of Georgia. To corroborate and assess the primary materials, we also interviewed experts in law in law enforcement, intelligence, policy, and academia, in the United States and other countries.

The strategy underlying the collection of data was to focus on the sources of interaction wherever they were located (e.g. developing countries and urban areas), rather than on instances of interaction in developed countries like the September 11th or the Madrid bombing investigations. In so doing, the project team hoped to avoid characterizing the problem "from out there." For example, one shortcoming of Naylor's approach to crime-terror interaction in *Wages of Crime* cites no primary ethnographic studies or interviews to corroborate media and scholarly references; the focus is uniquely that of an individual in a developed country.

We chose to use case studies drawn from developing and transitional countries to provide concrete examples of the relationships between terrorism and organized crime in order to provide an analytical perspective that is not often represented by looking at singular cases—a fact that the contesting quotes that opened this report illustrate in their examination of the financing of Al Qaeda. All three case studies highlight patterns of association that are particularly visible, frequent, and of lengthy duration. Because the conflict regions in the case studies also contribute to crime in the United States, our view was these models were needed to perceive patterns of association that are less visible in other environments. A further element in the selection of these regions was practical: in each one, researchers affiliated with the project had access to reliable sources with first-hand knowledge of the subject matter. Our hypothesis was that some of the most easy to detect relations would be in these societies that are so corrupted and with such limited enforcement that the phenomena might be more open for analysis and disclosure than in environments where this is more covert.

3. A new analytical approach: PIE

Investigators seeking to detect a terrorist activity before an incident takes place are overwhelmed by data. Pieces of evidence that might have been useful in detecting the Al Qaeda attacks of Sept. 11, 2001 in advance were held in a queue waiting for translation from Arabic. Since that date, the drastic increase in controls and checks on suspicious activity by the authorities in the United States has burdened investigators with a huge new mass of potential evidence.

From speaking to a wide spectrum of analysts and investigators concerned with potential collaborations between organized crime and terrorism, the TraCCC team learned that what was most urgent was the development of a strategic analytical method that focused on crime-terror interactions using more than one intelligence data source, like financial information. Interviews that the TraCCC team conducted with experts from U.S. and foreign government agencies, think tanks and universities all provided versions of this theme, most often noting the importance of escaping the exclusivity of "following the money" and devising a method that utilizes other sources of existing data like criminal activities and the movement of persons across international borders. A counterterrorist analyst at the Central Intelligence Agency took this further, noting that the discovery of crime-terror interactions was often the accidental result of analysis on a specific terror group, and thus rarely was connected to the criminal patterns of other terror groups. Finally, discussions with analysts from the National Security Agency, the Department of Defense, the Department of Homeland Security and elsewhere revealed little to no collective effort to assess the interaction of crime and terror groups in a systematic or strategic way.

The TraCCC team thus set out to formulate and evaluate a strategic analytical method rooted in a wide breadth of information and subject matter that simultaneously avoids overloading the analyst with complexity. Various techniques have been devised to whittle down and organize the data, but more fundamental approaches are still keenly required. Rather than simply organizing data more efficiently, investigators need analytic techniques to reduce the time spent locating potential interactions and by focusing their activities earlier on the most relevant evidence about the activities of terror and crime groups.

An approach that has long been the standard for such requirements in the military intelligence area is *intelligence preparation of the battlespace*. IPB enables commanders to make both tactical and strategic decisions. By examining known facts about an adversary (such as the speed of its vehicles), IPB seeks to determine what is not known about that adversary (such as the range of its future movements). The aim is of course to determine the enemy's most likely next move.

IPB is an attractive basis for analyzing the behavior of criminal and terrorist groups because it focuses on evidence about their operational behavior as well as the environment in which they operate. This evi-

dence is plentiful: communications, financial transactions, organizational forms and behavioral patterns can all be analyzed using a form of IPB.

The project team adapted IPB to provide search routes through the thicket of evidence about organized crime that in turn translated into specific indicators of cooperation with terrorists.

Thus the project team has devised a methodology based on IPB, which we have termed *preparation of the investigation environment*, or PIE. We define PIE as a concept in which investigators and analysts organize existing data to identify areas of high potential for collaboration between terrorists and organized criminals in order to focus next on developing specific cases of crime-terror interaction—thereby generating further intelligence for the development of early warning on planned terrorist activity.

While IPB is chiefly a method of eliminating data that is not likely to be relevant, our PIE method also provides positive indicators about where relevant evidence should be sought. The PIE process therefore not only analyzes evidence to suggest areas where these two types of groups might collaborate, but also uses indicators to frame physical, electronic, and data surveillance in such a way as to focus on specific collaborations.

3.1 The theoretical basis for the PIE Method

Despite significant challenges, criminologists and other scholars have devised methods for examining organized crime and terrorism. These methodologies are complicated given the covert nature of criminal groups and the need for intelligence and law enforcement agencies to withhold some data from public view.

Donald Cressey's famous study of organized crime in the U.S., with the analogy of an archeological dig, was the starting point for our model of crime-terror cooperation.[35] As Cressey defines it, archeologists first examine documentary sources to collect what is known and develop a map based on what is known. That map allows the investigator to focus on those areas that are not known—that is, the archeologist uses the map to focus on where to dig. The map also serves as a context within which artifacts discovered during the dig can be evaluated for their significance. For example, discovery of a bowl at a certain depth and location can provide information to the investigator concerning the date of an encampment and who established it.

A crucial reason for characterizing the interaction between criminal and terrorist groups is to provide law enforcement and intelligence agencies with actionable information. This data helps focus investigations, improve warning time, and reveal vulnerabilities. Military and intelligence analysts have long used the

IPB technique to accomplish these goals in their area of interest, and the TraCCC team saw an opportunity to employ IPB in a new sphere of analysis.

The U.S. Department of Defense defines IPB as an analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive database for each potential area in which a unit may be required to operate. The database is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form.[36] Alongside Cressey's approach, IPB was selected as a second basis of our methodological approach.

The goal of IPB is to identify how geography and man-made features limit the space available for military operations. Since ancient times, military operations on land have been confined to less than ten percent of the Earth's surface. Sea-based conflict is even more constrained, with the vast majority of sea battles taking place in coastal waters. In reality, major battles of history have taken place within an even narrower area, with many encounters clustered within a small area and even recurring many times on the same spot.[37]

IPB analyzes and models terrain, vehicular characteristics, and operational behavior to determine the most likely course of enemy action at various stages of a military operation. For example, an IPB analysis might note that robust lines of communication and flat open terrain are useful avenues for an opponent to advance using tanks and heavy transports. But the absence of hills, trees, and other natural cover along those same avenues would render an opponent open to an aircraft attack, and thus would make these avenues less attractive to an opponent. Thus the IPB analyst might recommend that commanders focus their attention on roads through wooded areas that provide such cover.

In the pre-computer age, IPB analyses consisted of a paper map upon which was overlaid with several layers of acetate film. Marked on each layer were the areas that were off-limits because of particular geographic, technical, or doctrinal constraints such as swamps or thick forests. The complete set of markings could then be glimpsed through the layers of film, revealing the unmarked areas where military engagement was still viable. These were termed *named areas of interest*.

This method was highly labor-intensive, however. Most IPB analyses were conducted once, and updated annually, if at all. Starting in the 1980s IPB was transferred to computer systems, which allowed more flexible planning that could be adapted and updated at will. Software was written that automatically placed movement corridors and launch positions onto the map. Databases captured various forms of enemy operational behavior and further segmented the battlespace. Increasingly inexpensive computing power and improved software tools to aid analysts made it possible to update IPB much more frequently

and thus made IPB a more dynamic process. Automated IPB has emerged as a very powerful tool for linking intelligence to military units in the 2000s, particularly in Afghanistan and Iraq.

IPB is a powerful investigative methodology for use against adversaries who are not military units, but instead engaged in transnational crime and terrorism. That value lies in the scheme's ability to identify the space in which where criminals might cooperate, using a combination of operational behavior and characterizations of the environment. Those characteristics include communications, financial transactions, organizational forms and behavioral features. By applying an IPB-like methodology, which we have termed *preparation of the investigation environment* (PIE), we can identify areas where the two entities can be expected to meet, and then develop indicators that suggest whether this has actually occurred.

Named areas of interest identified using conventional IPB are highly likely to see military operations at some point during a campaign. They provide a focus on areas of the battlespace that will probably host large numbers of enemy forces, and which must be placed under surveillance and disrupted at very short notice. The status and location of named areas of interest are crucial to military planning and execution. In the same way, PIE identifies areas where terror and organized crime are highly likely to meet, which we term *watch points*.

With the help of PIE, analysts can identify watch points that are highly specific and limited to certain locations. This in turn cuts down the analyst's workload by reducing the search space. They can also mine the data to refine or refute the indication of a terror-crime link.

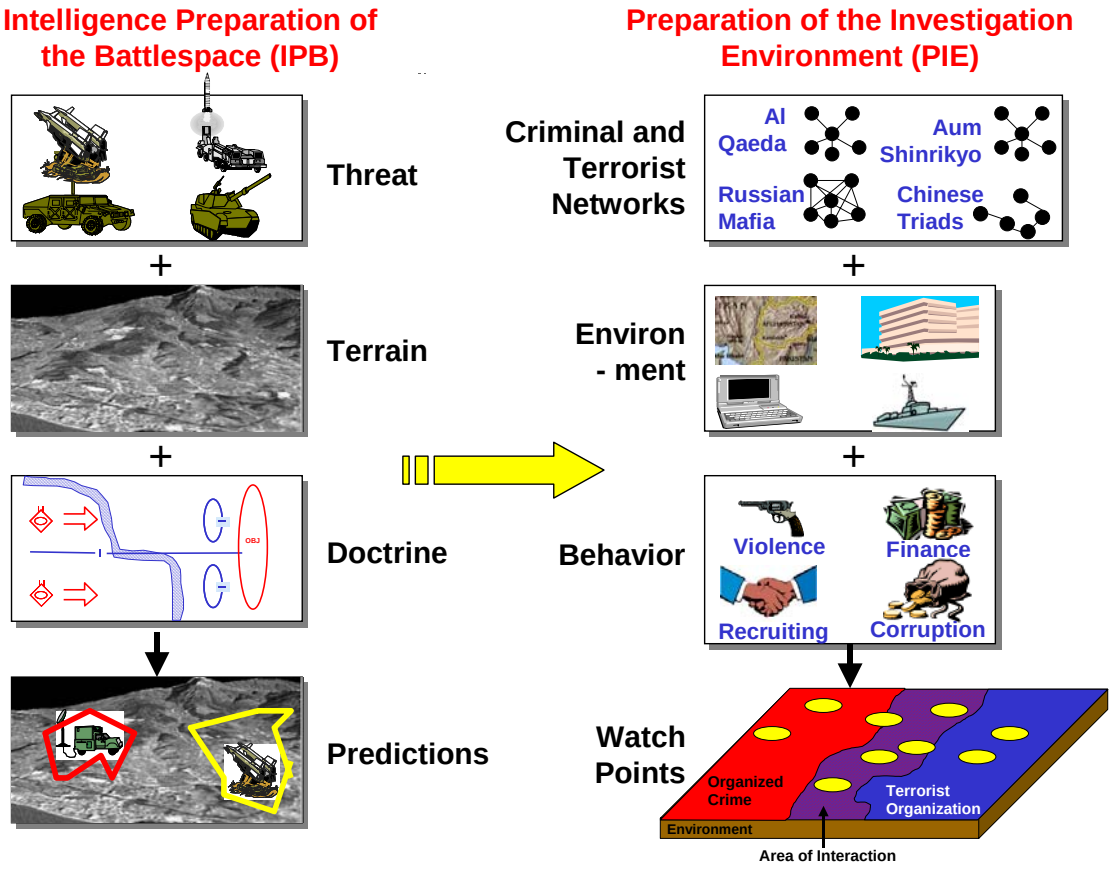

Figure 1: How IPB is adapted to form PIE

Figure 1 illustrates the methodological relationship between IPB and PIE. On the left of the diagram are the three components that serve as the foundation of IPB—the physical composition of the threat, the topography of the terrain, and the operational tendencies and capabilities that serve as the doctrine for the opposing force. By combining the three components, an IPB analysis results in a prediction of where an enemy might move on the battlefield.

Adapting IPB to PIE, these three components are the organizational composition of criminal and terrorist networks, the environment where they meet, and the behavioral patterns of each group. The combination of these three components results in a series of watch points, or areas where analysts and investigators might find crime-terror cooperation. Ultimately, indicators are generated that suggest specific evidence of such links.

There is prima facie evidence to support the applicability of IPB-like techniques to monitoring interactions between transnational crime and international terror.[38] Crime-terror connections are more likely to occur in areas of the world where the state has the least presence and means of control—that is, areas with large shadow economies and regional conflicts. Territory outside the control of the central state such as exists in failed or failing states, poorly regulated or border regions (especially those regions surrounding the intersection of multiple borders), and parts of otherwise viable states where law and order is absent or compromised, including urban quarters populated by diaspora communities or penal institutions, are favored locales for crime-terror interactions. It is these complex combinations that equated roughly to the named areas of interest found in the IPB method.

However, the shadow economy also includes non-geographical components such as cash businesses, illicit enterprises and offshore or underground banking. It was this combination that equated roughly to the named areas of interest found in the IPB method.

A critical function of PIE is to set sensible priorities for analysts. An exclusive focus on Pakistan's North West Frontier in the hope of spotting interaction between Al Qaeda and transnational criminal groups might well fail to detect such activity. That is because the interaction may be taking place in other chaotic areas of the world where military and law enforcement have even less presence. The Tri-Border Area straddling Paraguay, Brazil, and Argentina, for instance, is a favored meeting point for many different illegal networks. With a correct and informed use of PIE, the analyst would have realized that possibility.

3.2 Implementing PIE as an investigative tool

Forming PIE required significant modification of the IPB approach. First, we recognized that crime and terrorist groups are more diverse than military units. Organized crime and terrorist groups have significant differences in their organizational form, culture, and goals. Bruce Hoffman notes that terrorist organizations can be further categorized based on their organizational ideology.[39] Likewise, we have already introduced the notion that at least two different forms of organized crime group exist.

In converting IPB to PIE, we defined a series of watch points based on organizational form, goals, culture and other aspects to ensure PIE is flexible enough to compare a transnational criminal syndicate or a traditional crime hierarchy with an ethno-nationalist terrorist faction or an apocalyptic terror group.

The standard operating procedures and means by which military units are expected to achieve their battle plan are called doctrine, which is normally spelled out in great detail as manuals and training regimens. The doctrine of an opposing force thus is an important part of an IPB analysis. Such information is equally important to PIE, but is rarely found in manuals nor is it as highly developed as military doctrines. Consequently, the PIE approach focuses on common forms of behavior. For instance, engaging in criminal enterprises, purchasing of supplies, and document fraud are all areas where criminals and terrorists might intersect or collaborate to accomplish their goals.

Once the organizational forms, terrain and behavior of criminal and terrorist groups were defined at this level of detail, we settled on 12 watch points to cover the three components of PIE. For example, the watch point entitled *organizational goals* examines what the goals of organized crime and terror groups can tell investigators about potential collaboration or overlap between the two.

The next step was to locate indicators of crime-terror cooperation. Indicators are positive points that investigators can use to develop a sufficient level of suspicion that warrants further investigation. No single indicator is likely to provide 'smoking gun' evidence, however.

Investigators using PIE will collect evidence systematically through the investigation of watch points and analyze the data through its application to one or more indicators. That in turn will enable them to build a case for making timely predictions about crime-terror cooperation or overlap. Conversely, PIE also provides a mechanism for ruling out such links.

The indicators are designed to reduce the fundamental uncertainty associated with seemingly disparate or unrelated pieces of information. They also serve as a way of constructing probable cause, with evidence triggering indicators.

Although some watch points may generate ambiguous indicators of interaction between terror and crime, providing investigators and analysts with negative evidence of collusion between criminals and ter-

rorists also has the practical benefit of steering scarce resources toward higher pay-off areas for detecting cooperation between the groups.

3.3. PIE composition: Watch points and indicators

The first step for PIE is to identify those areas where terror-crime collaborations are most likely to occur. To prepare this environment, PIE asks investigators and analysts to engage in three preliminary analyses. These are first to map where particular criminal and terrorist groups are likely to be operating, both in physical geographic terms and through information traditional and electronic media; secondly, to develop typologies for the behavior patterns of the groups and, when possible, their broader networks (often represented chronologically as a timeline); thirdly, to detail the organizations of specific crime and terror groups and, as feasible, their networks.

By considering three similar aspects, an IPB analysis gives a prediction of where an enemy might move on the battlefield. The geographical areas where terrorists and criminals are highly likely to be cooperating are known in IPB parlance as *named areas of interest*, or localities that are highly likely to support military operations. In PIE they are referred to as watch points.

The second step of a PIE analysis concentrates on the watch points to identify named areas of interaction where overlaps between crime and terror groups are most likely. The PIE method expresses areas of interest geographically but remains focused on the overlap between terrorism and organized crime. Thus, the three preliminary analyses mentioned above are deconstructed into watch points, which are broad categories of potential crime-terror interactions. As the case studies will illustrate, the use of PIE leads to the early detection of named areas of interest through the analysis of watch points, providing investigators the means of concentrating their focus on terror-crime interactions and thereby enhancing their ability to detect possible terrorist planning.

The third and final step is for the collection and analysis of information that indicates organizational, operational or other nodes whereby criminals and terrorists appear to interact. While watch points are broad categories, they are composed of specific indicators of how organized criminals and terrorists might cooperate. These specific patterns of behavior help to confirm or deny that a watch point is applicable.

If several indicators are present, or if the indicators are particularly clear, this bolsters the evidence that a particular type of terror-crime interaction is present. No single indicator is likely to provide 'smoking gun' evidence of a link, although examples of this have occasionally arisen. Instead, PIE is a holistic approach that collects evidence systematically in order to make timely predictions of an affiliation, or not, between specific criminal and terrorist groups.

For policy analysts and planners, indicators reduce the sampling risk that is unavoidable for anyone collecting seemingly disparate and unrelated pieces of evidence. For investigators, indicators serve as a means of constructing probable cause. Indeed, even negative evidence of interaction has the practical benefit of helping investigators and analysts manage their scarce resources more efficiently.

3.4 The PIE approach in practice: Two Cases

The TraCCC team has recently applied the PIE approach to two of its research projects in order to validate its utility as an analytical approach for investigators and analysts. The first application, which focused on the Republic of Georgia, demonstrates the use of PIE to identify a specific crime-terror interaction. The second case provides a more strategic application of PIE, seeking out areas of Russia where crime-terror interactions might coalesce around weapons of mass destruction (WMD) smuggling.

Both cases are applications of the PIE analytical process described in the Appendix. In each case, the process began with the collection of relevant information (scanning) that was then placed into the larger context of watch points and indicators (codification) in order to produce the aforementioned analytical insights (abstraction). Each case will describe how the TraCCC team shared (diffusion) its findings in order to obtain validation and to have an impact on practitioners fighting terrorism and/or organized crime.

The second case will also demonstrate how the analysis benefited from the use of some of the information tools presented in the Appendix.

3.4.1 The Georgia Case

In 2003-4, TraCCC used the PIE approach to identify one of the largest money laundering cases ever successfully prosecuted. The PIE method helped close down a major international vehicle for money laundering. The ability to organize the financial records from a major money launderer allowed the construction of a significant network that allowed understanding of the linkages among major criminal groups whose relationship has not previously been acknowledged. In contrast to the analyses of western financial institutions, such as those that Naylor addressed in his work, where criminal money is inextricably mixed with legitimate capital, this bank handled almost exclusively dirty money for international crime groups.

The PIE approach applied by the TraCCC team allowed for very efficient use of limited human resources. It also provided Georgia, a country with limited expertise in transnational crime, terrorism or money laundering, the possibility to achieve a successful prosecution and to assist countries identified through subsequent network analysis to receive significant assistance in their investigations.

The TraCCC team started with a preliminary analysis that applied information to the PIE watch points and that found strong evidence to suggest that crime-terror interactions could be operating in or

facilitated by operations within the Republic of Georgia. While the findings of the analysis are discussed in more detail in the Black Sea case study below, some of the information most pertinent to Georgia included but that was not limited to:

1. Corrupt Georgian officials held high law enforcement positions prior to the Rose Revolution and maintained ties to crime and terror groups that allowed them to operate with impunity;
2. Similar patterns of violence were found among organized crime and terrorist groups operating in Georgia;
3. Numerous banks, corrupt officials and other providers of illicit goods and services assisted both organized crime and terrorists
4. Regions of the country supported criminal infrastructures useful to organized crime and terrorists alike, including Abkhazia, Adjaria and Ossetia.

Combined with numerous other pieces of information and placed into the PIE watch point structure, the resulting analysis triggered a sufficient number of indicators to suggest that further analysis was warranted to try to locate a crime-terror interaction. This interaction was to be addressed both in the conflict regions but also within loosely regulated sectors of the economy where illicit transactions of criminals and terrorists could operate.

The second step of the PIE analysis was to examine information within the watch points for connections that would suggest patterns of interaction between specific crime and terror groups. These points of interaction are identified in the Black Sea case study but the most successful identification was found from an analysis of the watch point that specifically examined the financial environment that would facilitate the link between crime and terrorism.

The TraCCC team began its investigation within this watch point by identifying the sectors of the Georgian economy that were most conducive to economic crime and money laundering. This included such sectors as energy, railroads and banking. All of these sectors were found to be highly criminalized. Closer scrutiny of the banking sector, using a PIE perspective, allowed determination of the parameters of the banking sector in Georgia. Numerous banks had developed within Georgia, a country which has an enormous shadow economy. Furthermore, the precipitous decline of the Georgian economy meant that there was not enough business to support several banking institutions let alone the variety of banks that were registered within the country. Interestingly, this finding was in direct contradiction with Naylor, demonstrating that banks can indeed exclusively serve illegitimate ends and thus act as the "dirty banks" that Naylor dismisses.

Therefore, within the context of the larger PIE watch points, a particular bank appeared particularly anomalous because it was small, had few commercial clients yet appeared to be doing a very significant volume of transactions. Its capital turnover was inconsistent with its holdings. Therefore, studying the terrain of the banking sector pointed to the "G" bank as one worthy of further scrutiny. Only by having researchers with knowledge of the economic climate, the nature of the business community and the banking sector determined that investigative resources needed to be concentrated on the "G" bank. By knowing the terrain, investigative focus was focused on "G" bank by the newly established financial investigative unit of the Central Bank. A six month analysis of the G bank and its transactions enabled the development of a massive network analysis that facilitated prosecution in Georgia and may lead to prosecutions in major financial centers that were previously unable to address some crime groups, at least one of which was linked to a terrorist group.

Using PIE allowed a major intelligence breakthrough. First, it located a large facilitator of dirty money. Second, the approach was able to map fundamental connections between crime and terror groups. Third, the analysis highlighted the enormous role that purely "dirty banks" housed in countries with small economies can provide as a service for transnational crime and even terrorism.

The PIE method's third step called for the TraCCC team to expand the organizational and operational aspects of the node to develop of fuller picture of the case. The TraCCC team did this through standard analytic techniques that identified the wire transfers emanating from the bank and their ties to criminals, terrorists or other individuals.

After a thorough analysis, the TraCCC team was able to hand over the data it collected to law enforcement investigators with the ability to examine data sources (e.g. wire transfers) that the TraCCC team did not have the ability to access. While specific details must remain sealed due to deference to ongoing legal proceedings, to date the PIE analysis has grown into investigations in Switzerland, and others in the US and Georgia.

Most important, however, is that law enforcement was able to use its sensitive information to complete the PIE analysis, which discovered that the Georgian bank served as both a money laundering node and as a site of crime-terror interactions for groups outside the region. For example, the TraCCC team learned that the bank serviced a Russian crime group with links to South American terror groups.

The PIE approach was in this case successful in providing a strategic basis for developing links between crime and terror groups. The process started with the generation of a named area of interaction (the Georgian banking system), proceeded to identify specific nodes of potential interaction (a Georgian bank) and then used different sources of information to identify organizational and operational links be-

tween criminal and terror groups. Adumbrating, the analysis also illustrates the importance for US investigators and analysts to look overseas for sites of crime-terror interactions that can come onshore. Before moving on, one final point is that the PIE case described here was not significantly intensive in terms of manpower in that it leveraged prior analysis with information collection through a handful of analysts to produce significant results.

Lastly, the PIE approach is one that favors the construction and prosecution of viable cases. As the Georgian case illustrates, the PIE approach is a platform for starting and later focusing investigations. When coupled with investigative techniques like network analysis, the PIE approach supports the construction and eventual prosecution of cases against organized crime and terrorist suspects.

3.4.2 Russian Closed Cities

In early 2005, a US government agency asked TraCCC to identify how terrorists are potentially trying to take advantage of organized crime groups and corruption to obtain fissile material in a specific region of Russia—one that is home to a number of sensitive weapons facilities located in so-called "closed cities." The project team assembled a wealth of information concerning the presence and activities of both criminal and terror groups in the region in question, but was left with the question of how best to organize the data and develop significant conclusions. Noting that the initial tasking called for the assessment of the potential for crime-terror interaction, the project team applied the PIE approach to structure the information and assess the likelihood that terror and crime groups might collaborate.

While the sensitivity of the project precludes a full accounting of the project's findings and conclusions, the application of the PIE analytical framework were impressive. The project's information supported connections in 11 watch points, including:

- A vast increase in the prevalence of violence in the region, especially in economic sectors with close ties to organized crime;
- Commercial ties in the drug trade between crime groups in the region and Islamic terror groups formerly located in Afghanistan;
- Rampant corruption in all levels of the regional government and law enforcement mechanisms, rendering portions of the region nearly ungovernable;
- The presence of numerous regional and transnational crime groups as well as recruiters for Islamic groups on terrorist watch lists;

In the end, the project benefited significantly from the PIE approach. The structure of the watch points and indicators served as a loose guide for the analysis of the data collected during the initial portions of the project. The lead analyst on the project, who was not a part of TraCCC's PIE team, found the watch points and indicators intuitive and readily adaptable to the task at hand. More importantly, employment of the watch points prompted creative leads to important connections that were not readily apparent until placed into the larger context of the PIE analytical framework. Specifically, the analysis might not have included evidence of trust links and cultural ties between crime and terror groups had the PIE approach not explained their utility.

Additionally, the project team found the discussion of how to integrate technology into the analytical process most useful for the organization and presentation of their data. As the appendix explains, technology tools exist that can aid the analyst who wishes to utilize PIE. When the TraCCC team applied the PIE to the closed cities case, the team found using the technologies reduced time analyzing data while improving the analytical rigor of the task. For example, structured queries of databases and online search engines provided information quickly. Likewise, network mapping improved analytical rigor by codifying the links between numerous actors (e.g. crime groups, terror groups, workers at weapons facilities and corrupt officials) in local, regional and transnational contexts.

3.5 Emergent behavior and automation

The dynamic nature of crime and terror groups complicates the IPB to PIE transition. The spectrum of cooperation demonstrates that crime-terror intersections are emergent phenomena. An analyst can update IPB to contend with the evolution of an adversary through feedback loops and regular adjustments to meet new data. For instance, an IPB analyst who discovers that the doctrine of an opposing force has changed significantly can adjust the IPB assessment accordingly.

Likewise, PIE must have feedback loops to cope with the emergent behavior of crime and terror groups. Given the amount of data facing analysts and the caseloads facing investigators, it is a daunting task to create, maintain and update a PIE approach. Time and again, when the project team spoke with analysts and investigators, the one deficiency they noted was the ability to conduct strategic intelligence given their operational tempo. A solution to this challenge can be found in the process of automating conventional IPB through the application of software packages. The automation of PIE, and the tools with which to do it, is discussed at length in the Appendix.

4. The terror-crime interaction spectrum

In formulating PIE, we recognized that crime and terrorist groups are more diverse in nature than military units. They may be networks or hierarchies, they have a variety of cultures rather than a disciplined code of behavior, and their goals are far less clear. Hoffman notes that terrorist groups can be further categorized based on their organizational ideology.[40]

Other researchers have found significant evidence of interaction between terrorism and organized crime, often in support of the general observation that while their methods might converge, the basic motives of crime and terror groups would serve to keep them at arm's length—thus the term "methods, not motives."[41] Indeed, the differences between the two are plentiful: terrorists pursue political or religious objectives through overt violence against civilians and military targets. They turn to crime for the money they need to survive and operate.

Criminal groups, on the other hand, are focused on making money. Any use of violence tends to be concealed, and is generally focused on tactical goals such as intimidating witnesses, eliminating competitors or obstructing investigators.

Yet the similarities are equally clear: both operate globally, utilize flexible network structures to complement or replace formal hierarchies, and thrive in chaotic environments with weak rule of law or shaky regulation. These shared traits are particularly striking in chaotic states where rule of law and efficient regulation have broken down. In a corrupt environment, the two groups find common cause.

Terrorists often find it expedient, even necessary, to deal with outsiders to get funding and logistical support for their operations. As such interactions are repeated over time, concerns arise that criminal and terrorist organizations will integrate and might even form new types of organizations.

Support for this point can be found in the seminal work of Sutherland, who has argued that the "intensity and duration" of an association with criminals makes an individual more likely to adopt criminal behavior. In conflict regions, where there is intensive interaction between criminals and terrorists, there is more shared behavior and a process of mutual learning that goes on. The same process can also be seen in urban areas of developed countries and in the prisons of Western Europe, Canada and the US—both locations where petty or professional criminals interact with terrorists. Similar patterns were observed in conflict zones, where such interactions often involve more large scale criminal elements.

The dynamic relationship between international terror and transnational crime has important strategic implications for the United States. The TraCCC team compared its empirical findings to prior studies of crime-terror interaction, like Naylor, Williams, Makarenko, and Dishman. The result is a model known as

the *terror-crime interaction spectrum* that depicts the relationship between terror and criminal groups and the different forms it takes.

Each form of interaction represents different, yet specific, threats, as well as opportunities for detection by law enforcement and intelligence agencies. For instance, the principle of activity appropriation outlined below means that small-to-medium fraud, drug dealing, and smuggling that might otherwise warrant little analysis may be seen in its full significance as possible evidence of terrorist cell activity. A typical clue might be found in small-scale criminal activity that is common knowledge, yet involves individuals or patterns of behavior that fit in with watch points. For example, Naylor's and other money laundering studies highlight the importance of cash businesses as either the entry point or laundering mechanism for illicit gains. An interview with a retired member of the Chicago organized crime investigative unit revealed that it had investigated taxi companies and taxicab owners as cash-based money launderers. Logic suggests that terrorists may also be benefiting from the scheme. But this line of investigation was not pursued in the 9/11 investigations although two of the hijackers had worked as taxi drivers.

Within the spectrum, processes we refer to as *activity appropriation*, *nexus*, *symbiotic relationship*, *hybrid*, and *transformation* illustrate the different forms of interaction between a terrorist group and an organized crime group, as well as the behavior of a single group engaged in both terrorism and organized crime. Dynamic movement among these conditions is, as we demonstrate below, possible. While some groups might move backwards or even skip a stage,[42] others may not ever move beyond a particular form of interaction. Given these dynamics of interaction, we have chosen to portray this scheme as a continuum.

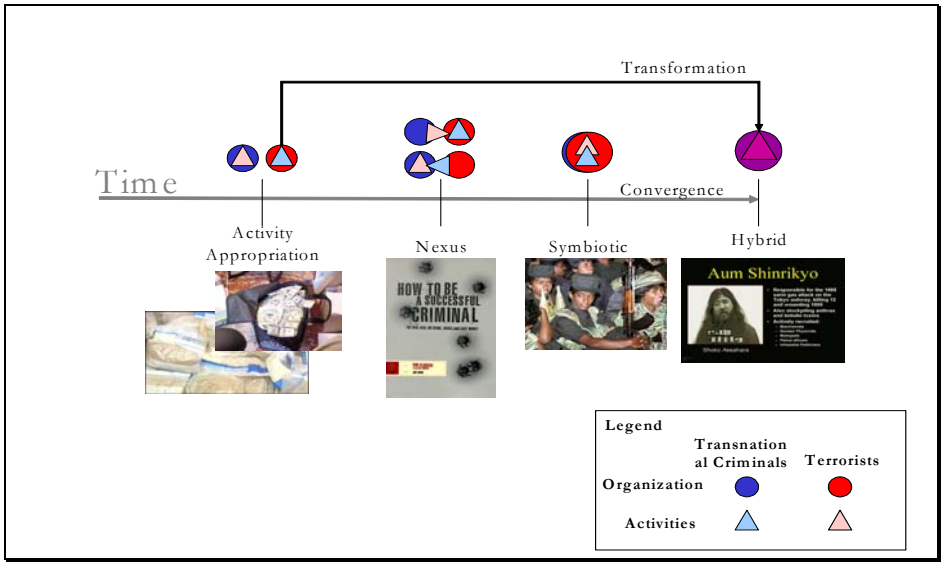

Figure 2: Terror-Crime Interaction Spectrum

Activity appropriation occurs when terror groups and organized crime adopt the other's methods without actually working together. To raise funds, terrorists habitually turn to credit card fraud, drug dealing, money laundering, and smuggling, the staple activities of organized criminals. John Horgan, for example, has heavily documented how cells of the Provisional Irish Republican Army's have engaged in a range of organized crime activities without any connection to organized crime groups.[43] Likewise, the Al Qaeda cells in Spain and Italy used credit card fraud and SIM card fraud to finance the strike cells based in Germany and France. Hezbollah has used cigarette smuggling in the U.S. and abroad,[44] while both Hezbollah and Al Qaeda have smuggled commodities, such as diamonds, in Africa. While less common, organized criminals have appropriated terror tactics when the authorities threatened their existence. In 1993, during a fresh attempt by the authorities to halt its activities, the Sicilian Mafia bombed the Uffizi museum in Florence and the Lateran Church in Rome.

While activity appropriation does not represent organizational linkages between crime and terror groups, it does capture the merger of methods that were well-documented in section 2. Activity appropriation is one way that terrorists are exposed to organized crime activities and, as Chris Dishman has noted, can lead to a transformation of terror cells into organized crime groups.

A terror group that is using the methods of organized crime does not always proceed to a nexus arrangement. This may be because no crime group is willing to do business with it, or because the terrorists see no benefit in working with outsiders. Instead, in a process known as transformation, a terrorist group becomes so attached to its criminal activities and the profits they generate that it abandons terrorism altogether, along with its old objectives. The Belfast bank robberies of December 2004, which followed a long period of relative inactivity by Republican terrorists in Northern Ireland, is another indication of what numerous British security officials told the project team was a process by which the IRA was transforming itself into an organized crime group.[45] In the Philippines, Abu Sayyaf started out as an Al Qaeda affiliate, but now is engaged more in economically motivated kidnapping for large ransoms and in piracy than in terrorism.[46]

Similarly, criminal groups can transform themselves into terrorist groups. There is no clear-cut example of this, however. In cases where organized crime has moved into terrorism, the shift has been temporary and can therefore be described as activity appropriation. On much rarer occasions has such a relationship resulted in a nexus, such as when Colombian drug lord Pablo Escobar hired ELN terrorists to wage a bombing campaign against the government on his behalf. Not capturing this form of convergence be-

tween organized crime and terrorism *as an activity* is to lose one explanation of why organized crime and terrorist *groups* might converge.

Applying the Sutherland principle of differential association, these activities are likely to bring a terror group into regular contact with organized crime. As they attempt to acquire forged documents, launder money, or pay bribes, it is a natural step to draw on the support and expertise of the criminal group, which is likely to have more experience in these activities. It is referred to here as a nexus. Interestingly, this progression is the contraposition of Makarenko, who sees organizational alliances occurring prior to groups appropriating the activity of the other. Williams, on the other hand, confirms this progression, noting that terrorists first engage in "do it yourself" organized crime and then turn to organized crime groups for specialized services like document forgery or money laundering.

The case study of the Tri-Border Area below provides a half-dozen examples of supplier-customer relationships between transnational organized crime and terror groups. However, such interactions are usually brief encounters rather than a sustained relationship, given that one group approaches the other to fulfill a specific requirement or service. In most cases a nexus involves the criminals providing goods and services to terrorists for payment although it can work in both directions. A typically short-term relationship, a nexus does not imply that the criminals share the ideological views of the terrorists, merely that the transaction offers benefits to both sides. After all, they have many needs in common: safe havens, false documentation, evasive tactics, and other strategies to lower the risk of being detected. In Latin America, transnational criminal gangs have employed terrorist groups to guard their drug processing plants. In Northern Ireland, terrorists have provided protection for human smuggling operations by the Chinese Triads.[47] To an investigator, such scanty contact might appear spontaneous and unimportant, and therefore be overlooked.

If the nexus continues to benefit both sides over a period of time, the relationship will deepen. More members of both groups will cooperate, and the groups will create structures and procedures for their business transactions, transfer skills and/or share best practices. We refer to this closer, more sustained cooperation as a symbiotic relationship, and define it as a relationship of mutual benefit or dependence. While it is prudent to note that few examples of this relationship exist, we agree with the characterizations of the close association of the Kosovo Liberation Army and Albanian crime gangs, as well as the liaison between the FARC and trafficking groups in Colombia.[48]

In the next stage, the two groups continue to cooperate over a long period and members of the organized crime group begin to share the ideological goals of the terrorists. They grow increasingly alike and finally they merge. That process results in a hybrid or *dark network*[49] that has been memorably described as

terrorist by day and criminal by night.[50] Such an organization engages in criminal acts but also has a political agenda. Both the criminal and political ends are forwarded by the use of violence and corruption.

These developments are not inevitable, but result from a series of opportunities that can lead to the next stage of cooperation. It is important to recognize, however, that even once the two groups have reached the point of hybrid, there is no reason per se to suspect that transformation will follow. Likewise, a group may persist with borrowed methods indefinitely without ever progressing to cooperation. In Italy and elsewhere, crime groups that also engaged in terrorism never found a terrorist partner and thus remained at the activity appropriation stage. Eventually they ended their terrorist activities and returned to the exclusive pursuit of organized crime. Indeed, the fact that the project team found no evidence of a hybrid organization existing aside from the case of the Aum Shinrikyo cult in Japan is a testament to the number of hurdles that hamper their formation.

Investigators can use the terror-crime interaction spectrum to analyze the behavior of both criminals and terrorists, and even to hypothesize about their future strategies. We argue above with reference to Sutherland that terrorist groups are more likely to be tracked down and infiltrated if they associate with criminal groups. In other words, provided that investigators are attuned to a crime-terror connection, the investigators might find it easier to launch counter-terrorist operations that focus on the criminal group providing support to the terrorist group.

Interestingly, the TraCCC team found no example where a terrorist group engaging in organized crime, either through activity appropriation or through an organizational linkage, came into conflict with a criminal group.[51] Neither archival sources nor our interviews revealed such a conflict over "turf," though logic would suggest that organized crime groups would react to such forms of competition. Indeed, while not a part of the spectrum given its focus on "interaction" between organized crime and terrorism (in both organizational and operational terms), conflict and non-interaction must remain categories of the relationship between organized crime and terrorism.[52]

The spectrum does not create exact models of the evolution of criminal-terrorist cooperation. Indeed, the evidence presented both here and in prior studies suggests that a single evolutionary path for crime-terror interactions does not exist. Environmental factors outside the control of either organization and the varied requirements of specific organized crime or terrorist groups are but two of the reasons that interactions appear more idiosyncratic than generalizable.

Hence, to create a method for investigators and analysts to identify when the cooperation occurs, to monitor such a relationship, and to respond appropriately when a trend becomes obvious, either locally or internationally, requires a methodological approach that considers a wide range of potential nodes of inter-

action. Using the PIE method, investigators and analysts can gain an understanding of the terror-crime intersection by analyzing evidence sourced from communications, financial transactions, organizational charts, and behavior. They can also apply the methodology to analyze watch points where the two entities may interact. Finally, using physical, electronic, and data surveillance, they can develop indicators showing where watch points translate into practice.

The result is a process for mapping how and where terror/crime interaction might occur, adding evidence to that hypothetical map, and then evaluating the patterns that emerge. An additional benefit is the semi-automated software tools (see Appendix) that allow analysts to monitor the evolving interaction between crime and terror without entrusting the process entirely to a computer system.

5. The significance of terror-crime interactions in geographic terms

While terror-crime interactions can occur in numerous settings, the research pointed to two broad categories of particular interest. The first were cities located in developed countries where terrorists often are supporting themselves through a range of seemingly petty yet organized crime activity. Examples of this have been observed in the 2004 Madrid bombers who were involved in mobile phone fraud and in United States where Chechen groups are engaged in Los Angeles in pornography.

Most often, one can classify such interactions as activity appropriation, with terror groups assuming the activities of crime groups and we do not have the terrorism-crime merger such as we see in conflict zones. Examples do exist, however, where terror groups have formed in these urban areas or in prisons to which these urban criminals are sent. There close links are formed between the organized criminals and the terrorists. The terrorists recruit individuals to assist their terrorist and/or criminal activity.[53] One of the central members of the Madrid terror cell, Jamal Ahmidan, was a former international drug dealer who converted to Islam while in prison and tapped his criminal past after his release to supply the cell's logistical needs—including the exchange of drugs for the explosives used in the attacks.

A very well documented case that serves as an exemplar of terror-crime interaction in urban areas of developed countries is that of Ahmed Ressam, who was arrested prior to an attempt to bomb Los Angeles International Airport during the millennium celebration. His case shows how the crime-terror interaction operates in diaspora urban communities in North America and Europe. In both these neighborhoods, law enforcement did not appreciate the importance of how even low level organized crime could be supporting terrorist activity.[54] Indeed, Ressam was active in crime as well as a part of Algerian Islamic terror groups that were co-located in Montreal, Canada and Roubaix, near Lille, France.

Some shared characteristics arose from examining this case. First, both neighborhoods shared similar diaspora compositions and a lack of effective or interested policing. Second, both terror cells had strong connections to the shadow economy. Shoplifting, theft, credit card fraud, and document fraud were staple activities for the men of the Montreal cell. The Roubaix cell also squarely fits the category of activity appropriation as it engaged in armed robberies in order to finance its terrorist activities. As such, the case demonstrated that each cell shared three factors—poor governance, a sense of ethnic separation amongst the cell (supported by the nature of the larger diaspora neighborhoods), and a tradition of organized crime.

But these factors are not limited to urban neighborhoods in developed countries. We noted in the introduction to this report that U.S. intelligence and law enforcement are naturally inclined to focus on manifestations of organized crime and terrorism in their own country, but they would benefit from study-

ing and assessing patterns and behavior of crime in other countries as well as areas of potential relevance to terrorism.

When turning to the situation overseas, one can differentiate between longstanding crime groups and their more recently formed counterparts according to their relationship to the state. With the exception of Colombia, rarely do large, established (i.e. "traditional") crime organizations link with terrorists. These groups possess long-held financial interests that would suffer should the structures of the state and the international financial community come to be undermined. Through corruption and movement into the lawful economy, these groups minimize the risk of prosecution and therefore do not fear the power of state institutions.

In contrast, the newer transnational crime groups thrive in a state of political anarchy or even ongoing conflict.[55] Their immediate need to finance military actions means they have little concern for existing financial institutions.

So although criminals of all types try to circumvent regulation and law enforcement, it was these newer groups that the TraCCC team found to most often be motivated by a desire to subvert or disregard the established order. And that is the key to their links to terrorism.

In a broader sense, we can argue that all kinds of criminal activity are more likely to thrive in a large shadow economy, that is, where illicit, unregulated, undeclared and illegal transactions take place and where there is little legitimate economy. But the size and scope of that phenomenon varies widely; it accounts for some 70 percent of the national economy in Georgia, for instance, compared with an estimated 5 to 10 percent in the United States. Therefore it makes more sense to focus on certain geographical areas as the nexus of crime-terror interaction.

As we mentioned in the PIE analysis of the Georgia banking sector, a crucial difference exists between illicit activity in the shadow economy in the United States and in the unregulated states of the former USSR. As Naylor has established in his research, money laundering occurs in an environment in which there is a mixture of illicit and licit funds. But in a large shadow or illicit economy such as exists in Moldova or Georgia, there is truly illicit banking that is servicing an international criminals, according to law enforcement. Recent FBI investigations in these countries, apart from the one mentioned previously of "G" bank, highlight the very different nature of illicit activity within these miniscule economies.

Developing countries with weak economies, a lack of social structures, many desperate, hungry people, and a history of unstable government are both relatively likely to provide ideological and economic foundations for both organized crime and terrorism within their borders and relatively unlikely to have much capacity to combat either of them. Conflict zones have traditionally provided tremendous opportu-

nities for smuggling and corruption and reduced oversight capacities, as regulatory and enforcements become almost solely directed at military targets. They are therefore especially vulnerable to both serious organized crime and violent activity directed at civilian populations for political goals – as well as cooperation between those engaging in pure criminal activities and those engaging in politically-motivated violence. Post-conflict zones are also likely to spawn such cooperation; as such areas often retain weak enforcement capacity for some time following an end to formal hostilities.

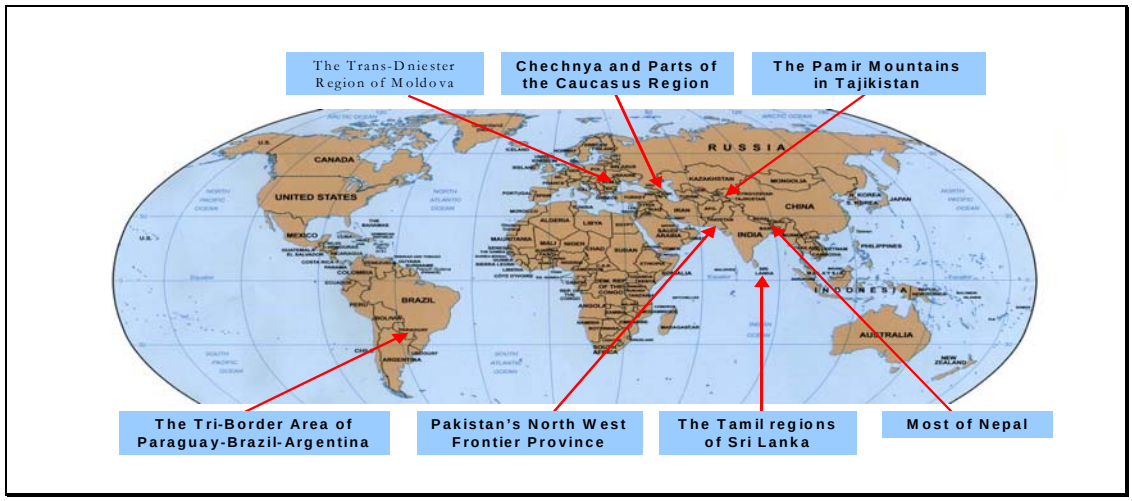

Figure 3: Regions Active with Crime-Terror Collaboration

In sum, there are certain types of locations where both organized crime and terrorism have long thrived. These can be grouped based upon features that make them most hospitable to organized crime and terrorism, which in turn makes it possible to identify terrain that enables both criminals and terrorists to thrive. Exhibit 2 shows some of these regions on a world map, but a larger list includes:

- Regions where the central state has lost control over some of its territory, as in Colombia, Georgia, the Sumatra peninsula of Indonesia, portions of Sri Lanka and Myanmar, Chechnya, the breakaway states of Georgia such as Abkhazia and South Ossetia, and the trans-Dniester region of Moldova;
- Regions straddling several national borders or jurisdictions such as Pakistan's North West Frontier, the Tri-Border Area of Paraguay, Brazil and Argentina, the Pamir Mountains in Tajikistan, and certain Balkan regions;
- Conflict zones where separatists are fighting government forces, such as the Tamil areas of Sri Lanka, and most of Nepal;

- Areas of countries that otherwise have a strong rule of law, but weak control over certain neighborhoods and slums, such as certain diaspora neighborhoods of cities, such as the outskirts of Marseilles, the northern sections of Naples, the favelas in Brazil.
- Penal institutions where correctional authorities are more concerned with maintaining order rather than probing the crime-terrorist interactions within their institutions.

All this is of first relevance to law enforcement and intelligence in the United States because these patterns of criminal behavior and organization can arise from areas as diverse as conflict zones overseas (which then tend can replicate once they arrive in the U.S.) to neighborhoods in U.S. cities. The problematic combinations of poor governance, ethnic separation from larger society, and a tradition of criminal activity (frequently international) are the primary concerns behind this broad taxonomy of geographic locales for crime-terror interaction. It is these features that these regions share most prominently, and that present a most interesting question for further research—are there other factors or more nuanced combinations of these three factors that give rise to crime-terror interactions?

6. Watch points and indicators

Taking the evidence of cooperation between organized crime and terrorism, we have generated 12 specific areas of interaction, which we refer to as watch points. In turn these watch points are subdivided into a number of indicators that point out where interaction between terror and crime may be taking place.

These watch points cover a variety of habits and operating modes of organized crime and terrorist groups. Going beyond a simple recitation of what the two groupings have in common--which might be explained by shared cultural norms or expediency in a constrained environment--meaningful watch points indicate how the habits of organized crime might translate into terrorism, as well as how terrorists might conceivably use the resources of organized criminal networks. How and why does an initial contact turn into cooperation for mutual benefit and in many cases progress to cooperation for the benefit of one side only? Once this approach is systematized in the terror-crime interaction spectrum, law enforcement agencies would have the opportunity to make connections and draw timely inferences about terrorist activity from data originally generated by studies of organized crime.

We have organized our watch points into three categories: environmental, organizational, and behavioral. Each of the following sections details one of the twelve watch points. We will describe the behavioral and environmental watch points (numbers 1-7) first, and then turn to the organizational watch points (numbers 8-12):

6.1. Watch Point 1: Open activities in the legitimate economy

Organized crime and terror may be associated with subterfuge and secrecy, but both criminal types engage legitimate society quite openly for particular political purposes. Yet in the first instance, criminal groups are likely to leave greater "traces," especially when they operate in societies with functioning governments, than do terrorist groups.[56]

Terrorist groups usually seek to make common cause with segments of society that will support their goals, particularly the very poor and the disadvantaged. Terrorists usually champion repressed or disenfranchised ethnic and religious minorities, describing their terrorist activities as mechanisms to pressure the government for greater autonomy and freedom, even independence, for these minorities. Some of these groups, such as the Kurdish PKK, turn to terrorism and openly take responsibility for their attacks. But their operational mechanisms are generally kept secret, and any ongoing contacts they may have with legitimate organizations are carefully hidden.

Criminal groups, like terrorists, may have political goals. For example, such groups may seek to strengthen their legitimacy through donating some of their profits to charity. Colombian drug traffickers

are generous in their support of schools and local sports teams.[57] Russian organized crime groups have been similarly active, as have criminal groups in the former Yugoslavia. But the political goals are in all cases subordinate to the economic goals, and it is in the latter area that those involved in criminal groups are usually most visible on a day-to-day basis.

At the operational level, criminals of all types could scarcely carry out criminal activities, maintain their cover, and manage their money flows without doing legal transactions with legitimate businesses. They buy clothing and food, rent apartments, purchase computers, explosives, and other specialized equipment, book airline tickets, and open bank accounts. They even use the services of government offices such as Consular sections that issue visas and passports. Front businesses set up by criminals to establish cover do much legitimate business. If they are also used as a vehicle for money laundering and other crimes, that is probably a secondary motive.

The many indicators of possible links include habits of travel, the use of mail and courier services, and the operation of fronts, two crucial operational needs of organized crime and terrorism alike:

- **Travel**: Frequent use of passenger carriers and shipping companies are potential indicators of illicit activity. Clues can be gleaned from almost any pattern of travel that can be identified as such. Particularly telling are travel patterns that coincide with changes in passport or visa control at border posts. Since Thailand created a new policy of visa-on-arrival that relaxes oversight on visa issuances to boost tourism, numerous members of major foreign criminal groups have been able to enter Thailand and thus establish themselves in south-east Asia generally. Suspicions that terrorists might do the same were confirmed: authorities recently discovered that Al-Qaeda operative Dawood Ibrahim hired gunmen from Pakistan who entered Thailand using visa-on-demand and then tried to kill an Indian organized crime boss living in Bangkok.[58] Here, the indicator that criminals were using the visa-on-demand mechanism could have provided an early-warning of the probability that the mechanism would be similarly attractive to Al-Qaeda.
- **Mail and courier services:** Indicators of interaction are present in the tracking information on international shipments of goods, which also generate customs records. Large shipments require bills-of-lading and other documentation. Analysis of such transactions, cross-referenced with information on crime databases, can identify links between organized crime and terrorist groups. In this way, a number of shipments of goods from unsuspecting U.S. companies to fronts controlled by Aum Shinrikyo were identified.[59] While this is a boon for law enforcement in the developed world where there is integrity and record keeping, it merely indicates a further difficulty

for investigators in other parts of the world where inventories, quantities, and even destinations are habitually disguised.

- **Fronts:** A shared front company or mutual connections to legitimate businesses are clearly also indicators of interaction. Aum Shinrikyo ran a huge front operation known as Devenir Millionaire, which it used to purchase gas masks, stun guns, night-vision equipment, inert hand grenades, and semiautomatic ammunition clips, among other items[60] Likewise the Sung-I, a Chinese organized crime group based in Paraguay, used its front companies as cover for a shipment of munitions to the Egyptian terror group al-Gama'a al-Islamiyya.[61]

6.2. Watch Point 2: Shared illicit nodes

The significance of overt operations by criminal groups should not be overstated. Transnational crime and terror groups alike carry out their operations for the most part with illegal and undercover methods. There are many similarities in these tactics. Both organized criminals and terrorists need forged passports, driver's licenses, and other fraudulent documents. Dishonest accountants and bankers help criminals launder money and commit fraud. Arms and explosives, training camps and safe houses are other goods and services that terrorists obtain illicitly.

These providers of goods and services in the shadow economy are increasingly specialized, which implies that crime and terror alike might use the same vendors or do business with each other. The clues may not be ubiquitous. Terror-crime cooperation discovered by investigators suggests that organized crime groups tend to provide a few specific services to the terrorists, rather than support across the board.

The many possible indicators of terror/crime interaction within this watch point include:

- **Fraudulent Documents.** Groups of both types may use the same sources of false documents, or the same techniques, indicating cooperation or overlap. A criminal group often develops an expertise in false document production as a business, expanding production and building a customer base. The Castorena-San Germán crime group built up a stock of over two million high-quality false documents to supply 55 U.S. cities in 32 states through couriers drawn from U.S. street gangs.[62] Some of the 9/11 hijackers fraudulently obtained legitimate driver's licenses through a fraud ring based at an office of DMV in the Virginia suburbs of Washington, DC. According to an INS investigator, this ring was under investigation well before the 9/11 attacks, but there was insufficient political will inside the INS to take the case further. Terrorists in prison in

Western Europe contract with Eastern European and criminals from the former USSR to provide fraudulent documents.[63]

- **Arms Suppliers.** Both terror and organized crime might use the same supplier, or the same distinctive method of doing business, such as bartering weapons or drugs. In 2001 the Basque terror group ETA contracted with factions of the Italian Camorra to obtain missile launchers and ammunition in return for narcotics.[64] A Balkan organized crime group led by a Tunisian named Mohamad bin Saleh bin Hmeidi has been supplying arms to the IRA, ETA, Islamic terrorist groups, and Italian mafia families.[65]
- **Financial experts.** Bankers and financial professionals who assist organized crime might also have terrorist affiliations. The methods of money laundering long used by narcotics traffickers and other organized crime have now been adopted by some terrorist groups. Riggs Bank, based in Washington, DC, is charged with facilitating terrorism, money laundering, and corruption and has already been convicted on some counts.
- **Drug Traffickers.** Drug trafficking is the single largest source of revenues for international organized crime. Substantial criminal groups often maintain well-established smuggling routes to distribute drugs. Such an infrastructure would be valuable to terrorists who purchased weapons of mass destruction and needed to transport them. Thus, studying drug trade routes may be a lucrative focus for terrorist investigators.
- **Other Criminal Enterprises.** An increasing number of criminal enterprises outside of narcotics smuggling are serving the financial or logistical ends of terror groups and thus serve as nodes of interaction. For example, piracy on the high seas, a growing threat to maritime commerce, often depends on the collusion of port authorities, which are controlled in many cases by organized crime. Such piracy has recently been loosely tied to some Southeast Asian terrorist groups. Analyzing criminal penetration of port authorities could provide an important tool for assessing terrorist risk, both from the perspective of straight piracy, and because of the larger problem of penetration of ports by terrorists.

These relationships are particularly true of developed countries with effective law enforcement, since criminals obviously need to be more cautious and often restrict their operations to covert activity. In conflict zones, however, criminals of all types feel even less restraint about flaunting their illegal nature, since there is little chance of being detected or apprehended. As a result, covert providers of such illicit services

in conflict zones are less sophisticated, and less well-organized. That may imply that they are easier to observe and detect.

6.3. Watch Point 3: Communications

The Internet, mobile phones and satellite communications enable criminals and terrorists to communicate globally in a relatively secure fashion. FARC, in concert with Colombian drug cartels, offered training on how to set up narcotics trafficking businesses used secure websites and email to handle registration.[66] Arabic-language websites display messages from members of Al Qaeda. Imprisoned criminals continue running their operations using cell phones from jail.[67]

Such scenarios are neither hypothetical nor anecdotal. Interviews with an analyst at the US Drug Enforcement Administration revealed that narcotics cartels were increasingly using encryption in their digital communications. In turn, the agent interviewed stated that the same groups were frequently turning to information technology experts to provide them encryption to help secure their communications. The same pattern was observed before 2001 in the Punjab, a conflict region in India, by law enforcement there.[68]

Nodes of interaction therefore include:

- **Technical overlap:** Examples exist where organized crime groups opened their illegal communications systems to any paying customer, thus providing a service to other criminals and terrorists among others. For example, a recent investigation found clandestine telephone exchanges in the Tri-Border region of South America that were connected to Jihadist networks.[69] Most were located in Brazil, since calls between Middle Eastern countries and Brazil would elicit less suspicion and thus less chance of electronic eavesdropping.
- **Personnel overlap:** Crime and terror groups that recruit common high-tech specialists to their cause. Given their ability to encrypt messages, criminals of all kinds may rely on outsiders to carry the message. Smuggling networks all have operatives who can act as couriers, and terrorists have networks of sympathizers in ethnic diasporas who can also help.

6.4. Watch Point 4: Use of information technology (IT)

Organized crime has devised IT-based fraud schemes such as online gambling, securities fraud, and pirating of intellectual property. Such schemes appeal to terror groups, too, particularly given the relative anonymity that digital transactions offer. Investigators into the Bali disco bombing of 2002 found that the laptop computer of the ringleader, Imam Samudra, contained a primer he authored on how to use online

fraud to finance operations.[70] Evidence of terror groups' involvement is a significant set of indicators of cooperation or overlap.

Both terrorist and criminal groups also use information technology in their operations: intelligence gathering, communicating with their associates, and sending messages to the media. Crucially, technology gives them relative anonymity when dealing with the legitimate economy, since these dealings may expose them to detection—a reason why some of the 9/11 hijackers purchased their airline tickets online rather than at a travel agent.

Indicators of possible cooperation or nodes of interaction include:

- **Fundraising:** Online fraud schemes and other uses of IT for obtaining ill-gotten gains are already well-established by organized crime groups[71] and terrorists are following suit. Such IT-assisted criminal activities serve as a another node of overlap for crime and terror groups, and thus expand the area of observation beyond the brick and mortar realm into cyberspace (i.e. investigators now expect to find evidence of collaboration on the Internet or in email as much as through telephone calls or postal services).
- **Use of technical experts:** While no evidence exists that criminals and terrorists have directly cooperated to conduct cybercrime or cyberterrorism, they are often served by the same technical experts. One Inspector General in India has noted that technicians and engineers who build software and network architecture also sell their services as hackers.[72] Russian organized crime groups hired hacker groups to assist with the extortion of online gambling firms. The Iron Guards, a hacker group with ties to Hezbollah, has launched denial of service attacks against Israeli targets and threatened similar attacks (or worse) on American corporations.[73] And experts have documented Al Qaeda's desire to develop an independent capability for online attacks against the interests of the U.S. and its allies.[74] As noted in the prior watch point, technical experts therefore serve as another node of interaction for criminals and terrorists.

Clearly, information technology provides nodes of interaction for organized crime and terrorism. What is not readily apparent, however, is the central role that private firms will play in locating these nodes. Internet service providers, for example, are routinely asked to provide law enforcement information on criminal activities and suspicious communications. Indeed, the edited volume of Abraham Sofaer and Seymour Goodman suggests the analogy of civil aviation as a model for how the public and private sectors should cooperate to fight crime and terrorism in cyberspace.[75] While other watch points will require information and cooperation from the private sector, this exigency is most pressing in the realm of information technology.

6.5. Watch Point 5: Violence

A number of studies and experts of terrorism have provided useful categorizations of the patterns of violence associated with terrorism.[76] Violence is not so much a tactic of terrorists as their defining characteristic. These acts of violence are designed to obtain publicity for the cause, to create a climate of fear, or to provoke political repression, which they hope will undermine the legitimacy of the authorities. Terrorist attacks are deliberately highly visible in order to enhance their impact on the public consciousness. Indiscriminate violence against innocent civilians is therefore more readily ascribed to terrorism. Possibly for this reason, inter alia, the TraCCC team found no examples exist where terrorists have engaged criminal groups for violent acts.

A more significant challenge lies in trying to discern generalities about organized crime's patterns of violence. Categorizing patterns of violence according to their scope or their promulgation is suspect. In the past, crime groups have used violence selectively and quietly to achieve their goals, but then have also used violence broadly and loudly to achieve other goals. Neither can one categorize organized crime's violence according to goals as social, political and economic considerations often overlap in every attack or campaign.[77]

A few exceptional cases exist where organized crime has either employed terrorist groups or directly engaged in terrorist campaigns of violence. The Sicilian Mafia's use of terrorist attacks against the Italian state[78] and the Medellin cartel's assault on the Colombian state[79] generally defy categorization, however. For example, the Medellin drug cartel employed ELN and M-19, Colombian guerilla groups, in their campaign to pressure the Colombian government to end its threats to extradite the leadership of the cartel. The cartel initiated attacks against civilians from a position of strength, seeking to use its power to cow the Colombian government into compliance and secure its base of operations. On the other hand, the Sicilian Mafia's campaign targeted symbols of the Italian state, deliberately avoiding civilian casualties, in response to an increasingly successful Italian anti-mafia campaign. While both campaigns had some similarities, the divergence of the political, economic and social elements behind the initiation, consummation and intentions of these two campaigns makes it difficult to generalize from them.

Examining violence associated with crime and terror groups resulted in two significant conclusions. First, the project team located no concrete indicators of collaboration between criminals and terrorists through the commission or patterns of violence. So while no indicators arose from this watch point, the TraCCC team cannot rule out that such indicators might evolve over time, such as the hiring of one group to bomb targets or assassinate persons of interest to another group. Second, the frequency and scope of

violence did prove important as it is an environmental factor for investigators and analysts considering an area of potential convergence between crime and terror groups. Prior sections of this report have discussed how high levels of violence foster an environment favorable to crime-terror interactions. Violence is therefore an important watch point that may not yield specific indicators of crime-terror interaction per se but can serve to frame the likelihood that an area might support terror-crime interaction.

6.6. Watch Point 6: Use of corruption

Both terrorists and organized criminals bribe government officials to undermine the work of law enforcement and regulation. Corrupt officials assist criminals by exerting pressure on businesses that refuse to cooperate with organized crime groups, or by providing passports for terrorists. The methods of corruption are diverse on both sides and include payments, the provision of illegal goods, the use of compromising information to extort cooperation, and outright infiltration of a government agency or other target.

Many studies have demonstrated that organized crime groups often evolve in places where the state cannot guarantee law or order,[80] or provide basic health care, education, and social services. The absence of effective law enforcement combines with rampant corruption to make well-organized criminals nearly invulnerable. Moreover, local people alienated and angry by high levels of corruption in such as in Uzbekistan Indonesia, and Nigeria may become politically alienated or turn to radical thoughts. Terrorism is sometimes the result. In Afghanistan under the Taliban, terror groups such as Al Qaeda were supported by drug trafficking. The trade in turn was facilitated by massive corruption, particularly corruption of officials in Nigeria, Indonesia, and the border regions of adjoining Tajikistan, Iran and Pakistan.[81] Likewise, official corruption in Pakistan has deprived citizens of needed basic services and provided an opening for charities funded by Saudi Arabia that support Islamic terror groups. The PLO has found popular support in the West Bank in the same way. In Uzbekistan, there is also a convergence of the drug trade, the IMU and high levels of corruption within the government. Fundamentalist Islam has found fertile ground in Uzbekistan in large part due to the collapse of living standards and the poor governance of the Uzbek state. The government has been repressing the traditional Islamic population, exacerbating the terrorist reaction. Partial funding of the IMU is derived from drug trafficking, and corruption exists at all levels of government to facilitate the drug trade.[82]

Colombia may be the only example of a conflict zone where a major transnational crime group with very large profits is directly and openly connected to terrorists. The interaction between the FARC and ELN terror groups and the drug syndicates provides crucial important financial resources for the guerillas to operate against the Colombian state - and against each another. This is facilitated by universal cor-

ruption, from top government officials to local police. Corruption has served as the foundation for the growth of the narcotics cartels and insurgent/terrorist groups.

In the search for indicators, it would be simplistic to look for a high level of corruption, particularly in conflict zones. Instead, we should pose a series of questions:

- **Cooperation** Are terrorist and criminal groups working together to minimize cost and maximize leverage from corrupt individuals and institutions?
- **Division of labor** Are terrorist and criminal groups purposefully corrupting the areas they have most contact with? In the case of crime groups, that would be law enforcement and the judiciary; in the case of terrorists, the intelligence and security services.
- **Autonomy** Are corruption campaigns carried out by one or both groups completely independent of the other?

These indicators can be applied to analyze a number of potential targets of corruption. Personnel that can provide protection or services are often mentioned as the target of corruption. Examples include law enforcement, the judiciary, border guards, politicians and elites, internal security agents and Consular officials. Economic aid and foreign direct investment are also targeted as sources of funds by criminals and terrorists that they can access by means of corruption.

6.7. Watch Point 7: Financial transactions & money laundering

That both terror groups and organized crime attempt to conceal their financial activities and money flows is a given. But despite the different purposes that may be involved in their respective uses of financial institutions (organized crime seeking to turn illicit funds into licit funds; terrorists seeking to move licit funds to use them for illicit means), the groups tend to share a common infrastructure for carrying out their financial activities. Both types of groups need reliable means of moving, and laundering money in many different jurisdictions, and as a result, both use similar methods to move money internationally. Both use charities and front groups as a cover for money flows. A number of charities have come under scrutiny for laundering funds for Al Qaeda in the 9/11 investigation, while the U.S. State Department runs a dedicated unit to track the numerous front companies associated with Russian organized crime. Transnational organized criminals and terrorists employ in-house specialists and also co-opt legitimate financial experts including accountants and bankers to facilitate their money laundering. Possible indicators include:

- Shared methods of money laundering
- Mutual use of known front companies and banks, as well as financial experts.

6.8. Watch Point 8: Organizational structures

The traditional model of organized crime used by U.S. law enforcement is that of the Sicilian Mafia - a hierarchical, conservative organization embedded in the traditional social structures of southern Italy. Investigators attempting to find common ground between organized crime and terror using the Sicilian Mafia as their organizational model would be unlikely to succeed, however. The reason is that among today's organized crime groups the Sicilian mafia is more of an exception than the rule.

Most organized crime now operates not as a hierarchy but as a decentralized, loose-knit network – which is a crucial similarity to terror groups.[83] Networks offer better security, make intelligence-gathering more efficient, cover geographic distances and span diverse memberships more effectively.

The larger significance of terrorists' and criminals' shared characteristics is that the two groupings are well-placed to find each other and to discover ways to do business. Many links between terror and organized crime are triggered by the criminals' desire to find new sources of business, and terrorists' desire to make money.

Some additional aspects of structure:

- **Membership dynamics** Both terror and organized crime groups – with the exception of the Sicilian Mafia and other traditional crime groups (i.e. Yakuza) – are made up of members with loose, relatively short-term affiliations to each other and even to the group itself. They can readily be recruited by other groups. By this route, criminals have become terrorists. A member of the Camorra, the organized crime network based in Naples, Italy, was introduced in prison to radical Islam that later served as a bridge between terror groups and the Camorra.
- **Scope of organization** Terror groups need to make constant efforts to attract and recruit new members. Obvious attempts to attract individuals from crime groups are a clear indication of cooperation. An intercepted phone conversation in May 2004 by a suspected terrorist called Rabei Osman Sayed Ahmed revealed his recruitment tactics: "You should also know that I have met other brothers, that slowly I have created with a few things. First they were drug pushers, criminals, I introduced them to the faith and now they are the first ones who ask when the moment of the jihad will be. Some have gone to Afghanistan and some are praying and waiting".[84] Moreover, if the same individuals are active in both groups, it is a clear indication of cooperation. A mid-level member of the Yakuza crime network in Japan joined Aum Shinrikyo, where he enjoyed high status as a rare convert. The fact that he joined the terrorist group also elevated his stature in the Yakuza because he was bringing in new business.

- **Need to buy, wish to sell** Often the business transactions between the two sides operate in both directions. Terrorist groups are not just customers for the services of organized crime, but often act as suppliers, too. Arms supply by terrorists is particularly marked in certain conflict zones. Thus any criminal group found to be supplying outsiders with goods or services should be investigated for its client base too. Investigators who discovered the money laundering in the above example were able to find out more about the terrorists' activities too. The Islamic radical cell that planned the Madrid train bombings of 2004 was required to support itself financially through a business venture despite its initial funding by Al Qaeda.[85] Likewise, a Chinese criminal family engaged in smuggling people into the United States and managed funds for a Hezbollah cell operating in the Tri-Border region of Argentina, Paraguay, and Brazil.

6.9. Watch Point 9: Organizational goals

In theory, their different goals are what set terrorists apart from the perpetrators of organized crime. Terrorist groups are most often associated with political ends, such as change in leadership regimes or the establishment of an autonomous territory for a subnational group. Even millenarian and apocalyptic terrorist groups, such as the science-fiction mystics of Aum Shinrikyo, often include some political objectives. Organized crime, on the other hand, is almost always focused on personal enrichment.

In developed countries, traditional criminal groups may shun terrorists out of distaste for their goals: a Sicilian Mafia group that was doing business with an Albanian gang ended the association when informed by a top Sicilian prosecutor that the Albanians were in fact terrorists.[86] Crime for the Sicilians was simply a means of making money, and they despised attempts to undermine society and the state. On the other hand, new crime groups in developed countries and crime and terror groups in developing countries, often share a dislike of those in power, of legislation and regulation, and the economic system. Cooperation may be welcomed as an opportunity to undermine all these.

Furthermore, even in developed countries, the goals of each organization have been known to shift. The Sicilian Mafia launched a terrorist bombing campaign against symbols of the Italian state in 1993 to try to force a reprieve from the effective anti-Mafia crackdown the Italian authorities had undertaken. Likewise, Al Qaeda's focus at about the same time was split between supporting operations against the U.S. and establishing legitimate businesses to generate cash flow.[87]

By cataloging the different – and shifting - goals of terror and organized crime groups, we can develop indicators of convergence or divergence. This will help identify shared aspirations or areas where these

aims might bring the two sides into conflict. On this basis, investigators can ask what conditions might prompt either side to adopt new goals or to fall back to basic goals, such as self-preservation.

- **Long view or short-termism** La Cosa Nostra's acts of terrorism described above were triggered by a vigorous crackdown by the Italian authorities and La Cosa Nostra reacted with an act of despair in order to survive. That low point was an ideal opportunity for a terror group to become involved since the divergence in goals largely had disappeared, at least temporarily.
- **Affiliations of protagonists** The Chinese crime groups that assisted Hezbollah terrorists in Latin America would have been unlikely to aid a Chinese terror group such as the separatists in Xijiang in western China. Such an association would have undermined some of their own values and brought on them the wrath of the Chinese authorities. But they evidently had no qualms about aiding a foreign group whose actions have no effect on Chinese society.

6.10. Watch Point 10: Culture

Both terror and criminal groups use ideologies to maintain their internal identity and provide external justifications for their activities. Religious terror groups adopt and may alter the teachings of religious scholars to suggest divine support for their cause, while Italian, Chinese, Japanese, and other organized crime groups use religious and cultural themes to win public acceptance. Both types use ritual and tradition to construct and maintain their identity. Tattoos, songs, language, and codes of conduct are symbolic to both.

However, incompatibilities between the two groups should come as no surprise. Many religious terrorist groups teach that their members will find rewards for their sacrifices after death, while organized crime groups emphasize earthly rewards.

Religious affiliations, strong nationalist sentiments and strong roots in the local community are often characteristics that cause organized criminals to shun any affiliation with terrorists. Conversely, the absence of such affiliations means that criminals have fewer constraints keeping them from a link with terrorists.

Indicators of divergence include such as conflicting positions on the place of religion in society, disagreement over cultural norms, or contrary opinions on personal lifestyles and identities. Even the lack of a cultural identity may be an indicator: Some recently established organized crime groups in Kosovo with no strong nationalist ties have formed links with the terrorist Kosovo Liberation Army (KLA).

In any organization, culture connects and strengthens ties between members. For networks, cultural features can also serve as a bridge to other networks.[88]

Indicators of interaction are shared features of network culture, such as:

- **Religion** Many criminal and terrorist groups feature religion prominently. Al Qaeda is perhaps the best-known religious/apocalyptic organization, but the cultural themes of an approaching end time are common in Jewish Messianism and the Christian Identity Movement, in whose name acts of terrorism have been committed.[89] Japan's Aum Shinrikyo has interwoven Christian and Buddhist symbolism with the science fiction series Millennium to lead its followers to believe that they are the people chosen to repopulate the Earth following nuclear war. Organized crime groups in Italy have used religion to validate the groups in relation to society. Gambetta notes how La Cosa Nostra has adopted icons of the Catholic Church, particularly Saint Michael the Archangel, to strike a pose as protectors of the local people.[90] Likewise a shared Islamic faith aided the cooperation between Al Qaeda, the Taliban, and Afghan warlords in the narcotics production and smuggling that sustained all three entities during the 1990s.
- **Nationalism** Ethno-nationalist insurgencies and criminal groups with deep historical roots are particularly likely to play the nationalist card. For instance, the Lebanese crime groups in the Tri-Border area of South America have demonstrated a close affinity for the religious and nationalist roots of Hezbollah.
- **Society** Many criminal and terrorist networks adapt cultural aspects of the local and regional societies in which they operate to include local tacit knowledge, as contained in narrative traditions. Manuel Castells notes the attachment of drug traffickers to their country, and to their regions of origin. "They were/are deeply rooted in their cultures, traditions, and regional societies. …they have also revived local cultures, rebuilt rural life, strongly affirmed their religious feeling, and their beliefs in local saints and miracles, supported musical folklore (and were rewarded with laudatory songs from Colombian bards)…"

6.11. Watch Point 11: Popular support

Both organized crime and terrorist groups engage legitimate society in furtherance of their own agendas. In conflict zones, this may be done quite openly, while under the rule of law they are obliged to do so covertly. One way of doing so is to pay lip service to the interests of certain ethnic groups or social classes. Organized crime is particularly likely to make an appeal to disadvantaged people or people in certain professionals though paternalistic actions that make them a surrogate for the state. For instance, the Japanese Yakuza crime groups provided much-needed assistance to the citizens of Kobe after the serious earthquake there. Russian organized crime habitually supports cultural groups and sports troupes.[91]

Both crime and terror derive crucial power and prestige through the support of their members and of some segment of the public at large. This may reflect enlightened self-interest, when people see that the criminals are acting on their behalf and improving their well-being and personal security. But it is equally likely to be that people are afraid to resist a violent criminal group in their neighborhood, as is the case in Northern Ireland, Colombia, and the Balkans.

This quest for popular support and common cause suggests various indicators:

- **Sources** Terror groups seek and sometimes obtain the assistance of organized crime based on the perceived worthiness of the terrorist cause, or because of their common cause against state authorities or other sources of opposition. In testimony before the U.S. House Committee on International Relations, Interpol Secretary General Ronald Noble made this point. One of his examples was that Lebanese syndicates in South America send funds to Hezbollah.[92] Interpol has also noted that an Indian organized crime syndicate led by Dawood Ibrahim found common cause with Muslim insurgents in India and Kashmir as well as with Al Qaeda.[93] This type of common cause might be founded on shared political, religious, or cultural views. Conversely, the absence of common cause can inhibit cooperation between terror and organized crime groups. Chechen organized crime groups operating in Russia helped fund Chechen insurgent movements while they operated as nationalists, but some ceased to fund these operations once the insurgents adopted the Islamic jihadist cause (see the Chechen case study that follows).
- **Means** Groups that cooperate may have shared activities for gaining popular support such as political parties, labor movements, and the provision of social services.
- **Places** In conflict zones where the government has lost authority to criminal groups, social welfare and public order might be maintained by the criminal groups that hold power. Where power is shared by terrorists and organized crime, such as in neighborhoods in Northern Ireland, areas of Lebanon and the Gaza Strip, cooperation may be present.

6.12. Watch Point 12: Trust

Like business corporations, terrorist and organized crime groups must attract and retain talented, dedicated, and loyal personnel. These skills are at an even greater premium than in the legitimate economy because criminals cannot recruit openly. A further challenge is that law enforcement and intelligence services are constantly trying to infiltrate and dismantle criminal networks. Members' allegiance to any such group is constantly tested and demonstrated through rituals such as the initiation rites common to

Russian, Japanese, and Italian groups. Thus trust is critical to any cooperation between terrorist and organized crime groups, as well as a key indicator of such activity.

We propose three forms of trust in this context, using as a basis Newell and Swan's model for interpersonal trust within commercial and academic groups.[94]

- **Companion trust** based on goodwill or personal friendships. The relationship between Osama bin Laden and Ayman al-Zawahiri evolved through membership in the anti-Soviet mujahideen and then through the common leadership of Al Qaeda and Egyptian Islamic Jihad, respectively. In this context, indicators of terror-crime interaction would be when members of the two groups use personal bonds based on family, tribe, and religion to cement their working relationship. Efforts to recruit known associates of the other group, or in common recruiting pools such as diasporas, would be another indicator.
- **Competence trust**, which Newell and Swan define as the degree to which one person depends upon another to perform the expected task. Competence trust can form under a variety of circumstances: an example was how Khalid Sheikh Mohammad trusted his lieutenants in Al Qaeda to plan and execute the attack on the U.S.S. Cole as well as the Sept. 11 attacks.
- **Commitment or contract trust**, where all actors understand the practical importance of their role in completing the task at hand. Commitment trust was evident among the members of the Al Qaeda cells that plotted the Los Angeles International Airport Millennium plot. Likewise communal living in a single apartment, and group training experiences in Afghanistan, created trust relationships between members of the Al Qaeda operations cell in Hamburg that helped prepare the Sept. 11 attacks[95]

7. Case studies

Having developed the watch points and indicators for terror-crime interaction, we sought to exercise the model. We analyzed three geographic regions in which there has been substantial evidence of organized crime and terrorist support and interactions, the Tri-Border Area of Paraguay, Brazil and Argentina, the Black Sea Region and the case of Chechnya within Russia. The summaries of all three case studies provide empirical support for the PIE model.

7.1. The Tri-Border Area of Paraguay, Brazil, and Argentina[96]

Hezbollah is mostly thought of as a terrorist group operating in the Middle East and is strongly associated with attacks on Israeli targets in Lebanon and Israel. In fact, Hezbollah has struck far away from its home base of operations—in South America. On March 17, 1992, a van bomb outside the Israeli embassy in Buenos Aires killed 29 people and injured 250. Two years later, another car bomb attack in Buenos Aires practically destroyed the Jewish-Argentine community center, killing 87.

In both cases, the evidence pointed to Hezbollah as the perpetrator, the staging area for the attacks was the Paraguayan city of Ciudad del Este in the so-called Tri-Border Area, a nexus for terrorist and criminal activity of all kinds.

With its lawlessness, Cuidad del Este (referred to here as CDE) has long allowed activities of malevolent non-state actors to flourish. But only since Sept. 11 has the city come under closer scrutiny by security analysts and intelligence agencies.[97]

CDE has become notorious as a remote place where the spotlights of law enforcement are dim and where everything may be purchased at the right price from the right people. Originally a village, this rapidly-expanding city of some 250,000 people was developed by Julius Stroessner, who turned Paraguay into a haven for fugitives from the law—including the Nazi war criminal Josef Mengele. Stroessner himself is suspected of having run a drug-trafficking organization.[98]

CDE is also an international crossroads where the borders of Argentina, Paraguay and Brazil meet. For many years these three countries have been blaming each other for tolerating widespread crime activities in the Tri-Border Area, yet achieved very little. Without a concerted effort by all three governments, criminal and terror groups continue to operate almost unchecked.

The roots of the problem are economic. Brazil is now the world's eighth-largest economy, while Paraguay remains one of Latin America's most corrupt and poorest countries.[99] Argentina has recently suffered a catastrophic economic crisis. Huge disparities in incomes and prices, combined with prohibitive import

tariffs in all three countries, have created a smuggler's paradise. Paraguayan tax laws and other regulations are lax and poorly enforced. The shadow economy in Paraguay is estimated at between 40 percent and 50 percent of gross domestic product[100]. All kinds of goods including sophisticated military hardware and all kinds of weapons are available for purchase in the shops. The resulting business opportunities have attracted diaspora communities from all over the world, including tens of thousands of people from the Middle East, Africa, and Southeast Asia. The Tri-Border Area includes a significant Muslim population, which is susceptible to extortion and a suitable hiding place for extremist elements. Furthermore, there is a very high volume of traffic across the border. Every day, some 40,000 people go unchecked as they cross the bridge between CDE and Foz do Iguaçu, its sister city in Brazil, along with more than 2,000 vehicles including many trucks laden with freight containers.[101] Some 5,000 businesses are crowded into just 20 square blocks in CDE's downtown area, making illicit transactions easy to hide. The result is a huge, varied, and dynamic shadow economy that evades almost all attempts at regulation or detection.

Organized crime groups of all types thrive in the tri-border area. Paraguay's return to democracy and the free market in 1993 brought in a sharp relaxation of regulation characterized by ineffective law, rising corruption, and weak state institutions. As the legitimate economy slumped, international criminal groups moved in. The Tri-Border Area is now a meeting place for the Yakuza as well as Colombian and other Latin American gangs, who pass illegal drugs through CDE on their way to the ports of Brazil, Argentina, and Uruguay, and thence to the U.S. and Europe. Chinese Triads such as the Fuk Ching, Big Circle Boys, and Flying Dragons are well established and believed to be the main force behind organized crime in CDE.

CDE is also a center of operations for several terrorist groups, including Al Qaeda, Hezbollah, Islamic Jihad, Gamaa Islamiya, and FARC.[102] The 1992 bombing of the Israeli Embassy in Buenos Aires provided the first evidence of this. While Islamic Jihad claimed responsibility, the U.S. State Department and others believe that the claim was a smokescreen for Hezbollah.

Watch points

Crime and terrorism in the Tri-Border Area interact seamlessly, making it difficult to draw a clean line between the types of persons and groups involved in each of these two activities. There is no doubt, however, that the social and economic conditions allow groups that are originally criminal in nature and groups whose primary purpose is terrorism to function and interact freely.

Organizational structure Evidence from CDE suggests that some of the local structures used by both groups are highly likely to overlap. There is no indication, however, of any significant organizational overlap between the criminal and terrorist groups. Their cooperation, when it exists, is ad hoc and without any formal or lasting agreements, i.e. activity appropriation and nexus forms only.[103] The Chinese mafia comprises about six Triads, which occasionally engage in turf battles but mostly respect each other's commercial areas. These groups are traditional hierarchies, each commanded by a single leader. Terrorist groups in the area, including Hezbollah, Al Qaeda, and al Gamma al Islamiya, have a loose hierarchical structure in which some groups work as financial wings (raising money and remitting it to the Middle East), while others are responsible for secure communications with the rest of the world.

Organizational goals In this region, the short-term goals of criminals and terrorists converge. Both benefit from easy border crossings and the networks necessary to raise funds. Some terrorists operating in the Tri-Border Area raise money through drugs and arms smuggling. In May 2002 Ali Assi, who ran a coffee shop in the Islamic Welfare Center in CDE, was arrested at the Beirut airport with 10 kilograms of cocaine.[104] Assi is the father-in-law of Ali Hassan Abdallah, who is one of the key operatives of the Hezbollah financial network in the CDE area and also a business partner of Sobhi Mahmoud Fayad, a convicted Hezbollah lieutenant.[105] Ali Hassan was expelled from Angola in March 2003 and is believed to have ordered funds transfers to Islamic fundamentalist groups in the Middle East through an associate in CDE.[106] There is no evidence that their longer-term goals converge in this environment, however, which suggests that their interaction did not go further than a nexus form.

Culture Cultural affinities between criminal and terrorist groups in the Tri-Border Area include shared ethnicities, languages and religions. Both Arab and Chinese criminal groups maintain local cells that specialize in imposing their rules on the local diaspora communities. Evidence indicates cooperation between Lebanese criminal groups and Hezbollah terrorist cells within smuggling networks transporting Colombian cocaine through CDE to the U.S. and Europe. In January 2003 Bassam Naboulsi, a cousin of Assad Ahmad Barakat, believed to be a member of a cocaine smuggling ring operating from CDE and Foz do Iguaçu, was arrested in Sao Paulo. Hassan Naboulsi, Bassam's brother, owned a store in the Page Gallery in CDE which is partially owned by Barakat. It emerged that 400 to 1000 kilograms of cocaine may have been shipped on a monthly basis through the Tri-Border Area on its way to Sao Paulo and thence to the Middle East and Europe[107]. Numerous arrests revealed the strong ties between entrepreneurs in CDE and criminal and potentially terrorist groups. From the evidence in CDE it seems that the two phenomena operate in rather separate cultural realities, focusing their operations within ethnic groups. But nor does culture serve as a major hindrance to cooperation between organized crime and terrorists.

Illicit activities and subterfuge The evidence in CDE suggests that terrorists see it as logical and cost-effective to use the skills, contacts, communications and smuggling routes of established criminal networks rather than trying to gain the requisite experience and knowledge themselves. Likewise, terrorists appear to recognize that to strike out on their own risks potential turf conflicts with criminal groups. Trafficking in stolen automobiles is big business in the region, and Paraguayan authorities estimate that out of 450,000 vehicles registered annually in that country, more than half are obtained illegally[108]. Some vehicles are smuggled all the way from their manufacturers in South East Asia and United States across the Pacific to the Chilean port of Iquique before being forwarded via truck to Paraguay. Some end up heading west and north-west to Bolivia and even further north if they are required as currency by drug traffickers in those countries. Clearly, the same routes used by the car-traffickers may be used by terrorists who need to transport people or goods in preparation for their attacks[109]. Although official Paraguayan sources are reluctant to admit that possibility, they do acknowledge that the car smuggling routes have also been used for weapons and illegal drugs[110]. There is a clear link between Hong Kong-based criminal groups that specialize in large-scale trafficking of counterfeit products such as music albums and software, and the Hezbollah cells active in the Tri-Border Area. Within their supplier-customer relationship, the Hong Kong crime groups smuggle contraband goods into the region and deliver them to Hezbollah operatives, who in turn profit from their sale. The proceeds are then used to fund the terrorist groups.[111] There is also evidence that Hezbollah has sent millions of dollars raised in the Tri-Border Area to Canada, Lebanon, and elsewhere.[112] That money comes from organized crime, fundraising and extortion within the Arab communities, arms smuggling, and an illicit market currency market. There are many other examples of terrorists linked to criminal activities in the Tri-Border Area. A local Hamas cell, which is associated with counterfeiting and drugs smuggling, is led by a man named Ayman Ghotme, who has also been a fundraiser in the Tri-Border Area for the Holy Land Foundation, a Texas-based Islamic charity that U.S. authorities closed after Sept. 11 for connections to terrorist financing.[113] Links between local crime groups and the Colombian terror group FARC date back to the mid-1990s, when Paraguayan General Oviedo protected the leading Brazilian drug trafficker Luiz Fernando Da Costa. In 2001, Da Costa was arrested in Colombia together with members of a FARC cell.[114] Before he was captured, he had sold arms to FARC in exchange for cocaine[115].

Open activities in the legitimate economy The knowledge and skills potential of CDE is tremendous; one of the recent cases investigated by the Central Bank of Paraguay involved counterfeit Iraqi currency. Business intelligence is so good that a few years ago, faked versions of famous French perfumes were available for purchase in CDE even before they were officially inaugurated in Paris[116]. The Galeria

Page shopping mall in CDE was partly owned by the Hezbollah financier Assad Ahmad Barakat. Investigations into the Buenos Aires bombings in 1992 and 1994 discovered that the mall was used as a front for that organization's crime operations. While no specific examples exist to connect terrorist and criminal groups through the purchase of legal goods and services, it is obvious that the likelihood of this is high, given how the CDE economy is saturated with organized crime.

Support or sustaining activities The Tri-Border Area has an usually large and efficient transport infrastructure, which naturally assists organized crime. In turn, the many criminals and terrorists using cover require a sophisticated and reliable document forgery industry. The ease with which these documents can be obtained in CDE is an indicator of cooperation between terrorists and criminals. In February 2002, the entire Tri-Border Area was searched by local law enforcement and international intelligence agencies in pursuit of five Afghanis believed to be linked with Taliban and Al Qaeda. Each of them was believed to use three or four sets of identity documents.[117] The fact that terrorist leaders travel quite freely into the Tri-Border Area is further evidence of potentially close relations between terrorist groups and criminal groups through highly-positioned governmental contacts. Khalid Sheikh Mohammad, the former number three in Al Qaeda who was captured by U.S. forces in 2003, spent about twenty days in Foz do Iguaçu, the Brazilian sister city of CDE. And Brazilian intelligence services have evidence that Osama bin Laden visited CDE in 1995 and met with the members of the Arab community in the city's mosque to talk about his experience as a mujahadeen fighter in the Afghan war against the Soviet Union.[118] Criminal groups and terrorists in the area have also cooperated on the purchase and shipment of arms. At least two Chinese criminal families based in the Tri-Border Area had been reported engaging in illegal business ventures with the operatives of Egyptian Gamaa Islamiya.[119] One of these, the Sung-I family, is known to have sold munitions to that group in December 2000. The shipment, marked as medical equipment and sent to Egypt, was intercepted in Limassol, Cyprus.

Use of violence Contract murder in CDE costs as little as one thousand dollars, and the frequent violence in CDE is directed at business people who refuse to bend to extortion by terror groups. Ussein Mohamed Taiyen, president of the CDE Chamber of Commerce, was one such victim—murdered because he refused to pay the tax. Another motive is retribution against officials who attempt to crack down on crime. In October 2002, Uruguayan Customs Director Victor Lissidini was shot at by four gunmen on two motorcycles. Lissidini had received threats of revenge for his confiscation of counterfeit materials headed for CDE—calls that were later linked to organized crime groups suspected of working on behalf of Islamist terrorists.[120] Though there is no clear evidence of their cooperation in particular instances of

violent crimes, the targets, the methods, and the explicit reasons behind the attacks suggest a confluence of terrorist and criminal motivations — or potentially the use of common hit men or squads.

Financial transactions and money laundering In 2000, money laundering in the Tri-Border Area was estimated at 12 billion U.S. dollars annually.[121] In 2003, an estimated 50 percent of all banking transactions in CDE were suspected to be of an illicit character. It is not just criminal elements who take advantage of the many international banks and illicit money exchanges. Between 1999 and 2001, at least 50 million U.S. dollars, and some officials say that the amount is probably much higher, was sent from Foz do Iguaçu to extremist Islamic groups through the CDE banks and exchange houses. As many as 261 million U.S. dollars annually has been raised in Tri-Border Area and sent overseas to fund the terrorist activities of Hezbollah, Hamas, and Islamic Jihad.

Use of corruption Most of the illegal activities in the Tri-Border Area bear the hallmark of corruption. In combination with the generally low effectiveness of state institutions, especially in Paraguay, and high level of corruption in that country, CDE appears to be a perfect environment for the logistical operations of both terrorists and organized criminals. Paraguay's government itself is highly corrupt – Transparency International declared Paraguay 129th out of 133 countries in its 2003 Corruption Perceptions Index. Even the few bona fide anti-corruption attempts made by the Paraguayan government have been undermined because of the pervasive corruption, another example being the attempts to crack down on the Chinese criminal groups in CDE. The Consul General of Taiwan in CDE, Jorge Ho, stated that the Chinese groups were successful in bribing Paraguayan judges, effectively neutralizing law enforcement moves against the criminals.[122]

The other watch points described earlier – including fund raising and use of information technology - can also be illustrated with similar indicators of possible cooperation between terror and organized crime.

In sum, for the investigator or analyst seeking examples of perfect conditions for such cooperation, the Tri-Border Area is an obvious choice.

7.2. Crime and terrorism in the Black Sea region[123]

The countries adjoining the Black Sea comprise an interesting mix of cultural, economic, political and social structures. The region is dynamic, with simultaneous and increasing flows of people, goods, and ideas tying the countries to one another. It is also riven with contention. Since the collapse of the Soviet Union, the region has suffered many violent conflicts which have resulted in the displacement of hundreds of thousands of individuals. The on-going conflict in Chechnya (examined in depth in the next case study) has spillover effects on Russia's Black Sea territories. Ukraine has avoided so far the violent conflicts that

have affected Russia, Georgia and Moldova, although the country recently endured a contentious election that threatened to render it in two. Georgia continues to try to consolidate its control over secessionist regions after the democratic Rose Revolution. Turkey has suffered over 40,000 fatalities in the last decades from Kurdish, right-wing and left wing terrorists.[124] Moldova is consumed by poverty and continues to suffer from the festering dispute in the Trans-Dniester region.[125] Further contributing to this tension is the rising ethno-nationalist consciousness among groups like such as the Meskhetian Turks in Crimea, whose Muslim identity have led them to provide support for the Chechen rebels in Russia.[126]

Such stubborn conflicts provide numerous opportunities for the growth of organized crime and terrorism. Government authority has been eroded, even voided, at both the local and national level, creating vacuums that criminal networks thrive in. The numerous trading ties between the countries that have coastlines adjoining the Black Sea, as well as their location astride the overland and sea-based shipping lanes linking Europe to Asia and the Middle East, provide ample opportunities for illicit movement of people and cargo to Europe or Asia. Regional instability as well as growing ties between ethnic minorities engaged in political struggles have made the region a useful one for terrorists to operate within.

Beyond fostering terrorism and organized crime separately, these factors have also driven a dramatic convergence between the two phenomena. Their interaction is more pronounced than in most other regions of the world due to the significant number of ethnic conflicts, the density of criminal and terrorist groups in the region, and the region's strategic geographic location.[127] In some cases, the groups participating in the conflicts started as nationalist rebels have transformed into crime groups, such as groups in Ossetia.[128]

Watch Points

Organizational structures Crime and terror groups alike often incorporate the patronage of the same government officials. During the tenure of Georgian President Eduard Shevardnadze, Minister of the Interior Kakha Targamadze protected crime groups and even received payments from terrorists. According to a former Minister of State Security, Targamadze received significant sums, estimated to be as high as 50,000 U.S. dollars, to permit Chechen fighters to cross Georgia into Abkhazia. Some of these government officials were sometimes also the leaders of organized crime organizations. Before the fall of Aslan Abashidze in Georgia, a leading minister in the Adjaran government ran extensive drug smuggling operations of the region. He was also observed by his subordinates with Chechens and their videos in his office. Both criminals and terrorists share logistical support in the region, including transport links and money laundering vehicles. The Black Sea port of Odessa in Ukraine is used by criminals to move drugs

whereas the illicit weapons trade of individuals like Victor Bout on an Interpol watch list also passes through this port.[129] The conflict region of Abkhazia on the Black Sea has been the locus of massive smuggling of contraband but at the same time has received fighters from Chechnya.

Culture The cultures of the criminals and the terrorist often diverge significantly. Post-Soviet organized crime is characterized by conspicuous consumption. In comparison, while the terrorist lives a life of relative asceticism, enormous physical difficulties and life on the move. Convergence between the two can be seen only in particular circumstances. For example the *tres zmedi*, or Forest Brothers, who fought on the Georgian side of the Abkhazian conflict, lived a primitive life dominated by their military objectives. Now that they have transformed into a cross-border smuggling group, they have continued to live their primitive lifestyles. In other cases, the importance of local community ties allows terrorism and crime to coexist. In villages in the Pankisi Gorge, many of the local Kist Chechens have turned a blind eye to the drug trade and the movement of fighters through their territory because those criminals and terrorists share their cultural background.[130] Likewise, in traditional Kurdish areas of Turkey, community members have tolerated the drug trade as well as the terrorist groups that are resident within their villages.[131]

Illicit or veiled operations Cigarette, drugs and arms smuggling have been major sources of financing of all the terrorist groups in the region. The PKK in Turkey has often worked with crime groups to get its drugs smuggled to market. Cigarette and alcohol smuggling has fueled the Kurdish-Turkish conflict as well as the terrorist violence in both the Abkhaz and Ossetian conflicts. The Transdniester region has maintained and supported the political violence through its very large illicit arms sales.[132] In conflict areas such as Transdniester and Adjaria, top officials supervise the illicit trade that supports terrorism and thus there is no need to conduct veiled operations. But even in regions of political dominance, front companies are used or illegitimate trade is hidden along with the legitimate. A noted cigarette company in Georgia was involved in cigarette smuggling as well as legal cigarette sales. Among the investors in this company were highly suspect Iraqis.[133]

Popular support Until the savagery of the Beslan assault turned many Russian Muslims against them, there was likewise support in many Muslim communities in Russia across the Volga region. Collective memory sustains other Muslim groups, such as the Meskhetian Turks who had been deported by Stalin along with the Chechens provided communities that housed rebel fighters. This is part of the reason that these fighters could obtain shelter and support in the Crimea, Abkhazia and the rebel leaders could be hidden outside of Chechnya for so long without detection.

Support or sustaining activities The terrorists and the criminals in the Black Sea region make significant use of falsified documents including passports, visas and other forms of personal identification.

These activities are supported by corrupt law enforcement, border officials and even diplomatic personnel. In Chechnya, highly sophisticated counterfeiting of U.S. dollars and other currencies has facilitated the financing of terrorism.

Communications and information technology High-level interception equipment, personnel used by the security services and the extensive involvement of former and existing personnel in organized crime has meant that criminals and terrorists have access to high level specialists or even have them within the network structures of their organizations. For example, the inability of the Russian secret services to detect the planning of Chechen terrorist acts or to monitor the movements of many of the top personnel indicates that they have managed to develop effective communication strategies. In Georgia, an amalgam of criminal, terrorist and law enforcement structures exploit technology to protect their financial and political interests. In an illustrative case, the lead researcher on a project exposing the links between smuggling and terrorism was attacked by armed gunmen in his home shortly after his research was presented in Parliament. The assailants, equipped with submachine guns and grenades, arrived at his home less than eight hours after he brought money home from his office to finance a trip to further investigate border smuggling in conflict regions. The only way that the bandits could have known of the money was by monitoring either the researcher's cell phone or his e-mails, or to have bugged the office phone. The political nature of this assault was clear from one gunman's words to a daughter of the researcher: *"We are not criminals, you do not need to fear us."*

Human resources In many of the conflict areas it is difficult to draw a line between those engaged in politically motivated activity and those that are motivated by money. In many case, the same individuals have both goals in mind. Youngsters are sometimes recruited by the crime groups in their neighborhood.[134] Likewise technical specialists, such as the information technology specialists in Ukraine mentioned earlier, are available to those who will pay for their services. They may belong to a community but are not associated with any particular crime or terrorist organization. In the Antalya region of Turkey on the Southern Mediterranean, where money from drug smuggling, corruption and money laundering from the former Soviet Union is funding resort development, businesses are often structured along family lines. Family members involved in money laundering activities bring in siblings and other family members into support activities of the business.

Use of violence In the Black Sea region of Russia and Georgia, it is very hard to differentiate between criminal and terrorist-motivated violence. The merger of the criminal world and the terrorist world blur distinctions. Criminals, as mentioned above in the case of the armed break-in, focus on intimidating individuals who threaten the political and economic interests of others. The involvement of government

officials in the activities of both the criminals and the terrorists, evidenced particularly in law enforcement complicity in the acts of Chechen terrorism, makes it impossible to distinguish between state and private initiated violence.

7.3. Chechnya[135]

Chechnya is a small nation – its people numbered little more than one million in the 2002 census – but it looms large in the strategic, political and crime-related life of Russia and the Caucasus. The history of their relations to Russia over the past two centuries is one of Russian conquest and Chechen resistance, resulting in a passionate national identity that is bolstered by clan and ethnic solidarity. The Chechens' ability to recuperate after mass repression has served as a foundation for the rise of Chechen organized crime and insurgent groups. Furthermore, their very high birth rate of some seven children per woman has meant that the Chechen economy has been unable to absorb all of its young people.

It was a natural progression, therefore, for many Chechens to leave for Russia and other neighboring countries to seek a livelihood there – in crime as well as legitimate activities. Their early activities included extortion and robbery of small traders, moving on to larger enterprises such as profiting from the widespread racketeering by car dealers. The Chechens, by the time of the collapse of the USSR, assumed a central role in organized crime activity occupying hotels and entering into the lucrative entertainment and casino sectors. Their role in human trafficking naturally followed from their activities in the hotel and entertainment sectors. They were among the wealthiest crime groups in the city.[136] From the very beginning, the Chechen separatist movement had close ties with the Chechen crime rings in Russia, mainly operating in Moscow. These crime groups provided and some of them still provide financial support for the insurgents.

Following the declaration of independence and the ensuing collapse of governance in the region in 1991, and through the first war with Russia between 1994 and 1996, the international terror networks such as Al Qaeda gradually became involved in the conflict. This contact was minimal at first, but slowly gained momentum. By the period of de-facto independence between 1996 and 1999, terrorist groups were collaborating closely with Chechen organized crime groups. The second, still ongoing war with Russia has seen a withdrawal of support from some Chechen organized crime groups based outside Chechnya itself that do not support the Islamist and Jihadi terrorist groups working with the Chechens.

Watch points

Organizational structures Chechen organized crime is structured as networks based on neighborhood, military units, or sports clubs. They are also kept together by bonds of kinship between the members, with an obligation of mutual defense and support between the groups. That design is determined by the traditional clan-based structure of Chechen society and centuries of repression. The Chechen organized crime in Moscow were initially formed along these lines, which made them resilient and cohesive compared to their rival Slavic crime groups.[137] In fact there have been no turf conflicts among the Chechen criminal groups. The same applies to the rebel organization in Chechnya: despite different, sometimes contradictory motivations of the different sub-groups in the Chechen resistance (secular separatists, Islamists, bandits, avengers etc.), the rebels maintained operational unity in the first war. In peacetime, however, differences in ideology and desire to maximize profits caused sporadic armed clashes among rival groups, as was the case between secular supporters of then rebel leader Aslan Maskhadov and groups of Islamists between the first and second Chechen wars. With Russia's formidable effort of re-establishing loyal ethnic Chechen leadership in Chechnya, some members and even leaders of groups proved vulnerable and surrendered. Penetration of the Chechen rebel cause by the Arab insurgents who actively proselytized in Chechnya, preaching Muslim brotherhood beyond national and ethnic self-actualization, also had a destructive impact on the Chechens self-concept as a super group.

The crime groups and networks share both similar personnel and structure. This has allowed some of the leaders of Chechen organized crime in the early 1990s to progress swiftly into the upper ranks of the Chechnya-based rebel networks when they were forced to seek refuge from Russian law enforcement. Illustrative of this is Khozh-Ahmet Nukhayev, one of the prominent Chechen figures, who combined participation in organized crime with separatism. While still a student at Moscow State University, Nukhayev helped to organize an illegal group for the liberation of Chechnya. In an interview with the German newspaper *Die Woche*, Nukhayev described how he formed a group of reliable and tough Chechens in the late 1980s to offer Moscow businessmen protection in exchange for acceptance of the Chechens as legitimate business partners. In 1994, Nukhayev was indicted by the federal authorities for extortion and fled Moscow for Chechnya where Dudayev, then president of Chechnya, offered him the position of counter-intelligence chief, which Nukhayev accepted.[138]

Use of violence The preparedness to use strategic, brutal violence is common to Chechen organized crime and terrorist groups. It explains both the success of Chechen organized crime in the turf wars with the Slavic gangs in early 1990s and their perseverance in the face of strong Russian military force. The Chechens continue to perceive themselves as a warrior-based society where fighters often lose their lives for the cause. It is not that they see glory in sacrificing their lives, but the Chechen social subculture pro-

vides a low psychological threshold for massive violent retaliation. This approach is formidably displayed both by Chechen organized crime and terrorists. Chechen gangsters have gained notoriety for being *bespredelshiki*, or 'over the top,' in executing violence and denying rules of engagement and interaction with other gangs.[139] The series of suicide bombings by Chechen terrorists in the past three years is another manifestation of the low valuation of life, allowing for a higher degree of violence (even of that directed against perpetrators.)[140]

Culture Members of both crime and terrorist groups are strongly expected to exhibit trust, based on their local clans and broader ethnic links. This trust makes the close-knit Chechen groups extremely difficult to infiltrate by informers and agents.[141] However, this ethnic solidarity is now being compromised by two groups which are condemned by most Chechens specifically for that reason. The first group is Wahhabi converts who deny fervently the traditional Chechen ethic and behavioral codes and promote radical Islam.[142] However, the separatist rebels have to tolerate Wahhabis in their ranks, since the Wahhabis generate most of the manpower, financial and political support from radical religious circles in Muslim countries. The second group is the so-called *kadyrovtsy*, the Chechen presidential guard led by Ramzan, a son of the late pro-Moscow Chechen leader Akhmad Kadyrov. His group became notorious for cooperating with Russian security officials in Chechnya.

Organizational goals The average Chechen, independent of membership in a particular social or political group, strongly conceives himself also as a member of a super-group – the Chechen people. The goals of the super-group (naturally, its own survival at the moment) and interests of a subgroup (be it organized crime or separatists) remain in a state of a dynamic balance. Obviously, the goal of Chechen organized crime and business outside Chechnya is personal enrichment and preservation of wealth, often seen as protection after years of forced exile under Stalin and a difficult return to their homeland after exile.

The rebels have other objectives. In the short term they seek an end to the Russian military and political presence in Chechnya. In a longer perspective, different factions of the resistance considered different scenarios of their group's existence: from more or less secular state-building to continuation of the jihad in neighboring Russian Muslim-populated territories such as Dagestan, Ingushetia, Karachayevo-Cherkessia and Kabardino-Balkaria, where underground antigovernment Islamist networks are active and politically motivated violence is becoming more acute.

The Chechen resistance can conveniently be presented as consisting of the following three subgroups, with gunmen fluctuating between them or belonging to more than one at once.[143] The first group is the core of the resistance; it unites ideological extremist fighters against the Russian presence in the Caucasus,

both separatists (formerly under Maskhadov[144]) and Islamists (Basayev). The second group is formed by criminals whose motivation is defined by what promises the maximal profit – from participating in paid jihad to oil smuggling to drug trafficking to criminal kidnappings. The third group, the least consistent as a subgroup, includes the avengers who had their family members or loved ones killed, abducted or tortured by Russian servicemen or pro-Russian Chechen police and security guards. The movement of members among these three groups is illustrative of the murky division between crime and terrorism.

Open and illicit activities Since there is no rule of law in Chechnya, the concept of illicit operations has no real meaning. Therefore these two watch points can be treated as one.

Support or sustaining activities Both Chechen criminals and terrorists use false passports, registration certificates (in Moscow) and migrant cards to move around Chechnya, to travel to Russian cities and to cross borders. Their methods of obtaining these documents are similar: bribing police officials or using specialized suppliers connected with corrupt police. The latter method is probably the best since the data on issued documents (passports) will go into the Interior Ministry's central database and their holder will have a new protected identity. The Chechen terrorists who seized the Dubrovka Theater in Moscow in 2002 had obtained false Moscow police registration certificates in this manner, just having bought them from one such firm that belonged to an ethnic Chechen, according to the Moscow police.[145] This fact may indicate possible cooperation in providing support activities, between the members of Chechen organized crime and terrorists. Corruption among law enforcement officials, described later in this case study, is extremely important for the rebels' sustaining activities.

Communications and information technology Chechen terrorists do not attack targets outside Russia, although they conduct fundraising activities abroad, lead the propaganda warfare from web servers located outside Russian borders and welcome foreign recruits. The major means of communication between the rebels in Chechnya and their associates abroad are e-mail (from Basayev and his people to the rebel website Kavkazcenter.com), satellite phones, and audiotapes (e.g. those from the late Maskhadov[146] to an envoy in London, Zakayev, or Radio Free Europe).

Popular support The ideology of the Chechen resistance has changed over time in an apparent effort to develop a broader base of sympathizers and, therefore, political and financial support for the cause. In the first war from 1994 to 1996, nationalist sentiment overwhelmingly dominated religious ones. Since the onset of the second war, the jihad motives have all but wiped out the original idea of a secular independent republic. Now, there is an obvious split in the resistance, allowing the terrorists to subscribe to both ideals. Basayev frames his activities as jihad with the final aim of creating an Islamic state in the Caucasus, from the Black Sea to the Caspian, while Maskhadov limited his mission to obtaining independent status for

Chechnya—the latter being a more moderate objective that may be lost since Russian forces killed Maskhadov on 8 March 2005.[147] Such division of missions and ideologies allowed the Chechen cause to enjoy sympathies of many European governments that first semi-officially acknowledged the diplomatic and political status of the late Maskhadov's envoys, as well as those of the Islamic world which remains the main source of financial and manpower support for what it deems 'jihad' in Chechnya.

The Russia-based Chechen organized crime of the early 1990s has not attempted to assert itself as an entity with legitimate claims in Russia. However, as Chechen businessmen have acquired stakes in the legitimate economy, they have begun to position themselves as leaders of the Chechen diasporas in Russian cities (i.e., Saidullayev, Djabrailov in Moscow, Sayid Tsentroyev in Samara) and then as Chechen politicians reflecting the aspirations of the pro-Moscow Chechens. The artificiality of such pretensions is obvious: although Saidullayev heads a self-proclaimed State Council of Chechnya, and Djabrailov represents Chechnya in the Federation Council (the upper chamber of the Russian parliament), neither has an armed power base and, therefore, lacks any real influence in Chechnya. However, high official status and wide political exposure make their businesses less vulnerable to crackdowns by law enforcement.

Human resources Both Chechen organized crime and the rebels have been recruiting mainly from one pool of human resources – the predominantly rural Chechen youth. By the end of the 1980s, unemployment was growing rapidly as the rate of increase in population was about 5 times higher than the rate of increase in jobs. Chechens had one of the highest birth rates of any group in Russia. Two thirds of the Chechen population was living below the poverty line.[148] These poor prospects for young people, the high social standing that wealth brings in Chechen society, the prejudice against Chechens in Russian society and the subculture of violence and mistrust toward non-Chechens provided significant motivation for young people to join the Chechen underworld. In the early years of the Chechen crime rings in Russia, which were engaged mainly in providing criminal protection, no specific requirements were expected from the recruits other than the deployment of violence and loyalty to tribe or clan.

A similarly spontaneous approach to recruitment dominated the formation of the separatist militia before and during the first war in Chechnya. The advent of the Arab fighters has brought systemic elements in the recruitment and training of terrorists. In the period of Chechnya's de-facto independence (1996-1999), the separatist envoys were actively recruiting young males in mosques and madrassas in the Muslim-populated Russian regions.[149] Also, the fact that the training in Chechnya was unobstructed by Maskhadov's government that was itself being quickly radicalized along the religious lines, attracted jihad volunteers from abroad.[150] Most of the trainees opted to stay in Chechnya; however, some of them returned to

Russia or joined terrorist rings abroad. Official Russian estimates put the number of volunteers trained in the camps in Chechnya between the two wars at around 20,000.[151]

Financial transactions and money laundering At the outbreak of the second war in Chechnya in 1999, senior Russian officials stressed the importance of Chechen organized crime and business in financing terrorists in Chechnya. Organized crime activities of Chechens, in fact, were the major justification behind the first military crackdown on Chechnya in 1994. The Russian Tax Police estimated that most of the financing for Chechen rebels comes from Chechen organized criminal groups, which controlled more than 2,000 private companies and banks across Russia in 1999. *Rossiiskaya Gazeta* quoted a deputy director of this service, Aslanbek Khaupshev, on November 20, 1999 as saying that dozens of companies that Chechens control in Moscow alone were involved in laundering money, some of which went to finance Chechen separatism. One scheme, which was exposed by the Russian tax police, provided for oil to be shipped from primitive oil refineries in Chechnya to be illegally sold through a firm in neighboring Dagestan. The refineries were owned by Chechnya-based Islamist warlords Shamil Basayev and al-Khattab (a non-Chechen Arab jihadist). By the end of 1999, the tax police had ruptured 'illegal channels of financing' that were set up by Chechen organized crime groups in Primorskii Krai, Astrakhan, Novgorod and Lipetsk regions. The police also exposed twelve companies owned by the so-called Wahabbis in Karachayevo-Cherkessia.[152]

Russian authorities have been blaming foreign sources of finance for the struggle in Chechnya since the mid 1990s when the Russian press reported complaints of the Russian government to the Saudis concerning their support for the Chechen movement. This element of Chechen financing has been emphasized since the U.S. launched a global effort against international terrorism. It has become especially useful for Russian policy-makers to portray Chechnya as part of the global jihad, rather than an internal Russian conflict, especially given the links between the Chechen rebels and foreign extremist and terrorist organizations. Russian officials claim that the largest sponsor of the Chechen rebels is Al Qaeda, which has donated, by different unconfirmed accounts in the Russian and foreign press, from 10 to 30 million U.S. dollars. Basayev said after the Beslan attack that he received no funds from Al Qaeda, but would accept them if offered. Another big donor, the FSB said, is a Saudi-based charity al-Haramain Islamic Foundation.[153] This allegation was independently confirmed by the U.S. government, which froze assets held by al-Haramain in Oregon and Missouri in February 2004, after the FBI had averted an attempt to illegally transfer 131 thousand dollars to 'Muslim fighters or refugees,' according to a court affidavit.[154] The head of another U.S.-based Islamic charity, Benevolence International, was convicted in the U.S. in 2003 for links

to bin Laden and reportedly wired hundreds of thousands of dollars to the Chechen rebels and supplied them with anti-mine boots.[155]

Other sources of Chechen terrorist funding that are regularly cited by Russian officials are unnamed public and private organizations in Turkey and Saudi Arabia. The Russian foreign minister recently said that the late Zelimhan Yandarbiyev, Dudayev's vice-president who had been living in Qatar for several years, was the key man in the fund-raising network of the Chechen terrorists.[156] This information, about money coming both from the Chechen diasporas in Muslim countries and also from jihad supporters among charities and Muslim public organizations, was recently confirmed by several Chechen insiders in Turkey and international crime experts.[157]

Use of corruption Given that corruption is a social norm in Russia and the former Soviet republics surrounding Chechnya, it is extremely difficult to distinguish the features of the phenomenon that would clearly indicate convergence or divergence of the Chechen organized crime and terror groups. Corruption is so widespread and the number of its channels and actors is virtually unlimited, so it is hard to point at some specific instances and claim them to be critical. Both groups use corruption for obtaining false documents, suggesting corrupt Interior officers. Corruption also secures passage of people and cargoes within Chechnya, across its border, within Russia and across Russia; suggesting corruption among military and police personnel. Judicial corruption is suggested by the release of those arrested, or the reduction in prison sentences. Also, intelligence can be gleaned from corrupt police officers. In some cases Chechen organized crime and terrorists cooperated in maintaining and funding corrupt officialdom in a failing state in order to create a territorial safe haven, or to exploit the political situation for generation of money. In the de-facto independent Chechnya of 1996-1999, terrorists who appropriated organized crime activities were intertwined with local organized crime. Their cooperative endeavors included intimidating Maskhadov's government, which kept it from interfering in criminal kidnappings, participating in diversion and illegal trading in oil, or trafficking narcotics. In 2000-2002, Chechen rebels and criminals who settled in Georgia's Pankisi Gorge were successful in neutralizing local and Tbilisi officials and could pursue drug-dealing and kidnapping activities in Georgia virtually unobstructed.

The resilience of the illegal oil business in Chechnya, now reportedly controlled by top Russian military personnel in Chechnya, could easily be undermined if the rebels' attacked the extremely vulnerable oil infrastructure. The on-going transport of oil suggests cooperation, or at least agreement, between the corrupt Russian military officials and the rebels. The fact of such cooperation was repeatedly brought up by the late pro-Russian Chechen president Akhmad Kadyrov, even with Russia's president Vladimir Putin; however, no reports of criminal investigations into diversion of oil have ever surfaced. The issue of possi-

ble cooperation between Chechen terror and crime networks in obtain WMD requires special attention. Chechen criminals are not likely to be involved in seeking WMD as they might face even more violent retaliation. But as their acts of terrorism escalate and conventional terror fails to advance their goals—they might resort to extreme acts and corrupt individuals to obtain access to WMD.

There are recorded occasions that could indicate such a threat. In March 2002, law enforcement personnel in the Sverdlovsk region arrested three Chechens who had been allegedly trying to sell weapons and explosives. One of the arrested Chechens carried a valid pass to a high-security community inhabited by workers of a local nuclear facility. However, the pass holder could have used it only to enter the community of Lesnoi, but would not have been able to access the facility where nuclear warheads are manufactured. A search of the apartment of arrested Chechens revealed more weapons, a remote-control bomb, and a book by the late Maskhadov entitled *Honor is More Valuable than Life*, a circumstance suggesting the allegiance of the arrested Chechens to the rebel cause.[158]

In another instance, in October 2002, the FSB arrested an officer of a special unit guarding the Kalininskaya nuclear power plant in the Tver region. FSB agents found a map that identified all of the plant's 'secret facilities,' as well as a list of coded phone numbers on the officer. When FSB agents decoded the phone numbers, they reported that the numbers belonged to 'natives of Chechnya.'[159]

As in the Black Sea and Tri-border areas, it is often hard to clearly differentiate between the crime groups and the terrorists. Although the terrorist activity of the Chechens is confined to Russia, the crime activity is transnational. Therefore, we are observing points of convergence that are important and can be useful to law enforcement. The recent discover by Los Angeles law enforcement of Chechen crime groups funding terrorist activity through their U.S. based pornography business highlights the importance of understanding this phenomenon and its possible manifestations in the United States. As shown in the body of the report, terrorist-crime activity observed overseas often subsequently manifests itself in similar form within the United States.

8. Conclusion and recommendations

The many examples in this report of cooperation between terrorism and organized crime make clear that the links between these two potent threats to national and global security are widespread, dynamic, and dangerous. It is only rational to consider the possibility that an effective organized crime group may have a connection with terrorists that has gone unnoticed so far.

Our key conclusion is that crime is not a peripheral issue when it comes to investigating possible terrorist activity. Efforts to analyze the phenomenon of terrorism without considering the crime component undermine all counter-terrorist activities, including those aimed at protecting sites containing weapons of mass destruction.

Yet the staffs of intelligence and law enforcement agencies in the United States are already overwhelmed. Their common complaint is that they do not have the time to analyze the evidence they possess, or to eliminate unnecessary avenues of investigation. The problem is not so much a dearth of data, but the lack of suitable tools to evaluate that data and make optimal decisions about when, and how, to investigate further.

The PIE method – along with the relevant tools described in the appendix to this report – offers a practical solution to this serious dilemma. Our Georgia case study and our analysis of Russian closed cities using this method have revealed valuable insights that were not previously apparent to law enforcement or security experts.

Yet the use of these new tools to replace some outdated tools has much broader implications than mere efficiency. By implementing PIE, intelligence and law enforcement agencies will be introducing a crucial new aspect to strategies to deal with terrorism and organized crime. Scrutiny and analysis of the interaction between terrorism and organized crime will become a matter of routine best practice. Awareness of the different forms this interaction takes, and the dynamic relationship between them, will become the basis for crime investigations, particularly for terrorism cases. Policy and planning decisions, too, will be guided by this tenet.

In conclusion, our overarching recommendation is that crime analysis must be central to understanding the patterns of terrorist behavior and cannot be viewed as a peripheral issue. Furthermore, resources diverted from the fight against transnational organized crime in the post September 11th era are giving criminals a greater chance to operate and even provide services to terrorists.

Other recommendations include:

For policy analysts:

1. More detailed analysis of the operation of illicit economies where criminals and terrorists interact would improve understanding of how organized crime operates, and how it cooperates with terrorists. Domestically, more detailed analysis of the businesses where illicit transactions are most common would help investigation of organized crime – and its affiliations. More focus on the illicit activities within closed ethnic communities in urban centers and in prisons in developed countries would prove useful in addressing potential threats.
2. Corruption overseas, which is so often linked to facilitating organized crime and terrorism, should be elevated to a U.S. national security concern with an operational focus. After all, many jihadists are recruited because they are disgusted with the corrupt governments in their home countries. Corruption has facilitated the commission of criminal acts such as the Chechen suicide bombers who bribed airport personnel to board aircraft in Moscow.
3. Analysts must study patterns of organized crime-terrorism interaction as guidance for what may be observed subsequently in the United States. For instance, Hezbollah smuggling of cigarettes in the Tri-Border Area was subsequently found in North Carolina.
4. Intelligence and law enforcement agencies need more analysts with the expertise to understand the motivations and methods of criminal and terrorist groups around the globe, and with the linguistic and other skills to collect and analyze sufficient data.

For investigators:

1. The separation of criminals and terrorists is not always as clear cut as many investigators believe. Crime and terrorists groups are often indistinguishable in conflict zones and in prisons. They also have overlaps such as in the recent large-scale IRA attack on a bank.
2. The hierarchical structure and conservative habits of the Sicilian Mafia no longer serves as an appropriate model for organized crime investigations. Most organized crime groups now operate as loose networked affiliations. In this respect they have more in common with terrorist groups.
3. The PIE method provides a series of indicators that can result in superior profiles and higher-quality risk analysis for law enforcement agencies both in the United States and abroad. The approach can be refined with sensitive or classified information.
4. Greater cooperation between the military and the FBI would allow useful sharing of intelligence, such as the substantial knowledge on crime and illicit transactions gleaned by the counterintelligence branch of the U.S. military that is involved in conflict regions where terror-crime interaction is most profound.

5. Law enforcement personnel must develop stronger working relationships with the business sector. In the past, there has been too little cognizance of possible terrorist-organized crime interaction among the clients of private-sector business corporations and banks. Law enforcement must pursue evidence of criminal affiliations with high status individuals and business professionals who are often facilitators of terrorist financing and money laundering. In the spirit of public-private partnerships, corporations and banks should be placed under an obligation to watch for indications of organized crime or terrorist activity by their clients and business associates. Furthermore they should attempt to analyze what they discover and to pass on their assessment to law enforcement. The need for this was dramatically illustrated by the Riggs Bank case in late 2004.
5. Law enforcement must work more with different sectors of the business community which are emerging sectors for money laundering connected with terrorist financing, i.e., real estate and art. Businesses have been writing off the cost of credit card losses, even while they conduct valuable analyses to establish patterns of these and other financial crimes. In fact, credit card fraud is becoming a major funding source for international terrorists. Law enforcement analysts should work more closely with corporations to understand the trends that highlight organized crime-terror involvement in this emerging area.
6. Law enforcement personnel posted overseas by federal agencies such as the DEA, the Department of Justice, the Department of Homeland Security, and the State Department's Bureau of International Narcotics and Law Enforcement should be tasked with helping to develop a better picture of the geography of organized crime and its most salient features (i.e. the watch points of the PIE approach). This should be used to assist analysts in studying patterns of crime behavior that put American interests at risk overseas and alert law enforcement to crime patterns that may shortly appear in the U.S.
7. Training for law enforcement officers at federal, state, and local level in identifying authentic and forged passports, visas, and other documents required for residency in the U.S. would eliminate a major shortcoming in investigations of criminal networks.

Appendix: Analytical tools for implementing PIE[160]

To implement and refine the *preparation of the investigation environment* (PIE) methodology and techniques, the TraCCC team anticipated that the audience of this report might seek to use semi-automated tools and their numerous heterogeneous data sources to provide geographic and temporal details of terror-crime interaction. This Appendix is intended to provide an assessment of existing tools and how investigators and analysts might combine them with the PIE approach. The audience that this report targets include software developers (architects), analysts and investigators in academia and government who employ decision support tools and analytical aids in their day-to-day operations (users) and managers like chief technology officers and chief information officers (customers).

Informed by the PIE watch points and indicators, the application of technology becomes a process of discovering organizational and personal relationships by examining physical and digital evidence of terror-crime interaction such as surveillance reports, shipping manifests and e-mails. Semi-automated tools that supply collaborative data visualization, structured argumentation, process/intent models, network/link analysis functionality and more can greatly aid researchers, investigating officers and intelligence analysts (hereafter referred to collectively as investigators).

This appendix provides a focused assessment of the information gathering and analysis tools that investigators implementing the PIE approach can use. While most of these tools are currently available and in use by the law enforcement community, the TraCCC team also examined additional tools that could evolve to a commercial or government off-the-shelf (COTS/GOTS) level of maturity in 12 to 24 months of development effort. The approach taken for this study took the following steps:

- Define the PIE analytical process to provide a context for the tool requirements discussion;
- Define a tool space that supports the mapping of tool requirements to key dimensions (e.g., the number of people who will be collaborating with the tool);

Each step in the analytical process:

- Identifies tool requirements that are focused on that step;
- Generates examples of how these tools might be used; and
- Develops a list of exemplar tools with a short description for each.

Although requirements are highlighted for each of the tool categories throughout this document, many requirements cut across categories.

A.1 Defining the PIE Analytical Process

In order to begin identifying the tools to support the analytical process, the process of analysis itself first had to be captured. The TraCCC team adopted Max Boisot's (2003) I-Space as a representation for describing the analytical process. As Figure A-1 illustrates, I-Space provides a three-dimensional representation of the cognitive steps that constitute analysis in general and the utilization of the PIE methodology in particular. The analytical process is reduced to a series of logical steps, with one step feeding the next until the process starts anew. The steps are:

1. Scanning
2. Codification
3. Abstraction
4. Diffusion
5. Validation
6. Impacting

Over time, repeated iterations of these steps result in more and more PIE indicators being identified, more information being gathered, more analytical product being generated, and more recommendations being made. Boisot's I-Space is described below in terms of law enforcement and intelligence analytical processes.

A.1.1. Scanning

The analytical process begins with scanning, which Boisot defines as the process of identifying threats and opportunities in generally available but often fuzzy data. For example, investigators often scan available news sources, organizational data sources (e.g. intelligence reports) and other information feeds to identify patterns or pieces of information that are of interest. Sometimes this scanning is performed with a clear objective in mind (e.g., set up through profiles to identify key players). From a tools perspective, scanning with a focus on a specific entity like a person or a thing is called a subject-based query. At other times, an investigator is simply reviewing incoming sources for pieces of a puzzle that is not well understood at that moment. From a tools perspective, scanning with a focus on activities like money laundering or drug trafficking is called a pattern-based query. For this type of query a specific subject is not the target, but a sequence of actors/activities that form a pattern of interest.

Many of the tools described herein focus on either:

- Helping an investigator build models for these patterns then comparing those models against the data to find 'matches', or
- Supporting automated knowledge discovery where general rules about interesting patterns are hypothesized and then an automated algorithm is employed to search through large amounts of data based on those rules.

The choice between subject-based and pattern-based queries is dependent on several factors including the availability of expertise, the size of the data source to be scanned, the amount of time available and, of course, how well the subject is understood and anticipated. For example, subject-based queries are by nature more tightly focused and thus are often best conducted through keyword or Boolean searches, such as a Google search containing the string "Bin Laden" or "Abu Mussab al-Zarqawi." Pattern-based queries, on the other hand, support a relationship/discovery process, such as an iterative series of Google searches starting at 'with all of the words' terrorist, financing, charity, and hawala, proceeding through 'without the words' Hezbollah and Iran and culminating in 'with the exact phrase' Al Qaeda Wahabi charities. Regardless of which is employed, the results provide new insights into the problem space. The construction, employment, evaluation, and validation of results from these various types of scanning techniques will provide a focus for our tool exploration.

A.1.2. Codification

In order for the insights that result from scanning to be of use to the investigator, they must be placed into the context of the questions that the investigator is attempting to answer. This context provides structure through a codification process that turns disconnected patterns into coherent thoughts that can be more easily communicated to the community. The development of indicators is an example of this codification. Building up network maps from entities and their relationships is another example that could support indicator development. Some important tools will be described that support this codification step.

A.1.3. Abstraction

During the abstraction phase, investigators generalize the application of newly codified insights to a wider range of situations, moving from the specific examples identified during scanning and codification towards a more abstract model of the discovery (e.g., one that explains a large pattern of behavior or predicts future activities). Indicators are placed into the larger context of the behaviors that are being monitored. Tools that support the generation and maintenance of models that support this abstraction process

will be key to making the analysis of an overwhelming number of possibilities and unlimited information manageable.

A.1.4. Diffusion

Many of the intelligence failures cited in the 9/11 Report were due to the fact that information and ideas were not shared. This was due to a variety of reasons, not the least of which were political. Technology also built barriers to cooperation, however. Information can only be shared if one of two conditions is met. Either the sender and receiver must share a context (a common language, background, understanding of the problem) or the information must be coded and abstracted (see steps 2 and 3 above) to extract it from the personal context of the sender to one that is generally understood by the larger community. Once this is done, the newly created insights of one investigator can be shared with investigators in sister groups.

The technology for the diffusion itself is available through any number of sources ranging from repositories where investigators can share information to real-time on-line cooperation. Tools that take advantage of this technology include distributed databases, peer-to-peer cooperation environments and real-time meeting software (e.g., shared whiteboards).

A.1.5. Validation

In this step of the process, the hypotheses that have been formed and shared are now validated over time, either by a direct match of the data against the hypotheses (i.e., through automation) or by working towards a consensus within the analytical community. Some hypotheses will be rejected, while others will be retained and ranked according to probability of occurrence. In either case, tools are needed to help make this match and form this consensus.

A.1.6. Impacting

Simply validating a set of hypotheses is not enough. If the intelligence gathering community stops at that point, the result is a classified CNN feed to the policy makers and practitioners. The results of steps 1 through 5 must be mapped against the opposing landscape of terrorism and transnational crime in order to understand how the information impacts the decisions that must be taken. In this final step, investigators work to articulate how the information/hypotheses they are building impact the overall environment and make recommendations on actions (e.g., probes) that might be taken to clarify that environment. The consequences of the actions taken as a result of the impacting phase are then identified during the scanning phase and the cycle begins again.

A.1.7. An Example of the PIE Analytical Approach

While section 4 provided some real-life examples of the PIE approach in action, a retrodictive analysis of terror-crime cooperation in the extraction, smuggling, and sale of conflict diamonds provides a grounding example of Boisot's six step analytical process. Diamonds from West Africa were a source of funding for various factions in the Lebanese civil war since the 1980s. Beginning in the late 1990s intelligence, law enforcement, regulatory, non-governmental, and press reports suggested that individuals linked to transnational criminal smuggling and Middle Eastern terrorist groups were involved in Liberia's illegal diamond trade. We would expect to see the following from an investigator assigned to track terrorist financing:

1. **Scanning:** During this step investigators could have assembled fragmentary reports to reveal crude patterns that indicated terror-crime interaction in a specific region (West Africa), involving two countries (Liberia and Sierra Leone) and trade in illegal diamonds.
2. **Codification:** Based on patterns derived from scanning, investigators could have codified the terror-crime interaction by developing explicit network maps that showed linkages between Russian arms dealers, Russian and South American organized crime groups, Sierra Leone insurgents, the government of Liberia, Al Qaeda, Hezbollah, Lebanese and Belgian diamond merchants, and banks in Cyprus, Switzerland, and the U.S..
3. **Abstraction:** The network map developed via codification is essentially static at this point. Utilizing social network analysis techniques, investigators could have abstracted this basic knowledge to gain a dynamic understanding of the conflict diamond network. A calculation of degree, betweeness, and closeness centrality of the conflict diamond network would have revealed those individuals with the most connections within the network, those who were the links between various subgroups within the network, and those with the shortest paths to reach all of the network participants. These calculations would have revealed that all the terrorist links in the conflict diamond network flowed through Ibrahim Bah, a Libyan-trained Senegalese who had fought with the mujahadeen in Afghanistan and whom Charles Taylor, then President of Liberia, had entrusted to handle the majority of his diamond deals. Bah arranged for terrorist operatives to buy all diamonds possible from the RUF, the Charles Taylor-supported rebel army that controlled much of neighboring civil-war-torn Sierra Leone. The same calculations would have delineated Taylor and his entourage as the key link to transnational criminals in the network, and the link between Bah and Taylor as the essential mode of terror-crime interaction for purchase and sale of conflict diamonds.

4. **Diffusion:** Disseminating the results of the first three analytical steps in this process could have alerted investigators in other domestic and foreign law enforcement and intelligence agencies to the emergent terror-crime nexus involving conflict diamonds in West Africa. Collaboration between various security services at this junction could have revealed Al Qaeda's move into commodities such as diamonds, gold, tanzanite, emeralds, and sapphires in the wake of the Clinton Administration's freezing of 240 million dollars belonging to Al Qaeda and the Taliban in Western banks in the aftermath of the August 1998 attacks on the U.S. embassies in Kenya and Tanzania. In particular, diffusion of the parameters of the conflict diamond network could have allowed investigators to tie Al Qaeda fund raising activities to a Belgian bank account that contained approximately 20 million dollars of profits from conflict diamonds.
5. **Validation:** Having linked Al Qaeda, Hezbollah, and multiple organized crime groups to the trade in conflict diamonds smuggled into Europe from Sierra Leone via Liberia, investigators would have been able to draw operational implications from the evidence amassed in the previous steps of the analytical process. For example, Al Qaeda diamond purchasing behavior changed markedly. Prior to July 2001 Al Qaeda operatives sought to buy low in Africa and sell high in Europe so as to maximize profit. Around July they shifted to a strategy of buying all the diamonds they could and offering the highest prices required to secure the stones. Investigators could have contrasted these buying patterns and hypothesized that Al Qaeda was anticipating events which would disrupt other stores of value, such as financial instruments, as well as bring more scrutiny of Al Qaeda financing in general.
6. **Impacting:** In the wake of the 9/11 attacks, the hypothesis that Al Qaeda engaged in asset shifting prior to those strikes similar to that undertaken in 1999 has gained significant validity. During this final step in the analytical process, investigators could have created a watch point involving a terror-crime nexus associated with conflict diamonds in West Africa, and generated the following indicators for use in future investigations:
    - Financial movements and expenditures as attack precursors;
    - Money as a link between known and unknown nodes;
    - Changes in the predominant patterns of financial activity;
    - Criminal activities of a terrorist cell for direct or indirect operational support;
    - Surge in suspicious activity reports.

A.2. The tool space

The key to successful tool application is understanding what type of tool is needed for the task at hand. In order to better characterize the tools for this study, we have divided the tool space into three dimensions:

- **An abstraction dimension**: This continuum focuses on tools that support the movement of concepts from the concrete to the abstract. Building models is an excellent example of moving concrete, narrow concepts to a level of abstraction that can be used by investigators to make sense of the past and predict the future.
- **A codification dimension:** This continuum attaches labels to concepts that are recognized and accepted by the analytical community to provide a common context for grounding models. One end of the spectrum is the local labels that individual investigators assign and perhaps only that they understand. The other end of the spectrum is the community-accepted labels (e.g., commonly accepted definitions that will be understood by the broader analytical community). As we saw earlier, concepts must be defined in community-recognizable labels before the community can begin to cooperate on those concepts.
- **The number of actors:** This last continuum talks in term of the number of actors who are involved with a given concept within a certain time frame. Actors could include individual people, groups, and even automated software agents. Understanding the number of actors involved with the analysis will play a key role in determining what type of tool needs to be employed.

Although they may appear to be performing the same function, abstraction and codification are not the same. An investigator could build a set of models (moving from concrete to abstract concepts) but not take the step of changing his or her local labels. The result would be an abstracted model of use to the single investigator, but not to a community working from a different context. For example, one investigator could model a credit card theft ring as a petty crime network under the loose control of a traditional organized crime family, while another investigator could model the same group as a terrorist logistic support cell.

The analytical process described above can now be mapped into the three-dimensional tool space, represented graphically in Figure A-1. So, for example, scanning (step 1) is placed in the portion of the tool space that represents an individual working in concrete terms without those terms being highly codified (e.g., queries). Validation (step 5), on the other hand, requires the cooperation of a larger group working with abstract, highly codified concepts.

Being able to identify both the step in the analytical process and the portion of the tool space will provide a context against which groups and individual tools may be discussed.

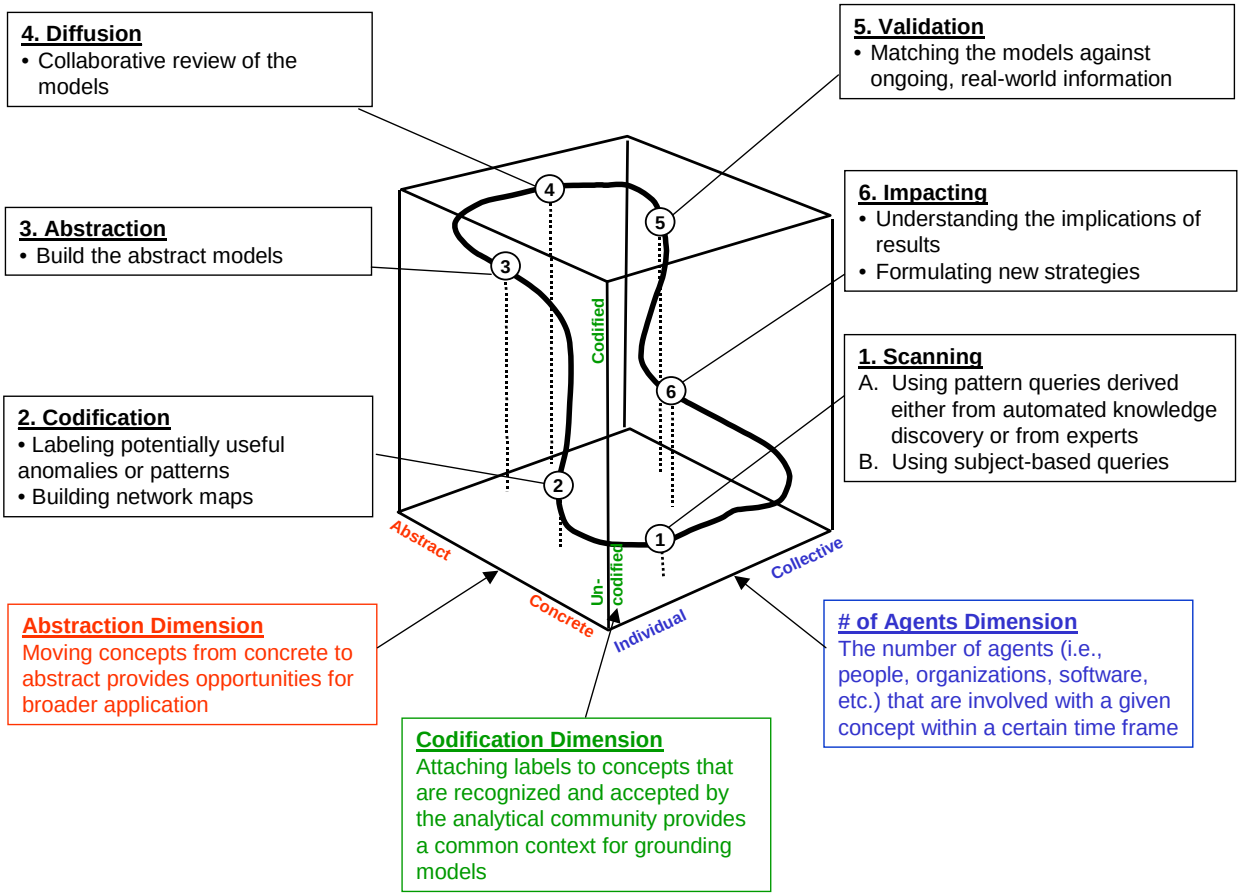

Figure A-1: Analytical Cycle [adapted from Boisot, 2003]

A.2.1. Scanning tools

Investigators responsible for constructing and monitoring a set of indicators could begin by scanning available data sources - including classified databases, unclassified archives, news archives, and internet sites - for information related to the indicators of interest. As can be seen from exhibit 6, all scanning tools will need to support requirements dictated by where these tools fall within the tool space. Scanning tools should focus on:

- How to support an individual investigator as opposed to the collective analytical community. Investigators, for the most part, will not be performing these scanning functions as a collaborative effort;

- Uncoded concepts, since the investigator is scanning for information that is directly related to a specific context (e.g., money laundering), then the investigator will need to be intimately familiar with the terms that are local (uncoded) to that context;
- Concrete concepts or, in this case, specific examples of people, groups, and circumstances within the investigator's local context. In other words, if the investigator attempts to generalize at this stage, much could be missed.

Using these criteria as a background, and leveraging state-of-the-art definitions for data mining, scanning tools fall into two basic categories:

- Tools that support subject-based queries are used by investigators when they are searching for specific information about people, groups, places, events, etc.; and
- Investigators who are not as interested in individuals as they are in identifying patterns of activities use tools that support pattern-based queries.

This section briefly describes the functionality in general, as well as providing specific tool examples, to support both of these critical types of scanning.

A.2.1.1. Subject-based queries

Subject-based queries are the easiest to perform and the most popular. Examples of tools that are used to support subject-based queries are Boolean search tools for databases and internet search engines.

Functionalities that should be evaluated when selecting subject-based query tools include that they are easy to use and intuitive to the investigator. Investigators should not be faced with a bewildering array of 'ifs', 'ands', and 'ors', but should be presented with a query interface that matches the investigator's cognitive view of searching the data. The ideal is a natural language interface for constructing the queries. Another benefit is that they provide a graphical interface whenever possible. One example might be a graphical interface that allows the investigator to define subjects of interest, then uses overlapping circles to indicate the interdependencies among the search terms. Furthermore, query interfaces should support synonyms, have an ability to 'learn' from the investigator based on specific interests, and create an archive of queries so that the investigator can return and repeat. Finally, they should provide a profiling capability that alerts the investigator when new information is found based on the subject.

Subject-based query tools fall into three categories: queries against databases, internet searches, and customized search tools. Examples of tools for each of these categories include:

- **Queries from news archives:** All major news groups provide web-based interfaces that support queries against their on-line data sources. Most allow you to select the subject, enter keywords, specify date ranges, and so on. Examples include the New York Times (at http://www.nytimes.com/ref/membercenter/nytarchive.html) and the Washington Post (at http://pqasb.pqarchiver.com/washingtonpost/search.html). Most of these sources allow you to read through the current issue, but charge a subscription for retrieving articles from past issues.
- **Queries from on-line references:** There are a host of on-line references now available for query that range from the Encyclopedia Britannica (at http://www.eb.com/) to the CIA's World Factbook (at http://www.cia.gov/cia/publications/factbook/). A complete list of such references is impossible to include, but the search capabilities provided by each are clear examples of subject-based queries.
- **Search engines**: Just as with queries against databases, there are a host of commercial search engines available for free-format internet searching. The most popular is Google, which combines a technique called citation indexing with web crawlers that constantly search out and index new web pages. Google broke the mold of free-format text searching by not focusing on exact matches between the search terms and the retrieved information. Rather, Google assumes that the most popular pages (the ones that are referenced the most often) that include your search terms will be the pages of greatest interest to you. The commercial version of Google is available free of charge on the internet, and organizations can also purchase a version of Google for indexing pages on an intranet. Google also works in many languages. More information about Google as a business solution can be found at http://www.google.com/services/. Although the current version of Google supports many of the requirements for subject-based queries, its focus is quick search and it does not support sophisticated query interfaces, natural language queries, synonyms, or a managed query environment where queries can be saved. There are now numerous software packages available that provide this level of support, many of them as add-on packages to existing applications.
    - **Name Search®**: This software enables applications to find, identify and match information. Specifically, Name Search finds and matches records based on personal and corporate names, social security numbers, street addresses and phone numbers even when those records have variations due to phonetics, missing words, noise words, nicknames, prefixes, keyboard errors or sequence variations. Name Search claims that searches using their rule-based matching algorithms are faster and more accurate than those based only on Soundex or similar techniques. Soundex, developed by Odell and Russell, uses codes based on the sound of each letter to translate a string into a canonical form of at most four characters, preserving the first letter

[Hall, 1980]. Name Search also supports foreign languages, technical data, medical information, and other specialized information. Other problem-specific packages take advantage of the Name Search functionality through an Application Programming Interface (API) (i.e., Name Search is bundled). An example is ISTwatch. See http://www.search-software.com/.

- **ISTwatch©**: ISTwatch is a software component suite that was designed specifically to search and match individuals against the Office of Foreign Assets Control's (OFAC's) Specially Designated Nationals list and other denied parties lists. These include the FBI's Most Wanted, Canadian's OSFI terrorist lists, the Bank of England's consolidated lists and Financial Action Task Force data on money-laundering countries. See http://www.intelligentsearch.com/ofac_software/index.html

All these tools are packages designed to be included in an application. A final set of subject-based query tools focus on customized search environments. These are tools that have been customized to perform a particular task or operate within a particular context. One example is WebFountain.

- **WebFountain**: IBM's WebFountain began as a research project focused on extending subject-based query techniques beyond free format text to target money-laundering activities identified through web sources. The WebFountain project, a product of IBM's Almaden research facility in California, used advanced natural language processing technologies to analyze the entire internet – the search covered 256 terabytes of data in the process of matching a structured list of people who were indicted for money laundering activities in the past with unstructured information on the internet. If a suspicious transaction is identified and the internet analysis finds a relationship between the person attempting the transaction and someone on the list, then an alert is issued. WebFountain has now been turned into a commercially available IBM product. Robert Carlson, IBM WebFountain vice president, describes the current content set as over 1 petabyte in storage with over three billion pages indexed, two billion stored, and the ability to mine 20 million pages a day. The commercial system also works across multiple languages. Carlson stated in 2003 that it would cover 21 languages by the end of 2004 [Quint, 2003]. See http://www.almaden.ibm.com/webfountain/.
- **Memex**: Memex is a suite of tools that was created specifically for law enforcement and national security groups. The focus of these tools is to provide integrated search capabilities against both structured (i.e., databases) and unstructured (i.e., documents) data sources. Memex also provides a graphical representation of the process the investigator is following, structuring the subject-based queries. Memex's marketing literature states that over 30 percent of the intel-

ligence user population of the UK uses Memex. Customers include the Metropolitan Police Service (MPS), whose Memex network that includes over 90 dedicated intelligence servers providing access to over 30,000 officers; the U.S. Department of Defense; numerous U.S. intelligence agencies, drug intelligence Groups and law enforcement agencies. See http://www.memex.com/index.shtml.

A.2.1.2. Pattern queries

Pattern-based queries focus on supporting automated knowledge discovery (1) where the exact subject of interest is not known in advance and (2) where what is of interest is a pattern of activity emerging over time. In order for pattern queries to be formed, the investigator must hypothesize about the patterns in advance and then use tools to confirm or deny these hypotheses. This approach is useful when there is expertise available to make reasonable guesses with respect to the potential patterns. Conversely, when that expertise is not available or the potential patterns are unknown due to extenuating circumstances (e.g., new patterns are emerging too quickly for investigators to formulate hypotheses), then investigators can automate the construction of candidate patterns by formulating a set of rules that describe how potentially interesting, emerging patterns might appear. In either case, tools can help support the production and execution of the pattern queries. The degree of automation is dependent upon the expertise available and the dynamics of the situation being investigated.

As indicated earlier, pattern-based query tools fall into two general categories: those that support investigators in the construction of patterns based on their expertise, then run those patterns against large data sets, and those that allow the investigator to build rules about patterns of interest and, again, run those rules against large data sets.

Examples of tools for each of these categories include

1. **Megaputer (PolyAnalyst 4.6)**: This tool falls into the first category of pattern-based query tools, helping the investigator hypothesize patterns and explore the data based on those hypotheses. PolyAnalyst is a tool that supports a particular type of pattern-based query called Online Analytical Processing (OLAP), a popular analytical approach for large amounts of quantitative data. Using PolyAnalyst, the investigator defines dimensions of interest to be considered in text exploration and then displays the results of the analysis across various combinations of these dimensions. For example, an investigator could search for mujahideen who had trained at the same Al Qaeda camp in the 1990s and who had links to Pakistani Intelligence as well as opium growers and smuggling networks into Europe. See http://www.megaputer.com/.

2. Autonomy Suite: Autonomy's search capabilities fall into the second category of pattern-based query tools. Autonomy has combined technologies that employ adaptive pattern-matching techniques with

Bayesian inference and Claude Shannon's principles of information theory. Autonomy identifies the patterns that naturally occur in text, based on the usage and frequency of words or terms that correspond to specific ideas or concepts as defined by the investigator. Based on the preponderance of one pattern over another in a piece of unstructured information, Autonomy calculates the probability that a document in question is about a subject of interest [Autonomy, 2002]. See http://www.autonomy.com/content/home/

3. **Fraud Investigator Enterprise**: the Fraud Investigator Enterprise Similarity Search Engine (SSE) from InfoGlide Software is another example of the second category of pattern search tools. SSE uses analytic techniques that dissect data values looking for and quantifying partial matches in addition to exact matches. SSE scores and orders search results based upon a user-defined data model. See http://www.infoglide.com/composite/ProductsF_2_1.htm

Although an evaluation of data sources available for scanning is beyond the scope of this paper, one will serve as an example of the information available. It is hypothesized in this report that tools could be developed to support the search and analysis of Short Message Service (SMS) traffic for confirmation of PIE indicators. Often referred to as 'text messaging' in the U.S., the SMS is an integrated message service that lets GSM cellular subscribers send and receive data using their handset. A single short message can be up to 160 characters of text in length - words, numbers, or punctuation symbols. SMS is a store and forward service; this means that messages are not sent directly to the recipient but via a network SMS Center. This enables messages to be delivered to the recipient if their phone is not switched on or if they are out of a coverage area at the time the message was sent. This process, called asynchronous messaging, operates in much the same way as email. Confirmation of message delivery is another feature and means the sender can receive a return message notifying them whether the short message has been delivered or not. SMS messages can be sent to and received from any GSM phone, providing the recipient's network supports text messaging. Text messaging is available to all mobile users and provides both consumers and business people with a discreet way of sending and receiving information

Over 15 billion SMS text messages were sent around the globe in January 2001. Tools taking advantage of the stored messages in an SMS Center could:

- Perform searches of the text messages for keywords or phrases,
- Analyze SMS traffic patterns, and
- Search for people of interest in the Home Location Register (HLR) database that maintains information about the subscription profile of the mobile phone and also about the routing information for the subscriber.

A.2.2. Codification tools

As can be seen from exhibit 6, all codification tools will need to support requirements dictated by where these tools fall within the tool space. Codification tools should focus on:

- Supporting individual investigators (or at best a small group of investigators) in making sense of the information discovered during the scanning process.
- Moving the terms with which the information is referenced from a localized organizational context (uncoded, e.g., hawala banking) to a more global context (codified, e.g., informal value storage and transfer operations).
- Moving that information from specific, concrete examples towards more abstract terms that could support identification of concepts and patterns across multiple situations, thus providing a larger context for the concepts being explored.

Using these criteria as a background, the codification tools reviewed fall into two major categories:

1. Tools that help investigators label concepts and cluster different concepts into terms that are recognizable and used by the larger analytical community; and
2. Tools that use this information to build up network maps identifying entities, relationships, missions, etc.

This section briefly describes codification functionality in general, as well as providing specific tool examples, to support both of these types of codification.

A.2.2.1. Labeling and clustering

The first step to codification is to map the context-specific terms used by individual investigators to a taxonomy of terms that are commonly accepted in a wider analytical context. This process is performed through labeling individual terms, clustering other terms and renaming them according to a community-accepted taxonomy.

In general, labeling and clustering tools should:

- Support the capture of taxonomies that are being developed by the broader analytical community;
- Allow the easy mapping of local terms to these broader terms;
- Support the clustering process either by providing algorithms for calculating the similarity between concepts, or tools that enable collaborative consensus construction of clustered concepts.

Label and cluster functionality is typically embedded in applications support analytical processes, not provided separately as stand-alone tools. Two examples of such products include:

COPLINK® – COPLINK began as a research project at the University of Arizona and has now grown into a commercially available application from Knowledge Computing Corporation (KCC). It is focused on providing tools for organizing vast quantities of structured and seemingly unrelated information in the law enforcement arena. See COPLINK's commercial website at http://www.knowledgecc.com/index.htm and its academic website at the University of Arizona at http://ai.bpa.arizona.edu/COPLINK/.

Megaputer (PolyAnalyst 4.6) – In addition to supporting pattern queries, PolyAnalyst also provides a means for creating, importing and managing taxonomies which could be useful in the codification step and carries out automated categorization of text records against existing taxonomies.

A.2.2.2. Network mapping

Terrorists have a vested interest in concealing their relationships, they often emit confusing or intentionally misleading information and they operate in self-contained and difficult to penetrate cells for much of the time. Criminal networks are also notoriously difficult to map, and the mapping often happens after a crime has been committed than before. What is needed are tools and approaches that support the mapping of networks to represent agents (e.g., people, groups), environments, behaviors, and the relationships between all of these.

A large number of research efforts and some commercial products have been created to automate aspects of network mapping in general and link analysis specifically. In the past, however, these tools have provided only marginal utility in understanding either criminal or terrorist behavior (as opposed to espionage networks, for which this type of tool was initially developed). Often the linkages constructed by such tools are impossible to disentangle since all links have the same importance. PIE holds the potential to focus link analysis tools by clearly delineating watch points and allowing investigators to differentiate, characterize and prioritize links within an asymmetric threat network. This section focuses on the requirements dictated by PIE and some candidate tools that might be used in the PIE context.

In general, network mapping tools should:

- Support the representation of people, groups, and the links between them within the PIE indicator framework;
- Sustain flexibility for mapping different network structures;
- Differentiate, characterize and prioritize links within an asymmetric threat network;

- Focus on organizational structures to determine what kinds of network structures they use;
- Provide a graphical interface that supports analysis;
- Access and associate evidence with an investigator's data sources.

Within the PIE context, investigators can use network mapping tools to identify the flows of information and authority within different types of network forms such as chains, hub and spoke, fully matrixed, and various hybrids of these three basic forms.

Examples of network mapping tools that are available commercially include:

Analyst Notebook®: A PC-based package from i2 that supports network mapping/link analysis via network, timeline and transaction analysis. Analyst Notebook allows an investigator to capture link information between people, groups, activities, and other entities of interest in a visual format convenient for identifying relationships, dependencies and trends. Analyst Notebook facilitates this capture by providing a variety of tools to review and integrate information from a number of data sources. It also allows the investigator to make a connection between the graphical icons representing entities and the original data sources, supporting a drill-down feature. Some of the other useful features included with Analyst Notebook are the ability to: 1) automatically order and depict sequences of events even when exact date and time data is unknown and 2) use background visuals such as maps, floor plans or watermarks to place chart information in context or label for security purposes. See http://www.i2.co.uk/Products/Analysts_Notebook/default.asp. Even though i2 Analyst Notebook is widely used by intelligence community, anti-terrorism and law enforcement investigators for constructing network maps, interviews with investigators indicate that it is more useful as a visual aid for briefing rather than in performing the analysis itself. Although some investigators indicated that they use it as an analytical tool, most seem to perform the analysis using either another tool or by hand, then entering the results into the Analyst Notebook in order to generate a graphic for a report or briefing. Finally, few tools are available within the Analyst Notebook to automatically differentiate, characterize and prioritize links within an asymmetric threat network.

Patterntracer TCA: Patterntracer Telephone Call Analysis (TCA) is an add-on tool for the Analyst Notebook intended to help identify patterns in telephone billing data. Patterntracer TCA automatically finds repeating call patterns in telephone billing data and graphically displays them using network and timeline charts. See http://www.i2.co.uk/Products/Analysts_Workstation/default.asp

Memex: Memex has already been discussed in the context of subject-based query tools. In addition to supporting such queries, however, Memex also provides a tool that supports automated link analysis on unstructured data and presents the results in graphical form.

Megaputer (PolyAnalyst 4.6): In addition to supporting pattern-based queries, PolyAnalyst was also designed to support a primitive form of link analysis, by providing a visual relationship of the results.

A.2.3. Abstraction tools

As can be seen from exhibit 6, all abstraction tools will need to support requirements dictated by where these tools fall within the tool space. Abstraction tools should focus on:

- Functionalities that help individual investigators (or a small group of investigators) build abstract models;
- Options to help share these models, and therefore the tools should be defined using terms that will be recognized by the larger community (i.e., codified as opposed to uncoded);
- Highly abstract notions that encourage examination of concepts across networks, groups, and time.

The product of these tools should be hypotheses or models that can be shared with the community to support information exchange, encourage dialogue, and eventually be validated against both real-world data and by other experts. This section provides some examples of useful functionality that should be included in tools to support the abstraction process.

A.2.3.1. Structured argumentation tools

Structured argumentation is a methodology for capturing analytical reasoning processes designed to address a specific analytic task in a series of alternative constructs, or hypotheses, represented by a set of hierarchical indicators and associated evidence. Structured argumentation tools should:

- Capture multiple, competing hypotheses of multi-dimensional indicators at both summary and/or detailed levels of granularity;
- Develop and archive indicators and supporting evidence;
- Monitor ongoing activities and assess the implications of new evidence;
- Provide graphical visualizations of arguments and associated evidence;
- Encourage a careful analysis by reminding the investigator of the full spectrum of indicators to be considered;
- Ease argument comprehension by allowing the investigator to move along the component lines of reasoning to discover the basis and rationale of others' arguments;
- Invite and facilitate argument comparison by framing arguments within common structures; and
- Support collaborative development and reuse of models among a community of investigators.

Within the PIE context, investigators can use structured argumentation tools to assess a terrorist group's ability to weaponize biological materials, and determine the parameters of a transnational criminal organization's money laundering methodology.

Examples of structured argumentation tools that are available commercially include:

Structured Evidential Argument System (SEAS) from SRI International was initially applied to the problem of early warning for project management, and more recently to the problem of early crisis warning for the U.S. intelligence and policy communities. SEAS is based on the concept of a structured argument, which is a hierarchically organized set of questions (i.e., a tree structure). These are multiple-choice questions, with the different answers corresponding to discrete points or subintervals along a continuous scale, with one end of the scale representing strong support for a particular type of opportunity or threat and the other end representing strong refutation. Leaf nodes represent primitive questions, and internal nodes represent derivative questions. The links represent support relationships among the questions. A derivative question is supported by all the derivative and primitive questions below it. SEAS arguments move concepts from their concrete, local representations into a global context that supports PIE indicator construction. See http://www.ai.sri.com/~seas/.

A.2.3.2. Modeling

By capturing information about a situation (e.g., the actors, possible actions, influences on those actions, etc.), in a model, users can define a set of initial conditions, match these against the model, and use the results to support analysis and prediction. This process can either be performed manually or, if the model is complex, using an automated tool or simulator.

Utilizing modeling tools, investigators can systematically examine aspects of terror-crime interaction. Process models in particular can reveal linkages between the two groups and allow investigators to map these linkages to locations on the terror-crime interaction spectrum. Process models capture the dynamics of networks in a series of functional and temporal steps. Depending on the process being modeled, these steps must be conducted either sequentially or simultaneously in order for the process to execute as designed. For example, delivery of cocaine from South America to the U.S. can be modeled as process that moves sequentially from the growth and harvesting of coca leaves through refinement into cocaine and then transshipment via intermediate countries into U.S. distribution points. Some of these steps are sequential (e.g., certain chemicals must be acquired and laboratories established before the coca leaves can be processed in bulk) and some can be conducted simultaneously (e.g., multiple smuggling routes can be utilized at the same time).

Corruption, modeled as a process, should reveal useful indicators of cooperation between organized crime and terrorism. For example, one way to generate and validate indicators of terror-crime interaction is to place cases of corrupt government officials or private sector individuals in an organizational network construct utilizing a process model and determine if they serve as a common link between terrorist and criminal networks via an intent model with attached evidence. An intent model is a type of process model constructed by reverse engineering a specific end-state, such as the ability to move goods and people into and out of a country without interference from law enforcement agencies.

This end-state is reached by bribing certain key officials in groups that supply border guards, provide legitimate import-export documents (e.g., end-user certificates), monitor immigration flows, etc.

Depending on organizational details, a bribery campaign can proceed sequentially or simultaneously through various offices and individuals. This type of model allows analysts to 'follow the money' through a corruption network and link payments to officials with illicit sources. The model can be set up to reveal payments to officials that can be linked to both criminal and terrorist involvement (perhaps via individuals or small groups with known links to both types of network).

Thus investigators can use a process model as a repository for numerous disparate data items that, taken together, reveal common patterns of corruption or sources of payments that can serve as indicators of cooperation between organized crime and terrorism. Using these tools, investigators can explore multiple data dimensions by dynamically manipulating several elements of analysis:

- Criminal and/or terrorist priorities, intent and factor attributes;
- Characterization and importance of direct evidence;
- Graphical representations and other multi-dimensional data visualization approaches.

There have been a large number of models built over the last several years focusing on counter-terrorism and criminal activities. Some of the most promising are models that support agent-based execution of complex adaptive environments that are used for intelligence analysis and training. Some of the most sophisticated are now being developed to support the generation of more realistic environments and interactions for the commercial gaming market.

In general, modeling tools should:

- Capture and present reasoning from evidence to conclusion;
- Enable comparison of information across situation, time, and groups;
- Provide a framework for challenging assumptions and exploring alternative hypotheses;

- Facilitate information sharing and cooperation by representing hypotheses and analytical judgment, not just facts;
- Incorporate the first principle of analysis—problem decomposition;
- Track ongoing and evolving situations, collect analysis, and enable users to discover information and critical data relationships;
- Make rigorous option space analysis possible in a distributed electronic context;
- Warn users of potential cognitive bias inherent in analysis.

Although there are too many of these tools to list in this report, good examples of some that would be useful to support PIE include:

NETEST: This model estimates the size and shape of covert networks given multiple sources with omissions and errors. NETEST makes use of Bayesian updating techniques, communications theory and social network theory [Dombroski, 2002].

The Modeling, Virtual Environments and Simulation (MOVES) Institute at the Naval Postgraduate School in Monterey, California, is using a model of cognition formulated by Aaron T. Beck to build models capturing the characteristics of people willing to employ violence [Beck, 2002].

BIOWAR: This is a cityscale multi-agent model of weaponized bioterrorist attacks for intelligence and training. At present the model is running with 100,000 agents (this number will be increased). All agents have real social networks and the model contains real city data (hospitals, schools, etc.). Agents are as realistic as possible and contain a cognitive model [Carley, 2003a].

All of the models reviewed had similar capabilities:

- Capture the characteristics of entities - people, places, groups, etc.;
- Capture the relationships between entities at a level of detail that supports programmatic construction of processes, situations, actions, etc. these are usually "isa" and "apartof" representations of object-oriented taxonomies, influence relationships, time relationships, etc.;
- The ability to represent this information in a format that supports using the model in simulations. The next section provides information on simulation tools that are in common use for running these types of models.
- User interfaces for defining the models, the best being graphical interfaces that allow the user to define the entities and their relationships through intuitive visual displays. For example, if

the model involves defining networks or influences between entities, graphical displays with the ability to create connections and perform drag and drop actions become important.

A.2.4. Diffusion tools

As can be seen from exhibit 6, all diffusion tools will need to support requirements dictated by where these tools fall within the tool space. Diffusion tools should focus on:

- Moving information from an individual or small group of investigators to the collective community;
- Providing abstract concepts that are easily understood in a global context with little worry that the terms will be misinterpreted;
- Supporting the representation of abstract concepts and encouraging dialogues about those concepts.

In general diffusion tools should:

- Provide a shared environment that investigators can access on the internet;
- Support the ability for everyone to upload abstract concepts and their supporting evidence (e.g., documents);
- Contain the ability for the person uploading the information to be able to attach an annotation and keywords;
- Posses the ability to search concept repositories;
- Be simple to set up and use.

Within the PIE context, investigators could use diffusion tools to:

- Employ a collaborative environment to exchange information, results of analysis, hypotheses, models, etc.;
- Utilize collaborative environments that might be set up between law enforcement groups and counterterrorism groups to exchange information on a continual and near real-time basis.

Examples of diffusion tools run from one end of the cooperation/dissemination spectrum to the other. One of the simplest to use is:

- **AskSam: T**he AskSam Web Publisher is an extension of the standalone AskSam capability that has been used by the analytical community for many years. The capabilities of AskSam Web Publisher include: 1) sharing documents with others who have access to the local network, 2) anyone who has access to the network has access to the AskSam archive without the need for an expensive license, and 3) advanced searching capabilities including adding key-

words which supports a group's codification process (see step 2 in exhibit 6 in our analytical process). See http://www.asksam.com/.

There are some significant disadvantages to using AskSam as a cooperation environment. For example, each document included has to be 'published'. The assumption is that there are only one or two people primarily responsible for posting documents and these people control all documents that are made available, a poor assumption for an analytical community where all are potential publishers of concepts. The result is expensive licenses for publishers. Finally, there is no web-based service for AskSam, requiring each organization to host its own AskSam server.

There are two leading commercial tools for cooperation now available and widely used. Which tool is chosen for a task depends on the scope of the task and the number of users.

- **Groove:** virtual office software that allows small teams of people to work together securely over a network on a constrained problem. Groove capabilities include: 1) the ability for investigators to set up a shared space, invite people to join and give them permission to post documents to a document repository (i.e., file sharing), 2) security including encryption that protects content (e.g., upload and download of documents) and communications (e.g., email and text messaging), investigators can work across firewalls without a Virtual Private Network (VPN) which improves speed and makes it accessible from outside of an intranet, 4) investigators are able to work off-line, then synchronize when they come back on line, 5) includes add-in tools to support cooperation such as calendars, email, text- and voice-based instant messaging, and project management.

  Although Groove satisfies most of the basic requirements listed for this category, there are several drawbacks to using Groove for large projects. For example, there is no free format search for text documents and investigators cannot add on their own keyword categories or attributes to the stored documents. This limits Groove's usefulness as an information exchange archive. In addition, Groove is a fat client, peer-to-peer architecture. This means that all participants are required to purchase a license, download and install Groove on their individual machines. It also means that Groove requires high bandwidth for the information exchange portion of the peer-to-peer updates. See http://www.groove.net/default.cfm?pagename=Workspace.

- **Sharepoint**: Allows teams of people to work together on documents, tasks, contacts, events, and other information. Sharepoint capabilities include: 1) text document loading and sharing, 2) free format search capability, 3) cooperation tools to include instant messaging, email and a group calendar, and 4) security with individual and group level access control. The TraCCC

team employed Sharepoint for this project to facilitate distributed research and document generation. See http://www.microsoft.com/sharepoint/.

Sharepoint has many of the same features as Groove, but there are fundamental underlying differences. Sharepoint's architecture is server based with the client running in a web browser. One advantage to this approach is that each investigator is not required to download a personal version on a machine (Groove requires 60-80MB of space on each machine). In fact, an investigator can access the Sharepoint space from any machine (e.g., at an airport). The disadvantage of this approach is that the investigator does not have a local version of the Sharepoint information and is unable to work offline. With Groove, an investigator can work offline, and then resynchronize with the remaining members of the group when the network once again becomes available. Finally, since peer-to-peer updates are not taking place, Sharepoint does not necessarily require a high speed internet access, except perhaps in the case where the investigator would like to upload large documents.

Another significant difference between Sharepoint and Groove is linked to the search function. In Groove, the search capability is limited to information that is typed into Groove directly, not to documents that have been attached to Groove in an archive. A Sharepoint support not only document searches, but also allows the community of investigators to set up their own keyword categories to help with the codification of the shared documents (again see step 2 from exhibit 6). It should be noted, however, that Sharepoint only supports searches for Microsoft documents (e.g., Word, PowerPoint, etc.) and not 'foreign' document formats such as PDF. This fact is not surprising given that Sharepoint is a Microsoft tool.

Sharepoint and Groove are commercially available cooperation solutions. There are also a wide variety of customized cooperation environments now appearing on the market. For example:

- **WAVE Enterprise Information Integration System** - Modus Operandi's Wide Area Virtual Environment (WAVE) provides tools to support real-time enterprise information integration, cooperation and performance management. WAVE capabilities include: 1) collaborative workspaces for team-based information sharing, 2) security for controlled sharing of information, 3) an extensible enterprise knowledge model that organizes and manages all enterprise knowledge assets, 4) dynamic integration of legacy data sources and commercial off-the-shelf (COtS) tools, 5) document version control, 6) cooperation tools, including discussions, issues, action items, search, and reports, and 7) performance metrics. WAVE is not a COtS solution, however. An organization must work with Modus Operandi services to set up a custom envi-

ronment. The main disadvantage to this approach as opposed to Groove or Sharepoint is cost and the sharing of information across groups. See http://www.modusoperandi.com/wave.htm.

Finally, many of the tools previously discussed have add-ons available for extending their functionality to a group. For example:

- **iBase4**: i2's Analyst Notebook can be integrated with iBase4, an application that allows investigators to create multi-user databases for developing, updating, and sharing the source information being used to create network maps. It even includes security to restrict access or functionality by user, user groups and data fields. It is not clear from the literature, but it appears that this functionality is restricted to the source data and not the sharing of network maps generated by the investigators. See http://www.i2.co.uk/Products/iBase/default.asp

  The main disadvantage of iBase4 is its proprietary format. This limitation might be somewhat mitigated by coupling iBase4 with i2's iBridge product which creates a live connection between legacy databases, but there is no evidence in the literature that i2 has made this integration.

A.2.5. Validation tools

As can be seen from exhibit 6, all validation tools will need to support requirements dictated by where these tools fall within the tool space. Validation tools should focus on:

- Providing a community context for validating the concepts put forward by the individual participants in the community;
- Continuing to work within a codified realm in order to facilitate communication between different groups articulating different perspectives;
- Matching abstract concepts against real world data (or expert opinion) to determine the validity of the concepts being put forward.

Using these criteria as background, one of the most useful toolsets available for validation are simulation tools. This section briefly describes the functionality in general, as well as providing specific tool examples, to support simulations that 'kick the tires' of the abstract concepts.

Following are some key capabilities that any simulation tool must possess:

- Ability to ingest the model information that has been constructed in the previous steps in the analytical process;
- Access to a data source for information that might be required by the model during execution;

- Users need to be able to define the initial conditions against which the model will be run;
- The more useful simulators allow the user to "step through" the model execution, examining variables and resetting variable values in mid-execution;
- Ability to print out step-by-step interim execution results and final results;
- Change the initial conditions and compare the results against prior runs.

Although there are many simulation tools available, following are brief descriptions of some of the most promising:

- **Online iLink**: An optional application for i2's Analyst Notebook that supports dynamic update of Analyst Notebook information from online data sources. Once a connection is made with an on-line source (e.g., LexisNexis™, or D&B®) Analyst Notebook uses this connection to automatically check for any updated information and propagates those updates throughout to support validation of the network map information. See http://www.i2inc.com.

One apparent drawback with this plug-in is that Online iLink appears to require that the line data provider deploy i2's visualization technology.

- **NETEST:** A research project from Carnegie Mellon University, which is developing tools that combine multi-agent technology with hierarchical Bayesian inference models and biased net models to produce accurate posterior representations of terrorist networks. Bayesian inference models produce representations of a network's structure and informant accuracy by combining prior network and accuracy data with informant perceptions of a network. Biased net theory examines and captures the biases that may exist in a specific network or set of networks. Using NETEST, an investigator can estimate a network's size, determine its membership and structure, determine areas of the network where data is missing, perform cost/benefit analysis of additional information, assess group level capabilities embedded in the network, and pose "what if" scenarios to destabilize a network and predict its evolution over time [Dombroski, 2002].
- **REcursive Porous Agent Simulation toolkit (REPAST)**: A good example of the free, open source toolkits available for creating agent-based simulations. Begun by the University of Chicago's social sciences research community and later maintained by groups such as Argonne National Laboratory, Repast is now managed by the non-profit volunteer Repast Organization for Architecture and Development (ROAD). Some of Repast's features include: 1) a variety of agent templates and examples (however, the toolkit gives users complete flexibility as to how

they specify the properties and behaviors of agents), 2) a fully concurrent discrete event scheduler (this scheduler supports both sequential and parallel discrete event operations), 3) built-in simulation results logging and graphing tools, 4) an automated Monte Carlo simulation framework, 5) allows users to dynamically access and modify agent properties, agent behavioral equations, and model properties at run time, 6) includes libraries for genetic algorithms, neural networks, random number generation, and specialized mathematics, and 7) built-in systems dynamics modeling.

More to the point for this investigation, Repast has social network modeling support tools. The Repast website claims that "Repast is at the moment the most suitable simulation framework for the applied modeling of social interventions based on theories and data," [Tobias, 2003]. See http://repast.sourceforge.net/.

A.2.6. Impacting tools

As can be seen from exhibit 6, all impacting tools will need to support requirements dictated by where these tools fall within the tool space. Impacting tools should focus on:

- Helping law enforcement and intelligence practitioners understand the implications of their validated models. For example, what portions of the terror-crime interaction spectrum are relevant in various parts of the world, and what is the likely evolutionary path of this phenomenon in each specific geographic area?

Support for translating abstracted knowledge into more concrete local execution strategies. The information flows feeding the scanning process, for example, should be updated based on the results of mapping local events and individuals to the terror-crime interaction spectrum. Watch points and their associated indicators should be reviewed, updated and modified. Probes can be constructed to clarify remaining uncertainties in specific situations or locations.

The following general requirements have been identified for impacting tools:

- Probe management software to help law enforcement investigators and intelligence community analysts plan probes against known and suspected transnational threat entities, monitor their execution, map their impact, and analyze the resultant changes to network structure and operations.

- Situational assessment software that supports transnational threat monitoring and projection. Data fusion and visualization algorithms that portray investigators' current understanding of the nature

and extent of terror-crime interaction, and allow investigators to focus scarce collection and analytical resources on the most threatening regions and networks.

Impacting tools are only just beginning to exit the laboratory, and none of them can be considered ready for operational deployment. This type of functionality, however, is being actively pursued within the U.S. governmental and academic research communities. An example of an impacting tool currently under development is described below:

DyNet – A multi-agent network system designed specifically for assessing destabilization strategies on dynamic networks. A knowledge network (e.g., a hypothesized network resulting from Steps 1 through 5 of Boisot's I-Space-driven analytical process) is given to DyNet as input. In this case, a knowledge network is defined as an individual's knowledge about who they know, what resources they have, and what task(s) they are performing. The goal of an investigator using DyNet is to build stable, high performance, adaptive networks with and conduct what-if analysis to identify successful strategies for destabilizing those networks. Investigators can run sensitivity tests examining how differences in the structure of the covert network would impact the overall ability of the network to respond to probe and attacks on constituent nodes. [Carley, 2003b]. See the DyNet website hosted by Carnegie Mellon University at http://www.casos.cs.cmu.edu/projects/DyNet/.

A.3. Overall tool requirements

This appendix provides a high level overview of PIE tool requirements:

- Easy to put information into the system and get information out of it. The key to the successful use of many of these tools is the quality of the information that is put into them. User interfaces have to be easy to use, context based, intuitive, and customizable. Otherwise, investigators soon determine that the "care and feeding" of the tool does not justify the end product.
- Reasonable response time: The response time of the tool needs to match the context. If the tool is being used in an operational setting, then the ability to retrieve results can be time-critical--perhaps a matter of minutes. In other cases, results may not be time-critical and days can be taken to generate results.
- Training: Some tools, especially those that have not been released as commercial products, may not have substantial training materials and classes available. When making a decision regarding tool selection, the availability and accessibility of training may be critical.
- Ability to integrate with the enterprise resources: There are many cases where the utility of the tool will depend on its ability to access and integrate information from the overall enterprise in

which the investigator is working. Special-purpose tools that require re-keying of information or labor-intensive conversions of formats should be carefully evaluated to determine the man-power required to support such functions.

- Support for integration with other tools: Tools that have standard interfaces will act as force multipliers in the overall analytical toolbox. At a minimum, tools should have some sort of a developer's kit that allows the creation of an API. In the best case, a tool would support some generally accepted integration standard such as web services.
- Security: Different situations will dictate different security requirements, but in almost all cases some form of security is required. Examples of security include different access levels for different user populations. The ability to be able to track and audit transactions, linking them back to their sources, will also be necessary in many cases.
- Customizable: Augmenting usability, most tools will need to support some level of customizability (e.g., customizable reporting templates).
- Labeling of information: Information that is being gathered and stored will need to be labeled (e.g., for level of sensitivity or credibility).
- Familiar to the current user base: One characteristic in favor of any tool selected is how well the current user base has accepted it. There could be a great deal of benefit to upgrading existing tools that are already familiar to the users.
- Heavy emphasis on visualization: To the greatest extent possible, tools should provide the investigator with the ability to display different aspects of the results in a visual manner.
- Support for cooperation: In many cases, the strength of the analysis is dependent on leveraging cross-disciplinary expertise. Most tools will need to support some sort of cooperation.

A.4. Bibliography and Further Reading

Autonomy technology White Paper, Ref: [WP tECH] 07.02. This and other information documents about Autonomy may be downloaded after registration from http://www.autonomy.com/content/downloads/

Beck, Aaron T., "Prisoners of Hate," Behavior research and therapy, 40, 2002: 209-216. A copy of this article may be found at http://mail.med.upenn.edu/~abeck/prisoners.pdf. Also see Dr. Beck's website at http://mail.med.upenn.edu/~abeck/ and the MOVES Institute at http://www.movesinstitute.org/.

Boisot, Max and Ron Sanchez, "the Codification-Diffusion-Abstraction Curve in the I-Space," Economic Organization and Nexus of Rules: Emergence and the Theory of the Firm, a working paper, the Universitat Oberta de Catalunya, Barcelona, Spain, May 2003. This draft paper may be found at http://www.google.com/url?sa=U&start=1&q=http://web.cbs.dk/departments/ivs/events/boisotsanchez.doc&e=9901

Carley, K. M., D. Fridsma, E. Casman, N. Altman, J. Chang, B. Kaminsky, D. Nave, & Yahja, "BioWar: Scalable Multi-Agent Social and Epidemiological Simulation of Bioterrorism Events" in Proceedings from the NAACSOS Conference, 2003. this document may be found at http://www.casos.ece.cmu.edu/casos_working_paper/carley_2003_biowar.pdf

Carley, Kathleen M., et. al., "Destabilizing Dynamic Covert Networks" in Proceedings of the 8th International Command and Control Research and technology Symposium, 2003. Conference held at the National Defense War College, Washington, DC. This document may be found at http://www.casos.ece.cmu.edu/resources_others/a2c2_carley_2003_destabilizing.pdf

Collier, N., Howe, T., and North, M., "Onward and Upward: the transition to Repast 2.0," in Proceedings of the First Annual North American Association for Computational Social and Organizational Science Conference, Electronic Proceedings, Pittsburgh, PA, June 2003. Also, read about REPASt 3.0 at the REPASt website: http://repast.sourceforge.net/index.html

DeRosa, Mary, "Data Mining and Data Analysis for Counterterrorism," CSIS Report, March 2004. this document may be purchased at http://csis.zoovy.com/product/0892064439

Dombroski, M. and K. Carley, "NETEST: Estimating a Terrorist Network's Structure," Journal of Computational and Mathematical Organization theory, 8(3), October 2002: 235-241. http://www.casos.ece.cmu.edu/conference2003/student_paper/Dombroski.pdf

Farah, Douglas, Blood From Stones: the Secret Financial Network of Terror, New York: Broadway Books, 2004.

Hall, P. and G. Dowling, "Approximate string matching," Computing Surveys, 12(4), 1980: 381-402. For more information on phonetic string matching see http://www.cs.rmit.edu.au/~jz/fulltext/sigir96.pdf. A good summary of the inherent limitations of Soundex may be found at http://www.las-inc.com/soundex/?source=gsx.

Lowrance, J.D., Harrison, I.W., and Rodriguez, A.C., "Structured Argumentation for Analysis," Proceedings of the 12th International Conference on Systems Research, Informatics, and Cybernetics, (August 2000).

Quint, Barbara, "IBM's WebFountain Launched – the Next Big Thing?" September 22, 2003 - from the Information today, Inc. website at http://www.infotoday.com/newsbreaks/nb030922-1.shtml Also see IBM's WebFountain website at http://www.almaden.ibm.com/webfountain/ and the WebFountain Application Development Guide at http://www.almaden.ibm.com/webfountain/resources/sg247029.pdf.

Shannon, Claude, "A mathematical theory of communication," Bell System technical Journal, (27), July and October 1948: 379-423 and 623-656.

Tobias, R. and C. Hofmann, "Evaluation of Free Java-libraries for Social-scientific Agent Based Simulation," Journal of Artificial Societies and Social Simulation, University of Surrey, 7(1), January 2003 may be found at http://jasss.soc.surrey.ac.uk/7/1/6.html.

A.5. Glossary of terms

Algorithm – a step-by-step procedure for solving a problem or accomplishing some end especially by a computer.

Application Programming Interface (API) - a set of routines, protocols, and tools for building software applications. A good API makes it easier to develop a program by providing all the building blocks. A programmer puts the blocks together.

Bandwidth – defines how much information one can send through a connection, usually measured in bits-per-second. For example, a full page of English text is about 16,000 bits. A fast modem can move about 57,000 bits in one second. Full-motion full-screen video would require high bandwidth to play, roughly 10,000,000 bits-per-second.

Bayesian Inference - named for Thomas Bayes, an English clergyman and mathematician, Bayesian inferencing is a branch of logic applied to decision making and inferential statistics that deals with probability inference: using the knowledge of prior events to predict future events. Based on probability theory, the theorem defines a rule for refining a hypothesis by factoring in

additional evidence and background information, and leads to a number representing the degree of probability that the hypothesis is true.

Citation Indexing – searches can result in thousands of documents being found that contain the search terms. One approach to prioritizing these results is to place the ones that are referenced the most often by others at the top of the list. The assumption is that if others have referenced this web page or document, then they have found it useful and the current searcher will as well. This indexing by counting the number of citations for the page or document is termed citation indexing. Google is one of the most obvious examples of a search engine that uses citation indexing.

Canonical Form – reduces a term (e.g., a person's name, the name of an organization, etc.) to the simplest and most significant form possible without loss of generality.

Fat Client – the software that runs the business logic, the user interface, etc. can either reside remotely on the server or locally on the machine that is connecting to the server (i.e., the client). If it resides on the client, that client is called fat. Fat in this case does not necessarily mean bad. the circumstances under which one might want a fat client is dependent on factors such as the connection speed, the complexity of the business logic, the complexity of the user interface, etc.

"isa" Representations – representations that help the searcher describe the search terms that help refine the results. For example, if a searcher has access to a taxonomy of terms that predefines that Al Qaeda "isa" terrorist organization, the extra context will improve the overall results of the search. Another useful representation is "apartof."

Monte Carlo - a problem-solving technique that uses random samples and other statistical methods for finding solutions to mathematical or physical problems.

Noise Word –words so commonly used in a language as to make them useless as discriminating words in a query. Some search tools, such as Google, will strip out the noise words before proceeding with the search.

Peer-to-peer Networks – allow the exchange of information between two computers without an intermediate of a server. Each time a member of the network joins, that member downloads any relevant updates that have taken place on the other members of the network. The advantage of this approach is that collaborators do not have to rely on a large central server. The disadvantage is scalability. Peer-to-peer networks can quickly become complex and the update times unacceptable.

Petabyte – a unit of measurement in computers of 1,024 terabytes. This, for example, represents billions of pages of text.

Terabyte - a unit of measurement in computers of 1,024 gigabytes (or 1,099,511,627,776 bytes). A terabyte usually refers to extremely large hard-disk capacities.

Web Crawlers - also known as a spider, ant, robot (i.e. "bot") and intelligent agent, a crawler is a program that searches for information on the Web. It is used to locate HTML pages by content or by following hypertext links from page to page. Search engines use crawlers to find new Web pages that are summarized and added to their indexes.

Endnotes

[1] Mapping the Global Structure, Report of the National Intelligence Council's 2020 Project, National Intelligence Council, Washington, December 2004, p. 96.
[2] Shelley, Louise, and John Picarelli, "Methods Not Motives: Implications of the Convergence of International Organized Crime and Terrorism," *Police Practice and Research* 3 (2002): 305-318.
[3] Manwaring, Max, *Street Gangs: The New Urban Insurgency*, Carlisle: Army War College, 2005. See http://www.carlisle.army.mil/ssi/pdffiles/PUB597.pdf.
[4] Seper, Jerry, "Al Qaeda Seeks Tie to Local Gang," *The Washington Times*, 28 September 2004.
[5] Cuthbertson, Ian, "Prisons and the Education of Terrorists," *World Policy Journal* 21 (Fall 2004): 15-22.
[6] For a more detailed treatment of this topic, see Body-Gendrot, Sophie and Martiniello, Marco (eds.), *Minorities in European Cities: The Dynamics of Social Integration and Social Exclusion at the Neighborhood Level*, New York: St. Martin's Press, 2000. In particular, see the chapters of Thomas Faist, "Economic Activities of Migrants in Transnational Social Spaces," and Simon Holdaway, "Migration, Crime and the City: Context of Social Exclusion."
[7] Cressey, Donald. "Methodological Problems in the Study of Organized Crime as a Social Problem," *The Annals of the American Academy of Political and Social Science* 374 (1967): 101-12.
[8] For a comprehensive and updated listing of definitions of organized crime, see Klaus van Lampe's website at http://www.organized-crime.de/OCDEF1.htm.
[9] For an excellent summation of the arguments, see Abadinsky, Howard (2003), *Organized Crime, 7th ed.*, Belmont: Wadsworth/Thompson Learning, 2003 and Williams, Phil, "The Nature of Drug Trafficking Networks," *Current History* (April 1998).
[10] Alon Daniel, for example, conducted a participant observation study in European prisons that observed Eastern European criminals recruited by imprisoned terrorists to provide fraudulent documents and commit other crimes. See Daniel, Alon, "Terrorist Recruitment in European Prisons," paper presented at the Istanbul Conference on Democracy and Global Security, 11 June 2005.
[11] For the full text of the convention and its protocols, see http://www.unodc.org/palermo/convmain.html.
[12] For more information on the shadow economy, see Fleming, Matthew et al, "The Shadow Economy," *Journal of International Affairs* 53 (Spring 2000): 387-409; Schneider, Friedrich and Dominik Enste, "Shadow Economies: Size, Causes and Consequences," *Journal of Economic Literature* 38 (March 2000): 77-114.
[13] Galleotti, Mark, "Underworld and Upperworld: Transnational Organized Crime and Global Society," in Josselin, Daphne and Williams Wallace, eds., *Non-State Actors in World Politics*, New York: Palgrave, 2005: 203-17.
[14] Schmid, Alex, *Political Terrorism: A Research Guide*, New Brunswick: Transaction Books, 1984; Laqueur, Walter, *Terrorism*, London: Weidenfeld & Nicolson, 1977.
[15] Hoffman, Bruce, *Inside Terrorism*, New York: Columbia University Press, 1998: 43.
[16] For the most recent listing, see http://www.state.gov/documents/organization/45323.pdf.
[17] Laqueur, *Terrorism*: 66-7, 105; Crenshaw, Martha, "'New' vs. 'Old' Terrorism," paper presented at the Kennan Institute, Washington DC, 23 May 2005.
[18] Ehrenfeld, Rachel, *Narco-Terrorism*, New York: BasicBooks, 1990.
[19] Stepanova, E.A., *Rol narkobiznesa v politekonomii konfliktov i terrorizma* (The Role of the Illicit Drug Business in the Political Economy of Conflicts and Terrorism), Moscow: Ves' Mir, 2005.
[20] Rosenau, James, *Turbulence in World Politics*, Princeton: Princeton University Press, 1990.
[21] Cusimano-Love, Maryann, ed., *Beyond Sovereignty: Issues for a Global Agenda (Second Edition)*, Belmont: Wadsworth, 2005.
[22] Castells, Manuel, *End of Millennium, Volume III (Second Edition)*, Oxford: Blackwell, 2000; Arquilla, John and David Ronfeldt, eds., *Networks and Netwars*, Santa Monica, RAND, 2001.
[23] Strange, Susan, *The Retreat of the State*, New York: Cambridge University Press, 1996.
[24] Scott, Erik "Russian Business and the Sustenance of Conflict in Georgia," Unpublished Manuscript, 7 March 2005; Kaldor, Mary, *New and Old Wars: Organized Violence in a Global Era*, Stanford: Stanford University Press, 1999.
[25] Sassen, Saskia, *Globalization and Its Discontents*, New York: The New Press, 1998; Mittelman, James, *The Globalization Syndrome: Transformation and Resistance*, Princeton: Princeton University Press, 2000; Naim, Moises, "Five Wars of Globalization." *Foreign Policy*, 2003: See www.foreignpolicy.com/wwwboard/fivewars.html.
[26] Makarenko, Tamara, "'The Ties that Bind': Uncovering the Relationship Between Organized Crime and Terrorism," in Siegel, Dina et al. eds., *Global Organized Crime: Trends and Developments*, Dordrecht: Kluwer Academic Publishers, 2003: 159-70.

[27] Dishman, Chris, "Terrorism, Crime and Transformation," *Studies in Conflict and Terrorism* 24 (1) (2001): 43-58.
[28] Williams, Phil. 1998. "Terrorism and Organized Crime: Convergence, Nexus or Transformation?" in Jervas (ed.). *FOA Report on Terrorism*, Stockholm, Defence Research Establishment: 69-92.
[29] Naylor, *Wages of Crime*: 45.
[30] Shelley and Picarelli, "Methods not Motives: Implications of the Convergence of International Organized Crime and Terrorism, Police Practice and Research."
[31] Schmid, Alex, "The Links Between Transnational Organized Crime and Terrorist Crimes," *Transnational Organized Crime* 2 (Winter 1996): 40-82.
[32] Silke, Andrew, "The Devil You Know," in Andrew Silke, ed., *Research in Terrorism: Trends, Achievements and Failures*, London: Frank Cass, 2004, pp. 57-71.
[33] Schmid, Alex and Albert Jongman, Political *Terrorism: A New Guide to Actors, Authors, Concepts, Databases, Theories and Literature*, North Holland: Oxford, 1988.
[34] Yin, Robert, *Case Study Research*, Thousand Oaks: Sage Publications, 2003: 5.
[35] Cressey, "Methodological Problems in the Study of Organized Crime as a Social Problem."
[36] See http://jdeis.cornerstoneindustry.com/jdeis/quickSearch/qsOverviewPortlet.jsp?conceptId=272&f=1&searchStr=I.
[37] Keegan, John, *History of Warfare*, New York: Random House, 1993: 63-76.
[38] Williams, "Terrorism and Organized Crime: Convergence, Nexus or Transformation?"
[39] Hoffman, *Inside Terrorism.*
[40] Benjamin, Daniel and Steven Simon, *The Age of Sacred Terror*, New York, Random House, 2003: 419-446.
[41] Some of the prior studies of crime-terror interactions that the TraCCC team consulted included Naylor, *Wages of Crime*; Phil Williams, "Terrorism and Organized Crime: Convergence, Nexus or Transformation?"; the Terrorism and Crime Studies conducted by the Federal Research Division of the US Library of Congress (see http://www.loc.gov/rr/frd/terrorism.html for a complete listing); and Jamieson, Alison, *Terrorism and Drug Trafficking in the 1990s*, Brookfield VT: Aldershot, 1994.
[42] For example, a terror group robs tourists for money and credit cards. The terror group comes to realize that it can leverage this by working with an organized crime group that can sell the credit cards. The terror group sells two batches of credit cards to the organized crime group, but then decides to return to simple theft. It has thus gone from activity appropriation to nexus and back to activity appropriation. Again, time and reward are the key analytical factors here—the terror and crime groups only came together twice and never found mutual benefit to support working closer together. Furthermore, steps could be eliminated, but the lack of trust between groups is a significant impediment that would have to be overcome.
[43] Horgan, John and Max Taylor, "Playing the 'Green Card'-Financing the Provisional IRA: Part 1," *Terrorism and Political Violence* 11(2) (Summer 1999): 1-38; Horgan, John and Max Taylor, "Playing the Green Card: Financing the Provisional IRA—Part 2," *Terrorism and Political Violence* 15(2) (Summer 2003): 11-7.
[44] Horwitz, Sari, "Cigarette Smuggling Linked to Terrorism," *Washington Post*, 8 June 2004: A1.
[45] Frankel, Glenn, "Police Pin Bank Heist on IRA," *Washington Post*, 8 January 2005.
[46] Our interviews.
[47] Cassidy, John, "UVF Link to Triad Gang: RUC Probe Attacks on Chinese Immigrants," *Sunday Mirror*, 2 July 2000.
[48] Our interviews.
[49] Dark networks have been defined as "adversaries who are modifying their structures and strategies to take advantage of networked design: e.g., transnational terrorist groups, black proliferators of weapons of mass destruction, drug and other crime syndicates, fundamentalist and ethno-nationalist movements, intellectual-property pirates, and immigration and refugee smugglers...urban gangs, rural militia groups, and militant single-issue groups...anarchistic and nihilistic leagues of computer-hacking 'cyboteurs,'....." See Arquilla and Ronfeldt, *Networks and Netwars*: 6-7.
[50] Dishman, Chris: "Terrorism, Crime and Transformation," *Studies in Conflict and Terrorism* 24(1), 2001: 43-58.
[51] However this may deserve further analysis in western European and American prisons where different crime-terror networks interact and may clash.
[52] Indeed, Naylor develops a spectrum of interaction between terrorism and organized crime in *Wages of Crime* that contains two non-cooperative stages prior to interaction between crime and terror.
[53] Cuthbertson, "Prisons and the Education of Terrorists."
[54] The same point was made by Daniel in his Istanbul address suggesting that the prison authorities did not recognize this and therefore did not isolate the terrorists from the criminals who they sought to recruit.
[55] This crucial difference between established and new transnational crime groups and their attitude to cooperation with terrorists is examined by Louise Shelley in an article entitled *The Unholy Trinity: Transnational Crime, Corruption, and Terrorism*, to be published in the *Brown Journal of International Affairs* (in press).
[56] Naylor, *Wages of Crime*, Chapter 4.

[57] Abadinsky, Howard, *Organized Crime*; Williams, "The Nature of Drug Trafficking Networks."
[58] Tang, Edward, "Thailand, the United Nations of Criminals?" *The Straits Times*, 10 Sep 2002.
[59] Picarelli, John, "Transnational Threat Indications and Warning: The Utility of Network Analysis," in David Jensen and Henry Goldberg, eds., *Artificial Intelligence and Link Analysis*, Menlo Park: AAAI Press, 1998: 88-93.
[60] Richardson, Lynda, "Father and Son Arrested in Sale Tied to Japanese Sect," *The New York Times*, 4 June 1996: B2.
[61] Hudson, Rex, *Terrorist and Organized Crime Groups in the Tri-Border Area (TBA) of South America*, Washington DC: U.S. Library of Congress, 2003: 43. See http://www.loc.gov/rr/frd/pdf-files/TerrOrgCrime_TBA.pdf.
[62] Miro, Ramon, *Organized Crime and Terrorist Activity in Mexico: 1999-2002*, Washington, U.S. Library of Congress, 2003: 24-5. See http://www.loc.gov/rr/frd/pdf-files/OrgCrime_Mexico.pdf.
[63] Daniel, "Terrorist Recruitment in European Prisons."
[64] Arostegui, Martin, "ETA has Drugs for Weapons Deal with Mafia," *United Press International*, 3 Oct 2002.
[65] Curtis, Glenn, *The Nexus Among Terrorists, Narcotics Traffickers, Weapons Proliferators and Organized Crime Networks in Western Europe*, Washington DC: U.S. Library of Congress, 2002: 11. See http://www.loc.gov/rr/frd/pdf-files/WestEurope_NEXUS.pdf.
[66] Williams, Phil and John Picarelli, "Information Technologies and Transnational Organized crime," in Alberts, David and Dan Papp, eds., *The Information Age Anthology: National Security Implications of the Information Age, Volume 2*, Washington DC: CCRP Publications, 2000: 365-402.
[67] Daniel, for example, noted that official visitors often provide these phones to inmates. See Daniel, "Terrorist Recruitment in European Prisons."
[68] *Transnational Crime, Corruption and Information Technology*, Washington DC: Transnational Crime and Corruption Center, 2000. See http://www.american.edu/tracc/Events/TC&IT_2000_Report.pdf.
[69] Berry, LaVerle et al., *A Global Overview of Narcotics-Funded Terrorist and Other Extremist Groups*, Washington DC: Library of Congress, 2002: 30-1.
[70] Talbot, David, "Terror's Server: How Radical Islamists use Internet Fraud to Finance Terrorism and Exploit the Internet for Jihad Propaganda and Recruitment," *Technology Review.com*, 27 January 2005. See http://www.technologyreview.com/articles/05/02/issue/feature_terror.asp?p=0.
[71] *Transnational Crime, Corruption and Information Technology*.
[72] *Transnational Crime, Corruption and Information Technology*: 12.
[73] "Al-Qaida Cyber Capability," Office of Critical Infrastructure Protection and Emergency Preparedness, Government of Canada, http://www.epc-pcc.gc.ca/emergencies/other/TA01-001_E.html.
[74] Denning, Dorothy, "Information Operations and Terrorism," Unpublished Manuscript, 2 Aug 2004.
[75] Soafer, Abraham and Seymour Goodman, eds., *The Transnational Dimension of Cyber Crime and Terrorism*, Stanford CA: Hoover Institution Press, 2001.
[76] Weinberg, Leonard and Louise Richardson, "Conflict Theory and the Trajectory of Terrorist Campaigns in Western Europe," in Silke, Andrew, ed., *Research on Terrorism: Trends, Achievements and Failures*, London: Frank Cass, 2004: 138-60; Poland, James, *Understanding Terrorism: Groups, Strategies and Responses* Upper Saddle River, NJ: Prentice Hall, 1988: chps 1-3 & 7.
[77] Works that have tackled the patterns of violence from the economic and sociological perspectives include Gambetta, Diego, *The Sicilian Mafia: The Business of Private Protection*, Cambridge: Harvard University Press, 1993; Varese, Frederico, *Russian Mafia: Private Protection in a New Market Economy*, Oxford: Oxford University Press, 2001; Volkov, Vadim, *Violent Entrepreneurs: The Use of Force in the Making of Russian Capitalism*, Ithaca: Cornell University Press, 2002.
[78] For much of the period since 1945, La Cosa Nostra had a cozy symbiotic relationship with Italy's Christian Democratic Party. The Mafia helped bring out the vote in Sicily and Southern Italy and in return received protection and was allowed a high degree of impunity. This relationship broke down during the 1980s with the emergence of crusading anti-Mafia magistrates such as Giovanni Falcone and Paolo Borsellino, increasing numbers of *pentiti* (turncoats) and large-scale criminal trials of the Mafia leadership. The Mafia was more vulnerable and felt a strong sense of betrayal. The result was a campaign of violence that started with the assassinations of politicians and magistrates and led to bombings and violent retribution against informers and their families. A bomb on the Naples-Milan train killed 15 and wounded 230. In 1993 a car bomb was planted in front of Rome's Olympic stadium during a soccer match (fortunately it failed to explode). Other operations had terrible consequences. Among the more notorious are the assassination of Salvo Lima, a Christian Democrat politician from Sicily who was a close ally of Prime Minister Andreotti; the 1992 assassinations of Falcone (along with his wife and three bodyguards) and Borsellino (along with five bodyguards) and the 1993 bombings on cultural landmarks including the Uffizi Museum in Florence and two churches in Rome.

[79] The terror attacks initiated by Pablo Escobar and Carlos Lehder of the Medellin Cartel in the mid-1980s included the assassination of the Justice Minister, Lara Bonilla, an attack on the Palace of Justice by the M-19 guerilla group in which information on drug traffickers was destroyed, and a bomb explosion on an Avianca aircraft.
[80] Gambetta, *The Sicilian Mafia*; Varese, *Russian Mafia.*
[81] Cornell, Svante, "Stemming the Contagion: Regional Efforts to Curb Afghan Heroin's Impact", *Georgetown Journal of International Affairs* 6 (1) (Winter/Spring): 2005; and Cornell, Svante, "Narcotics, Radicalism and Armed Conflict: The Islamic Movement of Uzbekistan," *Terrorism and Political Violence* 17: 2005.
[82] Jerbi, Monica, "Drugs, Thugs, Bombs, and Terror: Afghanistan's Spill Over and Central Asia" Unpublished Manuscript, Spring 2004. See http://www.american.edu/traccc/publications/studpub.html; Cornell, "Stemming the Contagion: Regional Efforts to Curb Afghan Heroin's Impact."
[83] Though it should be noted that not all organized crime groups are networked. Indeed, the Tri-Border Area case study notes that hierarchically-organized Triads have interacted with terror cells in the region.
[84] Sciolino, Elaine and Jason Horowitz, "The Talkative Terrorist on Tape," *The New York Times*, 12 July 2004; "In Their Own Words: Ahmed and a Protégé," *The New York Times*, 12 July 2004.
[85] The members of the March 11th 2004 Madrid bombing group are an exemplar of the evolving nature of terrorism. While they held a strong affinity for the goals of Al Qaeda and were influenced early on by a member of the September 11th conspiracy, but there is no evidence that they ever obtained direct assistance from Al Qaeda.
[86] Our interviews.
[87] Benjamin and Simon, *The Age of Sacred Terror*: 95-133.
[88] Arquilla and Ronfeldt, *Networks and Netwars:* 328
[89] Benjamin and Simon, *The Age of Sacred Terror:* 419-446
[90] Gambetta, *The Sicilian Mafia:* 48-52.
[91] Abadinsky, *Organized Crime.*
[92] Noble, Ronald, *The Links Between Intellectual Property Crime and Terrorist Financing*, testimony before the U.S. House of Representatives Committee on International Relations, 16 July 2003.
[93] Boliek, Brooks, "Interpol ID's Piracy Link to Funding of Terrorism," *The Hollywood Reporter*, 10 June 2004. See http://www.hollywoodreporter.com/thr/article_display.jsp?vnu_content_id=1000528473.
[94] Newell and Swan, "Trust and inter-organizational networking," *Human Relations* 53 (10) 2000: 1287-1328.
[95] Sageman, Marc, *Understanding Terror Networks*, Philadelphia: University of Pennsylvania Press, 2004: 99-107.
[96] Bartosz Stanislawski researched and authored this case study.
[97] This is an abbreviated version of a lengthy case study based on primary-source data from written documents, press releases, and three sets of interviews. The first set of interviews was conducted in Chile and Uruguay in the Spring of 1999 with officials from the Chilean, Paraguayan, Argentine, and Brazilian governments. The second set of interviews was conducted in CDE and the Tri-Border Area in the fall of 2002. The final set of interviews was completed late in 2004, and served to verify much of the contents of this case study. Information gathered in the Tri-Border Area region was conducted by means of ethnographic research comprising a series of interviews with residents of CDE, street vendors, store and restaurant owners, Brazilian tourists shopping in the city, and several police and border guard officers. In all cases consent to the interview was granted only on the condition of anonymity and thus no direct quotations are presented in the case.
[98] Bird, Kai and Max Holland, "Paraguay: the Stroessner Connection," *The Nation* 241, 26 October 1985.
[99] Rotella, Sebastian, "Jungle Hub for World's Outlaws," *Los Angeles Times*, 24 Aug 1998: 1.
[100] Our interviews.
[101] Rotella, Sebastian, "Jungle Hub for World's Outlaws."
[102] Berry, LaVerle et. al., *Nations Hospitable to Organized Crime and Terrorism*, Washington DC: U.S. Library of Congress, 2003: 174. See http://www.loc.gov/rr/frd/pdf-files/Nats_Hospitable.pdf.
[103] Our interviews.
[104] *ABC Color* [Internet version], May 28, 2002, as translated for FBIS, "Paraguay: Daily Reports More Evidence of Barakat's Contributions to Hezbollah," FBIS Document ID: LAP20020528000073.
[105] *Vanguardia* [CDE internet version], May 23, 2002, "Paraguay: Tri-Border Area Daily Says U.S. Has Not Shown Evidence Against Alleged Terrorist," FBIS Document ID: LAP20020523000084.
[106] *ABC Color* [Internet version], March 14, 2003, "Paraguay Press Highlights," FBIS Document ID: LAP20030314000106 (cited in Hudson, 2003); *ABC Color*, March 13, 2003, "Angola Ousts Lebanese Fugitive Linked to Hezbollah From Paraguay," FBIS Document ID: LAP20030313000120.
[107] Godoy, Marcelo, *O Estado de Sao Paulo* [Internet version], January 24, 2003, "Brazil: Lebanese Mafia Members in Sao Paulo Arrested, Drugs Seized," FBIS Document ID: LAP20030124000070.

[108] Berry, LaVerle et. al., *A Global Overview of Narcotics-Funded Terrorist and Other Extremist Groups*, Washington DC: U.S. Library of Congress, 2002: 16.
[109] Our interviews.
[110] Our interviews.
[111] *ABC Color* [Asunción], November 22, 2002, "Paraguay: 'Strong Ties' Seen Between Hong Kong Mafia, Tri-Border Area Hezbollah" (FBIS Document LAP20021122000047).
[112] Berry, Curtis, et al., *A Global Overview of Narcotics-Funded Terrorist and Other Extremist Groups.*
[113] Goldberg, Jeffrey, "In the Party of God," *New Yorker*, 28 Oct 2002.
[114] Sweeney, Jack, "DEA Boosts Its Role in Paraguay," *Washington Times*, 21 Aug 2001.
[115] *El Tiempo* [Bogota], 21 April, 2001, *El prontuario de Fernandiño* ("Fernandiño's Handbook); *El Tiempo* [Bogota], 22 April, 2001, *Muestran a Fernandiño a la prensa* ("Fernandiño Is Shown to the Press").
[116] Our interviews.
[117] *ABC Color* web site, February 5, 2002, as cited by "International Security Forces Search for Five Afghan fugitives in Paraguay, BBC Monitoring Service [UK]," 5 Feb 2002.
[118] Estado.com.br, 16 March 2003, "Bin Laden esteve em Foz do Iguacu e até deu palestra em mesquite." See http://www.estado.estadao.com.br/jornal/03/03/16/news245.html ; and "Bin Laden Reportedly Spent Time in Brazil in '95," *Washington Post*, 18 March 2003: A24.
[119] Bartolome, Mariano, "Amenazas a la seguridad de los estados: La triple frontera como 'area gris' en el cono sur Americano" [Threats to the security of states: the Tri-Border Area region as a 'gray area' in the Southern Cone], 29 November 2001:8. http://www.geocities.com/mcbartolome/triplefrontera1.htm.
[120] *El Pais* [Montevideo], 21 Nov 2002, "Justicia investiga atentado" ("Justice investigates the attack"); *La República en La Red*, 21 Nov 2002: 12, "Atendado a la colombiana contra vehiculo de Lissidini" ("Colombian-Style Attack on Lissidini's Car").
[121] Oviedo, Pedro, "En la Triple Frontera se lavan doce billiones de dòlares al año del narcotráfico, según un informe official" [Money Laundering of Drug Money in Tri-Border Area Reaches 12 Billion US Dollars Annually, Report Says] http://misionesonline.net/paginas/action.lasso?-database=noticias3&-layout=web&-response=noticia.html&id=11349&autorizado=si&-search (cited by Berry et al, 2003).
[122] Bartolome, Mariano Cesar, "Amenazas a la seguridad de los estados: La triple frontera como 'area gris' en el cono sur Americano" [Tri-Border Area is a security threat and 'gray area' in the Southern Cone], 29 November 2001:16. http://www.geocities.com/mcbartolome/triplefrontera1.htm (cited by Berry et al, 2003).
[123] Louise Shelley researched and authored this case study.
[124] Caglar, Ali. "Terror Spiral and General Overview," Presented at the Istanbul Conference on Democracy and Global Security, 10 June 2005.
[125] Ciobanu, Ceslav, "Frozen and Forgotten Conflicts in Post-Soviet States," paper presented at the US Institute of Peace in Washington DC, 22 July 2004.
[126] For more, see the research on terrorism produced by the Odessa Organized Crime Research Center, found at http://www.inter.criminology.org.ua/index.php?newlang=english.
[127] This case study is based on primary research in Moldova, Ukraine, Russia, and Georgia. Analysis of the two other Black Sea littoral countries, Bulgaria and Romania, informs this analysis but is not central to the discussion at hand.
[128] Kukhianidze, Alexandre et al., *Smuggling Through Abkhazia and Tskhinvali Region of Georgia*, Tbilisi: Polygraph, 2004: 24. See http://www.traccc.cdn.ge/publications/index.html.
[129] Landesman, Peter, "Arms and the Man," *The New York Times Magazine*, 17 August 2003: 28.
[130] Kukhianidze et. al., *Smuggling through Abkhazia and Tskhinvali*.
[131] Cengiz, Mahmut,"Profiling Organized Crime Groups in Turkey," paper presented at Istanbul Conference on Democracy and Global Security, 9 June, 2005.
[132] Ciobanu, "Frozen and Forgotten Conflicts in Post-Soviet States."
[133] See the work of the Money Laundering Project of the Transnational Crime and Corruption Center's Georgia Office, located at http://www.anitmoneylaundering.ge/ and www.traccc.cdn.ge.
[134] Teymur, Samih, "Terrorist Recruitment," paper presented at the Istanbul Conference on Democracy and Global Sceurity, 11 June 2005.
[135] Nabi Abdullaev researched and authored this case study.
[136] Handelman, Stephen, *Comrade Criminal: Russia's New Mafiya* New Haven: Yale University Press, 1995: 49.
[137] Khlebnikov, Pavel, *Razgovor s Varvarom (Conversation with a Barbarian)*, Moscow: Detektiv Press, 2003.
[138] Editorial, "Profile: Hozh-Ahmet Nuhayev," *RFE/RL*, August 24, 2001.
[139] Khlebnikov, *Razgovor s Varvarom*: 56-87.

[140] More on suicide bombers and particularly on use of women for suicide attacks in Abdullaev, Nabi, "Women at the Forefront of Chechen Terrorism," *ISN Security Watch*. See http://www.isn.ethz.ch/news/sw/details.cfm?ID=9781.
[141] Abdullaev, Nabi, "Picture of Their Methods Emerges," *The Moscow Times*, 6 Nov 2002: 1.
[142] "Chechen women have nightmares that their sons might become Wahhabis. In the Chechen mindset, these people might as well be dead." Our interviews.
[143] Classification offered by Boris Podoprigora, the deputy commander of the Russian troops in Chechnya in 2002, in "Kogda Zakonchitsya Chechenskaya Voina" (When the Chechen War Is Over)," *Fontanka.Ru*, 11 Dec 2003.
[144] On 8 March 2005 and after this case study was authored, Maskhadov was killed. For more, see http://news.bbc.co.uk/1/hi/world/europe/459302.stm.
[145] Karacheva, Yelena, "Falshivye Grazhdane (False Citizens)," *Argumenty I Facty*, 19 March 2003.
[146] See http://news.bbc.co.uk/1/hi/world/europe/459302.stm.
[147] Evident from the statements posted by Basayev at www.kavkazcenter.com and by Maskhadov at www.chechenpress.com; see "Chechen Leader Maskhadov Killed," *BBCNews World Edition Online*, 8 March 2005 at http://news.bbc.co.uk/2/hi/europe/4330039.stm.
[148] Yusupov, Musa, "Samoopredeliniye Chechni: Sostoyaniye I Perspektivy (Chechnya's Self-Determination: Current Condition and Prospects)," material for the seminar Ethnic Factors in the Federalization of Russia, Kazan, January 18, 2000. See http://federalmcart.ksu.ru/conference/seminar3/jusupov.htm.
[149] On May 21, 2004, a Moscow prosecutor office charged a 21-year-old Chechen woman with attempting to recruit terrorists among the young Chechen female parishioners in Moscow mosques.
[150] Less than a year after his election president, Maskhadov introduced Sharia courts and the Sharia criminal code.
[151] Estimate of the Russian Regional Public Fund for Rendering Security Assistance. See http://fssb.chat.ru/main/mag/8/home.htm.
[152] Borisov, Timofei, "Ekh Dollary, Da Na Tarelochke" (Dollar on the Plate)," *Rossiiskaya Gazeta*, 20 Nov 1999.
[153] See http://www.fsb.ru/press/2000/msg05191.html.
[154] Mintz, John, "U.S. Freezes Accounts of Large Saudi Charity," *Washington Post*, 20 Feb 2004.
[155] Mintz, John, "Head of Muslim Charity Sentenced," *Washington Post*, 19 April 2003.
[156] Editorial, "V Katare Arestovany Agenty Rossiiskih Spetssluzhb za Likvidatsiyu Yandarbiyeva (Agents of Russian Special Services Arrested in Qaatar for Killing Yandabiyev)," *Komsomolskaya Pravda*, See http://nnov.kp.ru/news/print/249952/.
[157] Meixler, "Pro-Chechen Groups Going Underground to Collect Money as Funding Stream Slows."
[158] Avdeyev, Sergei, "Chechentsy Poluchili Dostup k Yadernym Boyegolovkam (Chechens Gain Access to Nuclear Warheads,)" *Izvestia*, 22 March 2002.
[159] "Tver Region Captain of A Regiment Guarding Kalininskaya NPP Accused as Chechen Informant," Regnum, 19 Nov 2002.
[160] Douglas M. Hart and Patricia Craig-Hart researched and authored this report.