RUSSIAN ORGANIZED CRIME: WITHIN THE PARAMETERS OF A NATIONAL SECURITY THREAT

THESIS

Presented to the Graduate Council of
Texas State University-San Marcos
in Partial Fulfillment
of the Requirement

for the Degree

Master of SCIENCE

by

Valerie Hollier

Texas State University, San Marcos

San Marcos, Texas
August 2009

ACKNOWLDGEMENTS

I have a special circle of people whom I entrust to guide me. Individually they are family, friends and instructors--yet at times seem to embody all three roles. This thesis would not be a reality without their love and support. First and foremost, I must thank my mother. The concept of a "role model" has always seemed a little cliché to me until recently. My mother has continually proven herself a strong and confident woman, and I have tried my best to do the same. In that capacity, she is my role model. A special acknowledgement is extended to my stepfather. Thank you for impressing a sense of individualism upon me, and opening my mind to new extremes. Additionally, I thank my aunts and uncles: Dan, Lynna, Greg and Sonia. Their thoughts, prayers and continued support have given me the opportunity to attain the unattainable. Aside from family, I thank my friends Brooke, Jennifer, and Drew for always believing in me and providing the comic relief I desperately needed to complete this project.

I would also like to thank the instructors who guided me through the process of this project. Dr. Stafford, Dr. Vandiver, and Dr. Jamieson saw my vision, albeit a little too ambitious for a master's thesis, yet were patient enough to always guide me in the right direction. Overall, I consider Jennifer Carreon the most important instructor in the development and completion of this project. Jennifer is a colleague, yet throughout this entire process has demonstrated the intellect of someone far beyond her academic years. I

recognize Jennifer as a co-author in this project, as well as a lifelong companion with outstanding integrity in any situation.

The manuscript was submitted July 14, 2009.

TABLE OF CONTENTS

Page

ACKNOWLDGEMENTS iii

LIST OF FIGURES vi

ABSTRACT vii

CHAPTER

1 Introduction 1

2 Literature Review of Existing Studies 7

3 Research Methods and Procedures 33

4 Results 47

5 Conclusion and Discussion 57

REFERENCES 103

LIST OF FIGURES

Figure **Page**

4.1: Geographic Distribution of Economic Espionage Per Region 53

4.2: Geographic Distribution of Proliferation in Trafficking Per Region 54

4.3: Distribution of Targeting the National Information Infrastructure.....55

4.4: Geographic Distribution of Threat Categories 56

ABSTRACT

RUSSIAN ORGANIZED CRIME: WITHIN THE PARAMETERS OF A NATIONAL SECURITY THREAT

by

Valerie Hollier B.S.

Texas State University-San Marcos

August 2009

SUPERVISING PROFESSORS: DR. MARK STAFFORD & J.D. JAMIESON

Russian criminal enterprises are commonly understood among researchers and practitioners as an unconventional addition to the umbrella of existing organized crime groups. Recent literature attempts to convey Russian organized crime (ROC) as a significant threat to the U.S. by pinning the sophistication of Russian enterprises against the traditional methods of mafia groups. This thesis uses a combination of relevant literature and previously defined threat assessment variables as groundwork to establish ROC as a security threat in the U.S. Ultimately, results from this study suggest that ROC should be considered a national security threat, and establishes a geographic pattern of high- risk activity per region.

CHAPTER 1

Introduction

This chapter examines the international reach of transnational organized crime groups and addresses the potential threat caused specifically by Russian crime groups. Additionally, a brief overview of the method used in this study to assess Russian Organized Crime (ROC). In order to evaluate ROC as a national security threat, a series of follow-up interviews from a previous study were conducted using a pre-defined threat assessment method. To supplement this information, an Internet search utilizing Google News revealed articles that indicated ROC in one of the three pre-defined threat categories- proliferation, economic espionage and targeting the information infrastructure. Geographic points of reference from the news articles were used as data and imported into a mapping software program to visually portray "hot spots" of ROC.

The Global Threat of Organized Crime

Twentieth Century methods of transnational organized crime are only recently recognized as a complex phenomenon and significant global threat. This criminality weakens the stability of individual countries, but it is not yet officially recognized as a

threat to the United States. Transnational criminal organizations, however, present a unique threat to the U.S. due to the complexity of their activities, their ability to operate worldwide, and the threat they present to the market economy (Shelly, 2001). *The Need to Study ROC*

The Columbian, Italian and recently emerged Eastern and Central European organized crime groups are most commonly known for their ability to operate transnationally, along with the Chinese Triads, Japanese Yakuza and various Nigerian groups (Shelley, 2001). In particular, this thesis examines the various threats Russian organized crime (ROC) pose to the U.S., and attempts to determine whether their activities qualify as criteria for threats to national security.

Worldwide, Russian enterprises are involved in money laundering as well as trafficking of a variety of goods and services. The degree of skill and professionalism that Russian enterprises operate make it virtually impenetrable (Fickenauer, 2004). Recent literature illustrates the threat ROC poses, as well as the need to further understand the emergence of this highly decentralized and skilled group of criminals.

Background of Problem

The History of ROC

The potential threat ROC poses to the U.S. results from a variety of historical, economical and political aspects of influence. Organized crime in Russia is an institutionalized part of the political and economic development, and through years of collaboration with various spheres of societal influence, organized syndicate groups have gained substantial control over a large part of the Russian market (Serio, 2008).

Soviet Era (1927-1991).

ROC evolved and was shaped by the peculiar characteristics of the Soviet economy and politics. The short supply of goods and services during the seven decades of Soviet power led to the emergence of the "shadow economy" and the "black market". Years of successful operation in these illegitimate markets created a rewarded and conniving mentality among those who participated, thus creating a shadowy entrepreneurial class accustomed to operating outside the law (Alexeev, Gaddy, Lietzel,, 1995).

During the Soviet era, organized crime evolved into a three-tiered pyramid structure. At the top were Apparatchicks, or high-level government officials and Communist Party bureaucrats. Second, was the shadow economy and Black Market operators. At the bottom were the most sophisticated of the professional criminals, the Vory v Zakone, or products of the Soviet gulag prison system. Criminal actors among the three-tired pyramid blended legitimate with illegitimate activity in order to meet the demands for goods and services in Communist Russia (Galeotti, 2005).

Post-Soviet Era (1991-Present)

Post-soviet Russia produced an even larger demand for goods and services, thereby creating more opportunity for organized crime. The transition from communism to capitalism presented many opportunities for corruption at all levels of influence in Russia. Furthermore, there has been a failure to enforce law pertaining to organized crime in Russia as a result of mixing law from the former Soviet Union with recent efforts to abandon communism in favor of capitalism. Lack of uniformity in the law created a chaotic environment in which criminal networks thrived, and combined with the degree

of professionalism and skill at which they operated and the ability to corrupt government, ROC was able to penetrate other markets (Lietzel, et. al., 1995).

In particular, Russian entrepreneurs recognized the opportunity for organized crime in the U.S. and took advantage of the opportunity to immigrate. ROC became present in the U.S. and various other markets, creating a criminal enterprise that did not exist previously. With the ability to operate transnational, and the variety of highly skilled criminals, ROC became the source of many legitimate and illegitimate activities. Due to the diversity of transnational crimes organized groups are able to successfully commit, ROC is significant at a global level. More importantly, as a result of the legitimate sectors of the economy ROC has penetrated, efforts to dislodge these networks will come at a high price for the U.S.

ROC in the U.S.

Domestic ROC groups have caused economic damage in the U.S. by participating in a wide variety of activities such as fuel scams, health care fraud, bank fraud, stock market manipulation, and internet scams. These types of activities have shown the aptitude for circumventing the bureaucracy, rules, and procedures of government agencies, financial institutions, insurance companies and other businesses (O'Neal, 2000). ROC further threatens these institutions by blending legal and illegal operations, making it difficult for law enforcement agencies to detect their activities (Fickenauer & Waring, 2001).

ROC as a Threat to National Security

Although relevant literature suggests ROC as a threat to the U.S., there have been no attempts to establish any specific kind of threat. This paper attempts to establish ROC

as a threat to national security. There is a limited amount of research in this area, and less evaluating the various threats posed by ROC. Due to ongoing national security issues and recent economic downturn in the U.S., there is a need for awareness among the intelligence community, law enforcement, and society about the potential security threat ROC can pose. Criminal participants operate with a degree of sophistication and professionalism that is difficult to combat. Research that geographically measures activities of ROC may be helpful to formulate policy and tactical solutions to address the potential security threat.

Overview of Regional Assessment

Recent literature suggests measuring ROC regionally in order to focus on the personality, group structures, types of criminal activities, areas of operation, international linkages, and trends of Russian enterprises to determine which jurisdictions and potential criminal markets are most prone to exploitation (Webster, 1997). Using a regional assessment might be useful as a tool for allocating resources to combat organized crime in areas identified to be at great risk for ROC infiltration.

One of the purposes of this paper is to identify types of ROC in the U.S., and establish whether their activities fall under pre-defined categories for threats to national security; proliferation, economic espionage, and targeting the information infrastructure. The interview data will be used to formulate a regional assessment of organized crime in the U.S., and determine if activities are specific to certain geographic areas. In addition, a series of news articles identifying incidences of ROC as one of the three threat categories will be used as supplementary information. Geographic points of reference from each article will be used as data points to regionally map criminal hotspots of ROC. Both sets

of data will be used to identify regions most prone to the activities of ROC that fall under the pre-defined categories of threats to national security.

CHAPTER 2

Literature Review

ROC is best understood within a theoretical background that includes a historical and social perspective (Albini, Rogers, Shabalin , 1995). This chapter examines the history of ROC, and provides an overview of the various ways Russian crime groups have gained power and influence over the decades. First, a brief summary of the rise and fall of communism will illustrate the chaos in post Soviet Russia, which created an environment suitable for political and economic corruption. This environment created a demand for a "shadowy" market, in which goods and services were obtained through illicit means. Furthermore, legitimate business was at risk of extortion by officials, fraudsters, robbers, and gangs. The most notorious criminal fraternity in Russia, however, the vory v zakone, had somewhat of a monopoly over crime during this time. The vory had a tremendous influence on newly emerging criminal groups, and especially a "Russian Mafia".

Next, a brief explanation is given as to how three waves of immigrants increased Russian crime groups to the U.S. A comparison between ROC and traditional types of organized crime builds the discussion of ROC as a vastly different phenomenon. In addition to their ability to penetrate legitimate and illegitimate markets, members of the Russian criminal organizations operated with a level of professionalism and

sophistication, making it difficult for law enforcement to detect. A review of previous literature summarizes the various activities Russian crime groups are domestically and internationally involved with, for the purpose of providing an understanding of the threat ROC poses in the U.S. The information in the literature review is used as framework for this study.

This chapter also introduces a previous study that establishes variables to measure the risk of a crime group. An explanation of how these variables are used to evaluate ROC as a threat to national security is also included.

History of ROC

Soviet-Era Politics

The collapse of communism created what became known as the "transition state". In midst of the widely anticipated gap of Soviet power, which occurred after a breakdown of old power structures, an enormous amount of opportunities arose for achieving wealth and power, which criminal entrepreneurs and corrupt officials clearly took advantage of (Rawlinson, 2001). Prior to the fall of communism, Soviet-era politics created a social and economic climate suitable for greed and corruption (Schwartz, 1979).

Corruption and organized crime were prevalent in the ancient Soviet regime. Although the state was the supposed owner of goods and services, it was the people of the union who carried out state planned operations. Furthermore, the many individuals that had control over goods and services could illegally trade them through informal markets (Leitzel et al., 1995). For example:

> . . . butchers could sell choice cuts of meat "through the back door", a transaction favored and practiced by nearly all retail clerks. Consumers could use bribes to

> move to the front of queues for scare commodities such as automobiles. Special employees of state-owned enterprises used connections and bribes to secure vital supplies for the company. Even housing, constitutionally guaranteed in the U.S.S.R. to be distributed on the basis of need and with very low rents, was allocated in large measure via formal and informal markets. (1995, p. 17)

Money did not play the same role in the Soviet economic system as it does in a capitalist system. Moreover, political corruption, economic negligence, commodity scarcity, and unequal distribution of wealth created an opportunity for personal connections to perform the functions of the redistribution of goods and services (Frisby, 1998). Where there was a shortage of goods and services, the people of the state compensated using illegal means, thus commencing a system of near-total corruption.

Post Soviet-Era

The result of corruption among the various levels of society created fantastic wealth for few, and left almost a third of the nation below the already low poverty line. Those who had accumulated wealth were afraid of deceitful actions on behalf of their competitors, and afraid of criminals who used violence as a means of gaining wealth and power. Mostly, they were all fearful of the states power, greedily depriving them of life, liberty and property (Leitzel, et al., 1995; Schwartz, 1979).

The increase of crime in Russia during the early 1990s can be attributed to a demoralized working class, disillusioned by the declining standards of living and lack of prospects for social guarantees (Rawlinson, 2001). Many Russians felt betrayed by the state, and would do almost anything to avoid poverty. Crime began to increase in 1991

and 1992; crime rates fell in 1993 and stabilized in 1994. In reality, however, the crime rate was increasing because more people were becoming involved in criminal activity. The old Soviet Criminal Code became obsolete, and new forms of crime became latent by nature due to the inability to categorize them in emerging criminal law (Frisby, 1998).

Not only were law enforcement suffering from lack of coordination, they became increasingly entangled with the volume of work in processing all information (Frisby, 1998). The turnover among professionals in the investigative staff became high, and professionalism and morale sank rapidly. Wages were negatively affected by inflation; corruption among staff became a means for survival (Frisby, 1998). These circumstances created a need for private protection. Many resorted to taking justice into their own hands, with assistance from criminal fraternities. As a result, a "shadow justice" emerged, dictated by criminals and violence.

The most notorious source of private protection came from the inner-workings of Perm, an eastern city in Russia. The city is a major administrative, industrial, scientific, and cultural center. The leading industries include machinery, defense, oil production (about three percent of Russian output), oil refining, chemical and petrochemical, timber and wood processing and the food industry (Varese, 2001). Certain types of legitimate business were at great risk for harassment by officials, fraudsters, robbers, and gangs.

To minimize harassment, business-people turned to protection rackets. The best "roof" of protection was either provided by the state or the KGB, the Committee for State Security. They were able to provide people who were formerly part of those structures and had become businessmen. Some businessmen, however, would unknowingly buy bogus protection from swindlers. Imposters would pass as to real Mafiosi, use the

reputation of violent mafia-types as an illusion for a protection racket, take the money and run. Varese (2001), offers an example from Joe Serio, a former security consultant in Moscow.

> . . .An American firm was approached by three wannabes in search of easy money. They presented themselves as members of the Chechen criminal community, knowing that the Chechens have a reputation for being particularly fierce. The Moscow representative of the firm did not pay and the would-be Mafiosi failed to show up again (Varese, 2001, p. 95).

In the city of Perm, the operation of criminal protection rackets arose from the demand of business people being victimized by violent criminals, the vory v zakone. The vory v zakone, also known as the "thieves world", were a powerful group of criminals infiltrating Perm and other Russian cities. These criminals were from the gulag population of the Soviet prison (Sterling, 1994).

The Vory v Zakone

The vory v zakone, or "thieves in law" formed as a society for mutual support within the prison camps, ruled the shadowy gaps in Soviet life beyond the reach of the KGB, adopted a system of shared responsibility, and swearing a code of "complete submission to the laws of criminal life, including obligations to support the criminal ideal, and rejection of labor and political activities" (Varese, 2001, p. 152). For example, if a Vor was incarcerated in a prison camp, he had to refuse to perform any labor, as the code stipulated "Thy own prison shalt thou not make" (Varese, 2001, p 151). The group exclusively organized courts around a code of thieves honor and tradition. Furthermore,

acceptance into the group was often marked by extensive tattooing, indicating rank within the society, as well as criminal accomplishments (Handelman, 1995).

While the Communist Party had a steadfast grip on government and society, the Vory had something of a monopoly on crime. The vory v zakone are the strategists for all criminal undertakings in and out of prison, and were chosen by others for their superior intelligence and dominating personas. The Vory had nationwide policy meetings for clan representatives, thus able to form a loose structure of criminal networks. They were known for their ability to finance operations, bribe officials, support convicts families, as well as mediate peace within the group and maintain authority of the thieves' code (Varese, 2001).

After the breakup of the Soviet Union the Vory assumed a leading role within the Russian criminal hierarchy. The group was able to "infiltrate the top political and economic strata while taking command of a burgeoning crime network that spread murderously through the post-Soviet countries" (Varese, 2001; p. 175).

As capitalism took hold of Russia, an increasing number of college-educated criminals began to take over more lucrative ventures. While these new criminal actors first worked with the Vory in the 1990s, in the first decade of the 21st Century, ties to big business and government became more important. Consequently, the Vory are still actively involved in gambling and retail, but their importance in Russian economy has decreased.

The Vory have slowly been killed in what resembles ordinary gang warfare and intra-group conflicts. However, the Vory is an enormous factor in the development of the post Soviet Russian criminal network due to withstanding ability to instill traditions in

newly emerging criminal groups. Varese (2001) explains how the traditions of the vory have not disappeared.

> Their rich apparatus of rituals, rules of interaction, and mythology is being used in the new environment. After a period of transition, when entry criminal fraternities went virtually unchecked, territorially based groups resurrected the vory rituals. The vory ritual now marks the entry of powerful crew leaders into the "governing body" of the biggest criminal groups in Moscow. The governing body of the Solntsevo is a coalition of the vory. A number of other crime groups are said to be in broad agreement with the Solntsevo.

The groups that share Vory rituals and norms of interaction are federated with each other, and constitute what is commonly known as the Russian Mafia (Varese, 2001). However, the modern day Russian criminal network is not exclusively made up of criminal fraternities and does not necessarily operate as a traditional mafia, but as a criminal enterprise.

The "Russian Mafia" in Russia

The Russian criminal enterprise is made up of 12 to 15 major structures, each bringing a myriad of individual and small gangs or groups together, essentially making up a loose network of 3,000 to 5,000 participating criminal groups. Each group has a broad range of criminal interests, activities, and specializations (Galeotti, 2005). Participants include traditional mafia criminals, as well as scientists, PhD's, computer programmers, engineers, and various other professionals. Moreover, the Russian criminal enterprise is made up of a variety of ethnicities such as Georgians, Chechens, Ukrainians, Armenians, Azeris, Lithuanians, and Tartars (O'Neal, 2000). In Russia, these networks

are involved in extortion, drug trafficking, gambling, prostitution, fraud schemes, corruption of government officials and businessmen, ultimately enabling them to move billions of dollars outside of the country (O'Neal, 2000).

Due to the complexity of loose and flexible criminal networks, ROC is significantly threatening on a global level. However, due to the willingness of the U.S. to accept foreign immigrants, participants of ROC have been able to obtain citizenship and permanently reside there, thus creating an even larger threat for the U.S. ROC came to the U.S. in three waves of immigration.

Immigration Brings ROC to the U.S.

There have been immigrants to the U.S. from Mother Russia since the earliest days of European settlement in North America. Recent years, however, have seen increasing levels of U.S. immigration in general and from Russia in particular. This variation is due to a number of factors including political and social conditions in the former Soviet Union, U.S. regulation of immigration, U.S. political and economical conditions, and global events such as both world wars and the depression in the 1930s (Fickenauer, 1998). The two most recent wave of Russian immigrants included a variety of participants from the Russian criminal network (O'Neal, 2000).

The first wave of Russian immigrants in the U.S. arrived between 1970 and 1980. This group contained approximately 100,000 refugees, including a small number of criminals, dubbed "fraudsters" by law enforcement. These small groups of criminals were able to operated independently, or form loose-knit criminal networks to commit crimes, including a variety of confidence and white-collar schemes (O'Neal, 2000).

During the mid 1990s, the second wave of Russian immigrants arrived in the U.S. Due to political and economic chaos in Russia during this period, the number of Russian immigrants grew to 340,000. In addition, thousands of individuals entered with temporary visas and remained illegally. Many "professional" criminals made it to the U.S. during this time, and were less sophisticated, violent, and gang-oriented. This group of criminals provided illicit services such as prostitution, gambling, and extortionate credit (O'Neal, 2000).

The two waves of Russian immigrants brought a variety of different criminals into the U.S, all with the ability to successfully pull off scams that have shown the aptitude for circumventing the bureaucracy, rules, and procedures of government agencies, financial institutions, insurance companies, and businesses.

The Capabilities of ROC

Domestic ROC groups have caused the most economic damage in the U.S. by participating in white-collar crime such as fuel scams, health care fraud, bank fraud, and stock market manipulation (Galeotti, 2005). Criminal participants act with professionalism and sophistication and come together based on the specific skill sets needed to pull of the scam. After the scam is successfully completed, the small network of criminal participants disband, essentially making their activities undetectable to law enforcement agencies. In addition, ROC groups are different from traditional mafia structures in the U.S. because they do not fit orderly models. In ROC cases, investigators cannot effectively adopt the model pyramid charts they routinely use to outline the leadership rank and file such as La Cosa Nostra (O'Neal, 2000).

Traditional Organized Crime in the U.S.

Organized crime developed around the black market created by the void left between public demand for alcoholic beverages (and the other vices of prostitution and gambling) and the prohibition of them. Illegal alcohol manufacturing and distribution of speakeasies were prime factors in the development of organized crime in the U.S. during the 1920s. Albanese (1989), explains:

> Brewers of alcoholic beverages have a choice in 1920: shut down, covert their equipment to make legal one-half percent liquor, or do business as usual by becoming partners with questionable people who would market their product. Organized crime groups slowly evolved into more sophisticated criminal enterprises, as was made necessary by competition from other criminal entrepreneurs, to evade law enforcement, and to bribe public officials when necessary. (Albanese, 1989, p. 99)

These types of illicit operations were linked to traditional mafia structures, such as La Cosa Nostra.

Structure of Organization

In 1963, Joseph Valachi testified to the existence of a nationwide organization involved in widespread criminal activities. Valachi, an admitted lower-level criminal was associated with the Italian Genovese crime "family" in New York City. Valachi described the organization structure of the Cosa Nostra as consisting of individual bosses of individual families, with an underboss, a caporegima which is a lieutenant, and lower-level soldiers (Albanese, 1989). Although many organized crime figures testified about

La Cosa Nostra and other crime families, decades passed until public officials settled the debate over the existence of a "Mafia".

Combative Tactics

It was not until the 1980s and 1990s when the U.S. took new initiatives and began prosecutions of a large number of organized crime figures in courts around the country. The increase in prosecutions was not due to new laws, but was the result of utilizing existing resources to combat the problem. The Presidents Commission on Organized Crime (1986) was created by an executive order of President Reagan on July 28th, 1983.

The commission was directed to engage in a wide variety of activities, including public hearings, litigation, research studies and surveys, and investigations. Albanese (1989), effectively summarizes the seven public hearings and explain the focus on:

> Federal law enforcement strategies, money laundering, the activities of organized crime groups of Asian origin (Chinese, Japanese, and Vietnamese groups), narcotics trafficking (specifically cocaine and heroin importation and distribution), labor and management racketeering, and legal and illegal gambling activities. (Albanese, 1989, p. 77)

In addition, the committee went on to describe a host of other organized crime entities such as,

> Outlaw motorcycle gangs (Outlaws, Hells Angels, Bandidos, Pagans, Prison gangs (Mexican Mafia, La Nuestra Familia, Aryan Brotherhood, Black Guerilla Family, and Texas Syndicate), Cuban Marielito crime gangs, Columbian cocaine rings, and Russian organized crime groups or gangs allegedly operating in a number of cities across the country (Albanese, 1989, p. 77).

The commission recognized the failure of authorities to recognize any organized crime group but La Cosa Nostra, and the barrier it created for law enforcement. Furthermore, the commission recognized exclusively focusing on La Cosa Nostra would divert attention from the range of persons and groups potentially responsible for the majority of organized crime in the U.S (President's Commission, 1986). Building on these findings, Albanese (1989) reports three significant developments regarding U.S. organized crime in the past two decades. First, an increasing awareness of existing organized crime groups; second, the success of law enforcement against La Cosa Nostra, which it called the largest, most extensive, and most influential crime group in this country; and third, the increased involvement of organized crime in drug trafficking operations.

ROC vs. Other Organized Crime

In the mid 1990s, literature recognized emerging methods organized crime groups. Albanese (1989) explains this phenomenon as a function of criminal organizations responding to opportunities to crime as well as their ability to circumvent techniques of crime prevention and law enforcement. Organized crime groups around the world came together because of the enormous profits to be made. For example, in the late Twentieth Century, drug trafficking became the primary catalyst in the internationalization of organized crime.

Widely available telecommunications capabilities, accessible air travel enhanced, and political changes around the world made international travel possible almost everywhere. To ensure chances of survival, organized crime groups came together to take

advantage of international mobility and create an opportunity for their interests, thus creating a more sophisticated method of organized crime (Albanese, 1989).

Enhanced Professionalism

In particular, ROC was gaining notoriety among other criminal groups due to their proficiency in business. Friedman (2000, p. 34) explains, "the Italians were particularly impressed with the Russians' growing adeptness at bilking financial markets, which was aided by members of younger generation of Russians who were now returning from graduate schools with MBAs and getting jobs on Wall Street".

In addition to enhancing professionalism, prior literature suggests ROC participants are taking advantage of recent developments of international mobility, and becoming significantly involved in transnational criminal activity. For example, in an article discussing transnational organized crime as a threat to the U.S., Shelley (2001) explains how organized criminals from the former Soviet Union have perpetrated gasoline tax evasion in the New York-New Jersey area on a mass scale. Shelley further describes how ROC differs from traditional organized crime:

> While many crime groups specialize in a particular area such as drug trafficking, prostitution rings, gambling or weapons smuggling, post-Soviet organized crime is involved in a full range of illicit activities, including large-scale penetration into legitimate economy. (Shelley, 2001, p. 481)

In terms of sophistication and transnational operation, prior literature suggests ROC as a vastly different organization, as compared with traditional organized crime in the U.S. For example, traditional mafia groups are structured, and ROC groups are highly

decentralized. In addition, ROC groups participate in a wide variety of frauds and schemes that are virtually undetected by law enforcement, causing a significant threat in the U.S. However, a review of recent literature may be helpful when attempting to identify specific threats ROC poses to the U.S.

The Threat of ROC in the U.S

Characteristics of ROC

In a case study involving the activity of organized crime in the Urals, Fickenauer and Voronin (2001) examine a variety of ways ROC is a threat to the U.S. First, a defining characteristic of ROC is the use of violence to gain and maintain control of criminal markets. This is not surprising, due to extortion and protection rackets being used as a method of control among Russian enterprises. In the U.S., it is common for ROC groups to use arson against business that refuse to pay extortion money. For example, a 1999 case involving six ROC affiliates reflects arson as a means of violence; the perpetrators were terrorizing business owners to extort money.

Diversification of Activity

Another defining characteristic of ROC in the U.S. is the type of criminal activity. With exception to extortion and money laundering, Russian enterprises have little to do with traditional means of organized crime such as drug trafficking, gambling and loan sharking. Instead, ROC participants are involved in a range of frauds and scams including health care fraud, insurance scams, stock frauds, antiquities swindles, forgery and fuel tax evasion schemes. More recently, ROC enterprises have become the main source of credit card fraud in the U.S. (O'Neal, 2000).

Possibly the most defining characteristic of ROC is their ability to adept to change their activities and diversify into new criminal markets. A 1999 laundering case is used by Fickenauer and Voronin (2001) to illustrate the ability of ROC to involve participants in legitimate sectors of the economy. This case involved the Bank of New York (BONY). Russian organized crime used BONY to launder criminal money, as well as to assist Russian businesses and individuals in moving their assets out of Russia for the purpose of evading Russian law enforcement and tax officials.

The BONY case is illustrative of criminal diversification among ROC groups, and more importantly, their ability to blend of illegal and legal operations to avoid detection. Building on this notion, Fickenauer and Voronin (2001) suggest a long-term implication of ROC penetrating legitimate markets is that it will become increasingly more difficult to dislodge it.

Decentralization

O'Neal, a former instructor in the Investigative Training Unit at the FBI Academy, addresses the challenges faced by U.S. law enforcement when combating ROC in his article *Russian Organized Crime-A Criminal Hydra*. O'Neal (2000) explains that unlike the American La Cosa Nostra, the Italian Mafia, or the Chinese Triads, and other ethically-oriented crime groups, ROC typically does not fit orderly models; therefore, presenting an investigative hurdle to law enforcement accustomed to using pyramid charts to outline the leadership and rank and file of organized crime groups.

O'Neal (2000) discusses his experience with organized crime groups, explaining how past efforts to effectively combat organized crime involved identifying the leadership and chain of command of the target group, essentially leading to successful

investigations and prosecutions. Furthermore, traditional groups have permanent hierarchical structures and operate within specific geographic areas whereas ROC groups combine gangs that act independently or have loose ties to regional, national, or international networks, therefore making it difficult for law enforcement to identify a centralized ROC group.

Threatening Activities

O'Neal (2000) further discusses how the spread of ROC outside the borders of the former Soviet Union is the main concern of law enforcement in the U.S. Specifically, white-collar crime represents the greatest domestic threat posed by ROC, due to participant connection with other well-financed ROC groups. The more sophisticated ROC fraud includes fuel scams, health care fraud, bank fraud, and stock market manipulation.

Fuel Fraud

For example, fuel fraud has caused significant economic damage in the U.S. by the loss of hundreds of millions of dollars in tax revenues. O'Neal (2000, p. 4) clarifies the method of fuel fraud:

> By creating labyrinthine chains of burn corporations' and falsifying tax forms, ROC groups have deprived state and federal governments of substantial tax revenues. Other fuel frauds include blending fuel, rigging fuel pumps, and selling low-grade fuel as premium.

O'Neal (2000) also examines recent alliances ROC groups have formed with other criminal organizations, and illustrates the impact this had on traditional schemes of

organized crime groups. For example, ROC advanced the "pump and dump" stock fraud schemes for which La Cosa Nostra members have received much attention. ROC groups developed a more sophisticated method in which they release false information to encourage investors to purchase stock and to artificially inflate the value (the pump). After Russian fraudsters feel they have investors in a vulnerable position, they sell for a profit of the shares they had purchased prior to the fraudulent promotion (the dump). La Cosa Nostra, becoming increasingly aware of the money Russian enterprises made from this method of stock market manipulation, informed ROC groups they would work as partners in this scheme.

Medical Fraud

According to O'Neal (2000), ROC is taking advantage of the most costly crime in America, health care fraud. ROC groups successfully commit complex healthcare fraud schemes involving Medicare, Medicaid and private insurance companies through false and inflated claims. Staged accidents and "rolling labs" (mobile labs that conduct unnecessary tests) include fake doctors, pharmacists, medical supply companies, and attorneys.

Bank Schemes

ROC also is involved in a variety of bank fraud schemes. O'Neal examines the typical schemes ROC is involved in such as check kiting, credit card fraud, and bankruptcy fraud, in addition to the innovative measures of bank fraud. For example, and Armenian ring in Los Angeles devised and automated teller machine (ATM) car fraud scheme. This group employed electronic surveillance equipment and computers. According to O'Neal (2000, p. 3):

> The subjects, who included bank and service station insiders and a computer expert formerly employed by a national research laboratory, used computer-operated decoding devices and hidden video cameras to steal the magnetic codes and personal identification numbers of thousands of cards.

Computer Hacking

Lorek (2001) examines the threat posed by ROC rings by hacking into U.S. ecommerce and banking websites. Lorek found that ROC groups are penetrating computers in the U.S. to illegally obtain profits. In detail, Lorek explains how Russian enterprises exploit vulnerabilities in operation systems like Microsoft Windows NT, resulting in a number of ecommerce fraudulent schemes such as stealing credit card information and bank account numbers:

> By gaining access to a company's computer system, hackers are able to download proprietary information (i.e., trade secrets, customer databases, and credit card information) and then demand money to patch their systems against other hackers. To ensure funds are appropriated properly, ROC groups use violence to eliminate competition and informants and to punish those who abscond with funds. (Lorek, 2001, p. 13)

Furthermore, Lorek makes clear the uncertainty as to whether or not these attacks are indeed tied to the Russian "mafia". However, it is certain that street vendors sell Russian hacking software, and that Russian websites offer hacking tools (Lorek, 2001).

Dangerous Leaders with Transnational Connections

Although ROC does not follow a traditional hierarchical structure, there are "god father: figures, known for causing significant economic damage in the U.S. In their book

"Angels, Mobsters & Narco-Terrorists", Antonio Nicaso and Lee Lamothe discuss two prominent Russian mobsters, Vyacheslav Ivanknov and Simon Mogilevich.

Ivankov

Ivankov arrived in the United States in March 1992, after serving a prison sentence of around ten years and a reputation as one of the fiercest criminals in Russia. He had arrived on a regular business visa stating that he would be working in the film industry (Niscaso & Lamothe, 2005).

Niscaso and Lemothe summarize a number of operations Ivankov was allegedly involved in between 1992 and 1995, ranging from bribery the arms trading of military equipment that included machine guns and anti-aircraft defense systems worth $20 million. Law enforcement became increasingly concerned with Ivankov's power in the Russian network, and in may of 1994, the FBI formed C-24, a Russian organized crime squad in New York City. C-24 informants found that Ivankov had a "combat brigade", responsible for aiding him with murders, including the deaths of five or six top Russian crime figures. The "combat brigade" received a salary of $100,000 per month (Niscaso & Lamothe, 2005).

Despite the efforts to expose Ivankov, the FBI could not turn up enough evidence to get a wiretap from his phone. However, a relative of Ivankov, Vyacheslav Sliva, arrived in the U.S. shortly after serving a prison sentence in Canada. Authorities alerted U.S. law enforcement of Sliva's intention to conspire with Ivankov, and within days the FBI was authorized to wiretap Sliva's phone. By mid-June, C-24 had gathered enough evidence- through wiretaps, surveillance, and victim's complaints, to bring up Ivankov and five member of his crew on extortion charges (Niscaso & Lamothe, 2005).

Ivankov was arrested by the FBI in June 1995, charged with the extortion of several million dollars from an investment advisory firm run by two Russian businessmen, and in June the next year was convicted along with two co-defendants. This rises suspicion as to whether Ivankov was a big-time crime boss, since usually the criminal architects at the top are protected from direct criminal activity by several layers.

Niscaso and Lamothe summarize the weeks and months following Ivankov's incarceration as a barrage of bizarre events, in which a propaganda campaign in both the U.S. and Russia broke out, claiming Ivankov had been set up by the FBI so they could show that a major Russian vor had been taken down. Despite the attempts of several prominent figures to prove Ivankov a "revolutionary", Ivankov was ordered to be held for trial without bail (Niscaso & Lamothe, 2005).

On July 13, 2004 Ivankov was deported to Russia to face murder charges over two Turkish nationals who were shot in a Moscow restaurant. The jury found him not guilty and he was acquitted the same day on July 18, 2005. The witnesses, a police officer among them, claimed to have never have seen him in their lives (Niscaso & Lamothe, 2005).

Conclusively, evidence is lacking to link Ivankov with his role in the international Eastern European underworld. However, there is little doubt of the power of his expansive criminal organization. Niscaso and Lamothe compare Ivankov's reach and power with another Russian figure, Semion Mogilevich.

Mogilevich

In 1990, already a millionaire, Mogilevich moved to Israel, together with several of his associates. Here he invested in a wide range of legal businesses, continuing to

operate a worldwide network of prostitution and weapon and drug smuggling through a complex web of offshore companies. In 1991 Mogilevich married his Hungarian girlfriend, obtaining a Hungarian passport; at this point Mogilevich held Russian, Ukrainian, Israeli and Hungarian citizenship. Living in outside Budapest, he continued to which produced anti-aircraft guns (Niscaso & Lamothe, 2005).

In May 1995, a meeting in Prague between Mogilevich and Sergei Mikhailov, head of the Solntsevo group, was raided by police. Police had been informed that the Solntsevo group was going to execute Mogilevich at a party over a disputed payment of $5 million. Shortly after, the Czech Interior Ministry imposed a 10-year entry ban on Mogilevich, while the Hungarian government declared him persona non grata and the British barred his entry into the UK, declaring him one of the most dangerous people in the world (Niscaso & Lamothe, 2005).

In 1997 and 1998, the presence of Mogilevich and others associated with ROC groups behind a public company, YBM Magnex International Inc., trading on the Toronto Stock Exchange, and were exposed by Canadian journalists. On May 13, 1998 dozens of agents for the FBI and several other U.S. government agencies raided YBM's headquarters in Newtown, Pennsylvania. Shares in the public company, which had been valued at $1 billion, became worthless. Until 1998, Inkombank and Bank Menatep participated in the laundering of $10 through the Bank of New York (Niscaso & Lamothe, 2005).

In 2003, the FBI put Mogilevich on the "Most Wanted List" for participation in the scheme to defraud investors in YBM Magnex International Inc. Frustrated by previous efforts to charge him for arms dealing and prostitution, they had now settled on

the large-scale fraud charges as their best chance for obtaining a prosecution. He was still, however, considered possibly the most powerful Russian criminal around (Niscaso & Lamothe, 2005).

Niscaso and Lamothe (2005) depict Ivankov and Mogilevich as prominent figures of ROC crime, capable of operating in both legitimate and illegitimate markets, without leaving much of a paper trail. Furthermore, Niscaso and Lamothe (2005) assert their international reach as a threat to the U.S., because they have associates everywhere.

Methodically Evaluating the Threat of ROC

In their article "Challenging the Russian Mafia Mystique", Fickenauer and Waring (2001) suggest no evidence towards the existence of a "Russian Mafia", but that crime being committed by Russian criminals in an organized manner has the potential to pose a threat to U.S. law enforcement, due to the flexibility of the organization. Through the analysis of 404 separate documents collected by the Tri-State Joint Soviet-Émigré Organized Crime Project (TSP), a questionnaire, and in-depth interviews with individuals about ROC, Fickenauer and Waring intend to discover whether ROC is "mafia-like.

According to the TSP investigation, fraud is the most common type of crime among Russian criminals in the U.S., fuel tax being the greatest concern among law enforcement. Other fraudulent schemes include counterfeit credit cards, checks, Immigrations and Naturalization Service documents, and passports. Russians are also involved in the drug trafficking market through Columbian routes, and show a willingness to use violence including murder, extortion, and assaults (Fickenauer & Waring, 2001).

Fickenauer and Waring present a dichotomous view of the "Russian Mafia": (1) it does exist, and there is support of Vyalcheslav Ivankov as a "godfather" type figure; and (2) it does not exist, due to individual operations that do not fit hierarchical structure. Ultimately, Fickenauer and Waring conclude that neither view is entirely correct, and that there is evidence to support Russian crime and the nature of ROC in the U.S. is evolving.

Evaluating ROC as a National Security Threat

Recent literature has given insight about specific threats ROC poses in the U.S. Common themes throughout the literature point to several conclusions.

- Russian crime groups participate in a wide variety of frauds and schemes, blending legitimate and illegitimate markets to widen their economic gain in the U.S.
- ROC is highly decentralized. Loose and flexible criminal networks enable ROC to operate on a transnational level, making it difficult for U.S. law enforcement agencies to detect.
- Russian enterprises are comprised of a variety of criminal participants with different skill sets. They operate with professionalism and sophistication, and have the ability to pull of scams that cause significant economic damage in the U.S.

Although there have been attempts to identify ROC as a threat to the U.S., none have sought to pinpoint any specific kind of threat. This thesis will evaluate ROC as a threat to national security by expanding on a previous study by Jennifer Carreon (2009), "Organized Crime as a Threat to National Security", which evaluated the activities of criminal organizations. Overall, the purpose of the study was to establish organized crime

as a threat to national security. The study used a unit of analysis suggested by Albanese (2008) in which the risk of organized crime can be greater assessed by targeting high-risk activities. Assumingly, "following the activities will lead to the high risk people involved with them" (2008, p. 13).

Using a Previous Measurement

In order to establish the activities of organized crime groups as a threat to national security, a comparison was made among federal agencies as to what constitutes a threat to national security. The Federal Bureau of Investigations' (FBI) national security threat contains eight key threat issues, and was used as a major point of reference because it is the leading investigative agency in the U.S. According to the FBI, the eight key threat issues include Terrorism, Economic Espionage, Proliferation in Trafficking, Targeting the Information Infrastructure, Targeting of the U.S. Government, Espionage, Perception Management, and Foreign Intelligence Activities.

Targeting the U.S. Government, Perception Management, Espionage, and Foreign Intelligence Activities were not considered threat categories among the other federal agencies, and were not used as variables of measurement in the study. Table 1 illustrates commonalities among the federal agencies that combat organized crime in reference to what activities are considered a security threat (Department of Homeland Security, 2008; Federal Bureau of Investigation, 2008; U.S. Department of Justice, 2005, 2007, 2009).

Ch. 2; Table 2.1 Commonalities Between what Agencies Percieve as Threating Activity

	Terrorism	Economic Espionage	Proliferation in Trafficking	Targeting the Information Infastructure	Targeting of the U.S. Government
FBI	X	X	X	X	X
DEA			X		
ATF	X		X		
DOJ	X	X	X	X	X
DHS		X		X	X

Notes. "X" indicates agreement with threat category. FBI = Federal Bureau of Intelligence; DEA = Drug Enforcement Administration; ATF= Alcohol, Tobacco and Firearms; DOJ= Department of Justice; DHS= Department of Homeland Security (Carreon, 2009).

Organized Crime as a Threat to National Security

An analysis of the variables revealed at least three out of five agencies agreed each category constitues a threat to national security. In order to establish organized crime as a threat to national security, operational definitions of each threat category were compared with the activities of organized crime groups. The study found the activities of organized crime groups fit into three out of five threat categories, proliferation in trafficking, economic espionage, and targeting the information infrastructure.

The study emphasized various ways organized crime groups participates in the three categories. For example, proliferation in trafficking, including drugs, arms and humans; economic espionage, including scams and frauds that effect the U.S. economic structure; and targeting the information Infrastruture, including unauthorized computer

hacking for the purpose of gathering sensitive information. Conclusively, Carreon (2009) established organized crime as a threat to national security, due to the nature of its activities and participation in three out of five threat categories. This study will utilize the method of measurement found in Carreon's (2009) "Oragnized Crime as a Threat to National Security", to establish the activities of ROC as a national security threat. In addition, this study will analyze the geographic distribution of the network's criminal activities in the U.S. in order to determine whether certain areas are more prone to being effected by ROC.

ROC as a Threat to National Security

Previous literature describes various ways ROC thrives in the U.S. including participation in a variety of white collar scams, trafficking in human and drugs, as well as cyber crime (Fickenauer & Voronin, 2001; Fickenauer & Waring, 2001; Fickenauer, 2004; Galeotti, 2005; Lorek, 2001; O'Neal, 2000). The next chapter relies upon this information as framework to establish ROC as a national security threat, as well as outline the method for collecting and analyzing original data.

CHAPTER 3

Methods

Description of Research Approach

This thesis utilizes Carreon's (2009) threat-assessment variables to establish ROC as a threat to national security. Carreon established Proliferation, Economic Espionage, and Targeting the Information Infrastructure as major variables when assessing the security risk of a criminal organization. ROC participants are involved in all three of these activities, internationally and within the U.S. In addition, ROC as a domestic threat to the U.S. This study utilizes the previously mentioned variables, as well as interviews, news articles, and mapping software in order to determine if ROC is a national security threat. It is useful to recognize the highly qualitative nature of both studies, and justify for the method of sampling used.

The Use of Informants in Qualitative Research

Statistical representativeness is not necessarily needed when conducting qualitative research given that the objective is to better understand the social phenomenon, in which usually little information is available. Therefore, it is common to use non-probabilistic methods of samples in qualitative research. This approach to sampling allows the researcher to identify a wide range of individuals who are present in

circumstances relevant to the social process being studied (Mays & Pope, 1995).

Interviews from Previous Study

Carreon (2009) conducted 10 interviews with agents from the Organized Crime Drug Enforcement Task Force (OCDETF). Interview participants were selected by using a non-probablistic sample convenience sample, representing confidential informants. Furthermore, in order to effectively determine the geographic distribution of activites, Carreon (2009) targeted participants in major regions of the U.S., West, Midwest, South, and Northeast (as defined by the U.S. Census Bureau). Ultimately, the final sample included four OCDETF task force agents, and six OCDETF U.S. Attorneys. Carreon encouraged interviewees to participate in a follow up interview about ROC.

Interviews for ROC Study

For the purpose of her study, Carreon (2009) inquired about the presence of ROC in each region. Participants who indicated a presence of ROC became informants for this study and were contacted for a follow-up interview about the nature and extent of ROC activity in their region. In the event the interviewees did not wish to participate in a follow- up interview due to the sensitivity of the subject, or if there was no indication of ROC in their region, they were asked to provide contact information for another OCDETF agent who would participate. The interview relied upon for this study was constructed by using information from preliminary interviews.

Creation of Interview

A series of preliminary interviews were conducted in order to determine the need to further examine the threat ROC poses to the U.S (see Appendix A). Informants remained anonymous, and included five experts in the field of ROC, both practitioners

and researchers. When questioned about Russian crime groups in the U.S., participants confirmed the possibility of their activities posing a security threat. Moreover, data from the interview confirmed that ROC groups heavily participate in the activities (Carreon, 2009) established as a national security threat. To further understand the security threat ROC groups potentially cause in the U.S., the information from the preliminary interviews was used to compile a series of questions which indepthly focused on the risk assessment variables: proliferation, economic espionage and targeting the national information infrastructure.

Interview Participants

Of the 10 informants contacted, two informants refused to participate, but they provided contact information on other OCDETF agents in that region, and the contact information was used to produce two alternative informants. The final sample consisted of one ATF OCDETF agent, five FBI OCDETF agents, and four OCDETF U.S. Attorneys.

Format of Interview

Using a semi-structured interview with open ended questions, informants were questioned about the structure and activity of ROC groups in their region, as well as the effect of ROC groups on their communities. Additionally, participants were asked to describe any barriers to tactical solutions against ROC. Participants were asked if they felt ROC is a threat to national security, and if so, why (see Appendix B).

Supplementary Data

To supplement the data from the interview, news articles containing information about ROC were analyzed on the basis of high- risk activity and geographic location.

News articles pertaining to ROC in the U.S. with specific geographic references were analyzed and used as data points to import into mapping software. The objective of using supplementary data in this study is to reconcile information in the interviews with external records of ROC. Essentially, news articles were used to determine if occurences of ROC in the U.S. fit within the threat categories, and if the occurence was specific to a geographic area. In turn, this information was used to pinpoint geographic locations most prone to the threat of ROC.

Google news, a search engine that archives news articles by date and content, was used to find articles pertaining to ROC in the U.S. The search term "Russian Mafia" was selected because of its ability to encompass all news articles covering ROC. While academics and practitioners hesitiate to make reference to a "Russian Mafia", it is a term generally used by the media to describe Russian crime groups (Rawlinson, 2000). Therefore, using "Russian Mafia" as a search term would essentially produce the largest number of news articles.

The selection of articles was limited to those between 2002 and 2009. Justification to use this time frame was based on information obtained in a preliminary interview, suggesting a shift in combative focus after 9/11 from organized crime to terrorism, ultimately allowing ROC groups to thrive in the U.S. Furthermore, article selection was limited to those that mention a geographic reference and criminal occurence within the U.S.

Sampling

Google News produced 9,440 results for the search term "Russian Mafia". Therefore, guidelines were set in order to facilitate an efficent data- gathering process and

reduce the number of articles to be analyzed. First, a sample size calculator was used to determine the number of articles needed to attain a representative sample. For a 95% confidence level, the calculator showed that 100 of the 9,440 articles needed to be sampled.

Using systemic sampling, every 60th article was chosen for the sample, unless it did not produce useful information. For instance, some articles did not contain a geographic location within the U.S., or any information about an occurence of ROC. In any of those circumstances, the next article was reviewed, and so on until useful information was found. At that point, the sampling continued, and the next 60th article was reviewed. Information from the article was used as data to import into a MapPoint, a computer program that produces a visual output of the geographical distribution of criminal activity.

Research Questions

Data from the interview, as well as news articles and maps are, used to answer the following research questions:

> Research Question 1: Do the activities of ROC groups fit within the pre-defined threat categories (Proliferation, Economic Espionage, and Targeting the Information Infrastructure) and pose a potential security threat to the U.S.?
>
> Research Question 2:Are their activities specific to certain geographic areas?
>
> Research Question 2a: If activitites are related to specific geographical areas, are there regions in the U.S. more prone to certain types of high risk activity that fit within the pre-defined threat categories?

In order to answer these questions, it is necessary to first operationally define the concepts and variables.

Operational Definitions

ROC

ROC has been described in many different ways. This study, however, conceptualizes ROC by using a definition from an article by Galeotti (2005) entitled, "The Russian 'Mafiya': Consolidation and Globalisation". Galeotti (2005) characterizes ROC as "a distinctive, even post-modern phenomenon, characterized by loose and flexible networks of semi-autonomous criminal entrepreneurs and with an especially keen awareness of the political environment in which it operates" (Galeotti, 2005, p. 55). This defintion is the most current, and includes all the elements of ROC discussed in literature.

Threat-Assessment Variables

The threat-assessment variables in this study are those that have an effect on national security: proliferation, economic espionage and targeting the information infrastructure. Carreon (2009) established these as major variables when assessing the risk of criminal groups. These activities are part of a larger list of what the FBI considers "key threat issues". This study, therefore, uses the FBI's definition of proliferation, economic espionage, and targeting the information infrastructure, as well as give insight as to how organized crime falls into these categories.

1.) Proliferation – Foreign power-sponsored or foreign power-coordinated intelligence activity directed at the U.S. Government or U.S. corporations, establishments or persons, which involves:

- the proliferation of trafficking or creating weapons of mass destruction to include chemical, biological, or nuclear weapons, and delivery systems of those weapons of mass destruction;
- the proliferation of trafficking or creating advanced conventional weapons;
- the proliferation of trafficking illicit drugs or;
- the proliferation of human trafficking.[1]

2.) Economic Espionage – Foreign power-sponsored or foreign power-coordinated intelligence activity directed at the U.S. government or U.S. corporations, establishments, or persons that involves:

- the unlawful or clandestine targeting or acquisition of sensitive financial, trade or economic policy information, propriety economic information, or critical technologies; or
- the unlawful or clandestine targeting of influencing sensitive economic policy decisions.[2]

3.) Targeting the National Information Infrastructure – Foreign power-sponsored or foreign power-coordinated intelligence activity directed at the U.S. Government or U.S. corporations, establishments, or persons which involves the targeting of facilities,

---

[1] Organized crime groups participate in the illicit trafficking of arms, drugs and humans (Carreon, 2009).

[2] Crime groups unlawfully gain access to sensitive economic information and/or critical technologies that enable them to successfully pull off a variety of frauds and schemes (Carreon, 2009).

personnel, information, or computer, cable, satellite, or telecommunications systems which are associated with the National Information Infrastructure. Proscribed Intelligence activities include:

- Denial or disruption of computer, cable, satellite, or telecommunications services;
- unauthorized monitoring of computer, cable, satellite, or telecommunications systems;
- unauthorized disclosure proprietary or classified information stored within or communicated through computer, cable, satellite, or telecommunications systems;
- unauthorized modification or destruction of computer programming codes, computer network databases, stored information or computer capabilities; or
- manipulation of computer, cable, satellite, or telecommunications services resulting in fraud, financial loss, or other federal criminal activities.[3]

---

[3] Organized crime groups participate in a variety of cybercrime by illegally gaining access to network databases, and downloading proprietary information (i.e., trade secrets, customer databases, and credit card information), resulting in fraud as well as financial loss (Carreon, 2009).

Data Collection and Analysis

Data Collection

Interviews were given to ten participants, both federal agents and U.S. Attorneys from OCDETF units. In addition, a total of 100 news articles with specific reference to ROC were taken from a population of 9,440.

Data Analysis

A content analysis was preformed on the interviews to reveal common themes. In addition, each news article was summarized by specific elements: content, date, activity and geographic location of activity. The geographic location of activity was converted into latitudinal and longitudinal points, and used as data to import into MapPoint, a program used to map criminal activity.

Content Analysis of Qualitative Data

Content analysis is a method in social sciences to study the content of communication, most commonly applied when analyzing transcripts of interviews. The assumption underlying content analysis is that words and phrases used during interviews are communacative of important concerns. In turn, keywords can be derived from words and phrases to form a basis for coding data (Hagan, 2007). Hagan (2007, p. 266) suggests that the reliability of a content analysis is dependent upon its replicability, that is, "a different group, using the scoring sysem and instructions assigned to come up with the same categorizations".

A content analysis is best suited for the interview and supplementary data in this study because it is qualitative, and categorically restrictive. For example, high- risk activities are categorized as proliferation in trafficking, economic espionage, or targeting

the national information infrastructure. Furthermore, to verify the reliability of the content analysis, two groups of graduate students were given the instructions for coding the interview and supplementary data. Both groups assigned roughly the same codes to both sets of data, thus verifying the reliability of the content analysis. The system for coding the interview and supplementary data is outlined below.

Coding Method for Interview

Feedback from interview participants is used to identify key words and phrases in order to assign codes for each question. Multiple codes are used for questions if the interviewee provided information that fit more than one category. The first question inquires about the types of activities linked to Russian crime groups for each region. The available codes for this question include; economic espionage, proliferation in trafficking, or targeting the information infrastructure.

- Economic Espionage - activity such as money laundering, medical fraud, bank fraud, ATM fraud, identity theft, real estate fraud, or phishing scams.
- Proliferation in Trafficking - participation in illicit trafficking of arms, drugs, or humans.
- Targeting the National Information Infrastructure - Russian crime groups illegally gain access to network databases in order to download proprietary information (i.e., trade secrets, customer databases, and credit card information) resulting in fraud and financial loss.

The purpose of the second question is to identify the structure of Russian crime groups for each region. The available codes for this question include: highly decentralized, small networks, or large networks.

- Highly Decentralized - Russian crime groups are not at all structured, and/or operate internationally.
- Small networks - Russian crime groups act in small groups and/or on an individual basis.
- Large networks - Russian crime groups act in large groups.

The third question asks the interviewee to describe any barriers to combatting ROC in their region. This question was not coded, however, due to the wide range of information provided by interview participants. Instead, the information will be used in the concluding statements of this paper to form a discussion about tactical solutions for ROC.

The fourth question asks the interviewee to describe the effect of ROC on communities that encompass his region. The available codes for this question include: no threat to community, semi-threat to community, or significant threat to community.

- No Threat to Community - Russian crime groups act only in their interest, and do not inflict harm on community members.
- Semi-Threat to Community - Russian crime groups are sometimes linked to murder, arson, or violent crimes in the region.
- Significant Threat to Community - Russian crime groups are often linked to murder, arson, or violent crimes in the region.

The purpose of the fifth question is to determine to what degree the interview participant felt ROC affects national security. The available codes for this question include: no threat to nation, semi-threat to nation, or significant threat to nation.

- No Threat to Nation - ROC does not have the potential to effect national security.
- Semi Threat to Nation - ROC has the potential to effect national security because of variation in activity, and sophisticated operation.
- Significant Threat to Nation- ROC is a significant threat to national security due to its international reach, and ability to pull of frauds and scams that cause significant damage to the U.S.

Coding Method for News Articles

The method to code news articles is the same as used in the first interview question. News articles were reviewed to identify a high risk activity, and coded according to the category into the activity which fit. Multiple codes are given to articles which indicate more than one high risk activity. It is useful to note that the codes are essentially derived from the threat categories, in order to determine if certain regions are more prone to high- risk activity. Codes for the news articles include: economic espionage, proliferation in trafficking, and targeting the information infrastructure.

- Economic Espionage - activity such as money laundering, medical fraud, bank fraud, ATM fraud, identity theft, real estate fraud, or phishing scams.
- Proliferation in Trafficking - participation in illicit trafficking of arms, drugs, or humans.
- Targeting the National Information Infrastructure - Russian crime groups illegally gain access to network databases in order to download proprietary information (i.e., trade secrets, customer databases, and credit card information) resulting in fraud and financial loss.

Coding Method for Maps

A similar approach called "hotspot analysis", suggested by Hagan (2007), will be used to analyze the output from MapPoint. Hagan (2007) suggests this method to compare the locations of hotspots across time, or simply to compare different types of crime in terms of high- risk areas. To further expland on hotspot analysis, Hagan (2007, p. 77) references the Charolette Mecklenberg Police homepage:

> Crime hotspots that have been identified over several months can be displayed at the same time. This allows for the identification of areas with chronic problems and indicates the direction in which a crime problem may be shifting. These types of maps can also be used to solicit resources for an area from other public and/or private in order to work towards solving a community's problems.

Hagan demonstrates the capability of hotspot analysis when attempting to identify areas most prone to high- risk activity, and the potential to use it as a guide for combative efforts. Thus, hotspot analysis was applied to the geographic data in the study through the use of MapPoint, in order to pinpoint areas most prone to high risk activity of ROC.

Assumptions

There are several assumptions with reference to ROC as a national security threat. First, information within the interviews will correspond with the pre-defined threat categories, thus establishing their participation in activities which constitute a national security threat. Second, interview data will reveal ROC is regionally distributed among certain regions, and that certain areas are more prone to high-risk activity. Third, details from the articles will support interview data, and further establish ROC is regionally

distributed. The distribution of ROC will executed by using geographical mapping software, in order to portray "hotspots" more prone to high-risk activity.

Limitations

Response Rates

Although federal agents participated in the interviews and provided useful information concerning ROC, data collection during the study did not go without problems. Initially, response rates were low due to the gravity of the topic. Some informants from Carreon's (2009) study expressed their uneasiness to talk about ROC because some of the information was confidential. Once assured of their anonymity and ability to stop the interview whenever they felt neccesary, however, most agreed to participate.

Additionally, only federal agents participated in the interview. No information was obtained from local law enforcement officials. Therefore, results are not be generalizable because only the views and opinions of federal agents were obtained. It may have been useful to contact local police departments and interview officers about their experiences with ROC.

This study became extensive in terms of time and money. There was a limited amount of time to conduct the interviews, thus reducing the sample size. Had there been more time to contact more agents willing to participate, the sample size could have been larger. Furthermore, this project was unfunded and had to be conducted within a budget. If funds were available, it would have been possible to travel to different regions to conduct the interviews and gain a rapport with the participants. In effect, estabilishing a rapport may have lead to gaining more contacts, and possibly increasing the sample size.

CHAPTER 4

Results

The following pages contain an outline of commonalities found within the interview data (see Appendix C). In addition, a report of news articles is discussed by region to geographically illustrate the areas most prone to high risk activity. Results and findings from interview and supplementary data will be used to form conclusions about the research questions (see Appendix D for news sources). Appendix C contains coded interviews, and Appendix D lists sources for the news articles.

Discussion of Interview Analysis

Geographic regions previously stipulated by the U.S. Census Bureau will be used in the content analysis. The regions are classified as South, West, Midwest, and Northeast.

Southern Region: Texas, Florida, and Maryland

In the southern region, Russian crime groups participate in a wide range of activities, which fall into all threat categories: economic espionage, proliferation in trafficking, and targeting the information infrastructure. Crime groups in Florida participate heavily in frauds and schemes, while Maryland and Texas are concentrated with groups involved in the trafficking of illicit goods and services. In addition, groups in

Texas are heavily involved with cybercrime. In regards to structure, most Russian crime groups are highly decentralized. However, there are small networks acting in Maryland. Finally, two out of three interview participants agreed that ROC is a regional and national security threat.

Western Region: Washington, California, and Colorado

In the western region, Russian crime groups contribute to proliferation in trafficking and economic espionage. Interview participants from all three states described trafficking as a lucrative market within their regions. In addition, Washington and California have groups that participate in various fraudulent schemes, such as identity fraud, healthcare fraud, and credit card fraud. In relation to structure, most Russian crime groups are comprised of small networks, except in the California area where they are highly decentralized. Overall, participants agreed ROC is a semi-threat to surrounding communities and a significant threat to national security.

Midwestern Region: Michigan and Illinois

In the Midwest, Russian crime groups are mostly occupied with proliferation in trafficking. In Michigan, trafficking for the purpose of sexual slavery is common. In addition, Russian crime groups frequently smuggle tobacco into Illinois. Economic espionage is somewhat of a threat in Michigan, due to health insurance fraud, credit card fraud, and fuel scams. With regards to structure, most ROC groups operate within small networks. In general, interview participants gave information about ROC as a regional threat, yet they strongly agreed that ROC is a national security threat.

Northeastern Region

ROC groups in the Northeast participate in a variety of activities, such as stock market manipulation, financial scams, money laundering, and trafficking in goods and services, thus filling all threat categories-proliferation in trafficking, economic espionage, and targeting the information infrastructure. In reference to structure, ROC groups are mostly decentralized, with some small and large networks. Overall, interview participants designated ROC as a significant threat to surrounding communities and national security.

Conclusions

Overall, interview data show that ROC participants are involved in economic espionage and proliferation in trafficking throughout the U.S. In addition, there have been significant attacks to the national information infrastructure in the southern region. Accordingly, ROC seems to involve all predefined threat categories. In regards to structure, participants generally indicated that Russian crime groups operate in small networks. As a final point, most interviewees agreed that ROC is a security threat locally and nationally. A brief report of news articles is discussed below in an attempt to support interview data.

Report of News Article Data

Supplementary data will be reported by region in order to show the concentration of high-risk activity in certain geographic areas.

Southern Region

The sample of news articles shows the south is heavily concentrated with activity that falls under all three threat categories: proliferation in trafficking, economic espionage, and targeting the national information infrastructure. For instance, ten articles

mention activity that threatens the national information infrastructure; 17 articles cover activities related to economic espionage, and seven articles report on trafficking incidences. Overall, Texas seems to contain the most amount of activity in the U.S. that threatens the national information infrastructure such as network and systems hacking. In addition, there were reports of activity that constitutes economic espionage in Texas and Florida, including credit card fraud, medical fraud, money laundering, and identity theft. There were articles to confirm activities related to proliferation, such as trafficking of drugs, arms, and human trafficking in both Texas and Florida.

Western Region

Again, news articles confirm activity in all three threat categories: proliferation in trafficking, economic espionage, and targeting the information infrastructure. For example, five articles mention activity that threatens the national information infrastructure; 15 articles cover activity related to economic espionage; and nine articles report on trafficking incidences. In general, the western region accounts for the most articles that report proliferation in trafficking, especially in California, with several articles that cover drug and arms trafficking rings. In addition, the articles show California is heavily concentrated with activity that constitutes economic espionage, such as extortion and credit card fraud. There was a smaller number of reports of attacks on the national information infrastructure, such as computer hacking and fraud in California and Arizona.

Midwestern Region

The Midwest has a small number of articles to support activity that constitutes economic espionage and proliferation in trafficking. For instance, five articles cover

activity related to economic espionage, and three articles report on trafficking incidences. There are reports of proliferation in trafficking of humans and drugs in Kansas and Oregon, as well as trafficking of goods in Illinois. In addition, articles mention activities that constitute economic espionage, such as insurance fraud, credit card fraud, money laundering and extortion in Michigan, Oregon, and Iowa. Overall, this region is not heavily concentrated activity in any of the threat categories.

Northeastern Region

The sample of news articles show the northeast is concentrated with activity that falls under all three threat categories: proliferation in trafficking, economic espionage, and targeting the national information infrastructure. For example, eight articles mention activity that threatens the national information infrastructure; 14 articles cover activity related to economic espionage; and seven articles reported on trafficking incidences. In general, activities that constitute economic espionage, such as money laundering, extortion, stock market manipulation, and fuel tax evasion are reported throughout New York, New Jersey, Pennsylvania. In addition, several articles report instances of trafficking of arms and drugs in New York and New Jersey. Finally, there were a smaller number of reports of attacks on the national information infrastructure, such as internet scams and network hacking, in New York and Pennsylvania.

Similarities Between Interview and Supplementary Data

Overall, supplementary data reinforce interview data illustrating that ROC participants are highly involved in economic espionage and proliferation in trafficking throughout the U.S. In total, there are 52 articles reporting activity that constitutes economic espionage and 27 articles that report on trafficking incidences. For instance,

both interview and supplementary data indicate that proliferation in trafficking is common throughout California, Texas, Florida, New York, New Jersey and Pennsylvania. Also, activity related to economic espionage is prevalent in California, Texas, Florida, New York, and New Jersey. The majority of the 22 articles reporting attacks on the national information infrastructure came from the southern region. Therefore, supplementary data support information from the interviews, showing attacks on the information infrastructure are common in the south, especially in Texas. Overall, ROC seems to include all predefined threat categories in both interview and supplementary data. The following pages contain a hotspot analysis of the supplementary data, in order to visually illustrate the concentration of high-risk activity in certain geographic areas.

Geographic Distribution of Economic Espionage Per Region

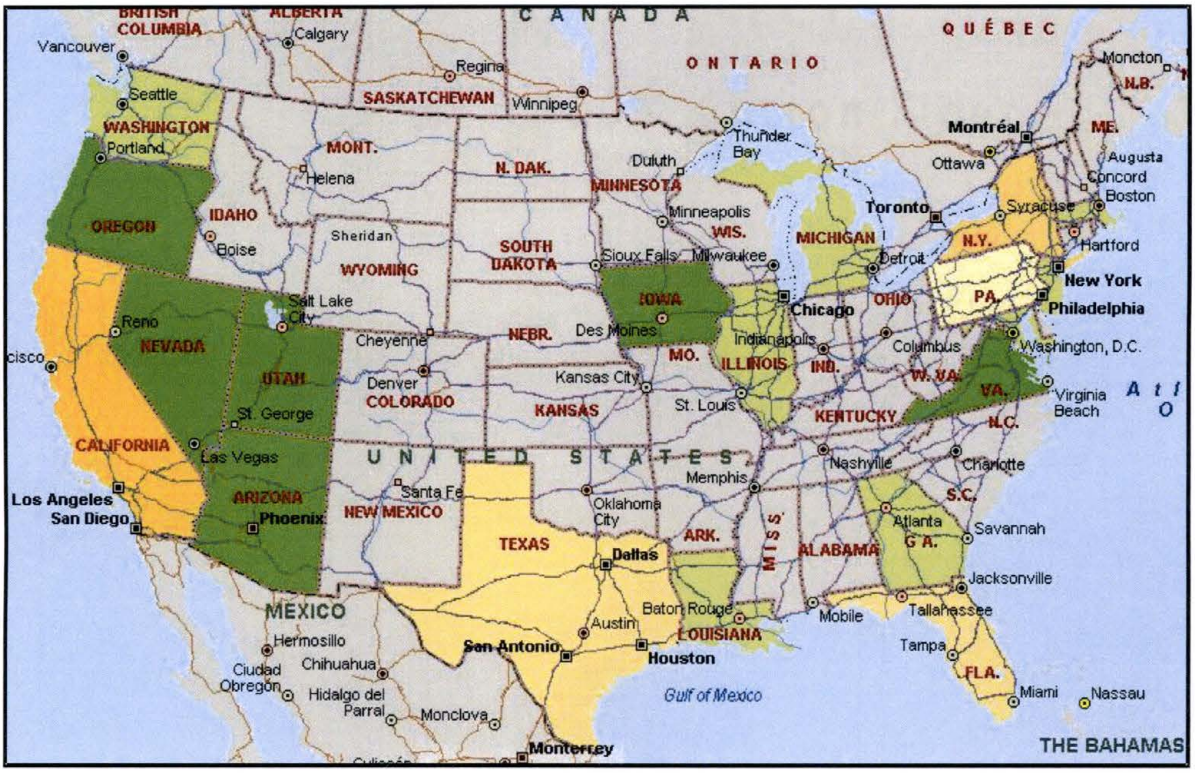


Figure 4.1 Economic Espionage in the U.S.

Number of Incidences

9

5

1

Reports of high-risk activities that constitute economic espionage were mostly in California, New York and Texas. There are some reports in Florida, Pennsylvania and Texas as well as Georgia, Illinois, Louisiana, and Michigan.

Geographic Distribution of Proliferation Per Region

Figure 4.2 Proliferation in Trafficking in the U.S.

Number of Incidences

5

3

1

Reports of high- risk activity that constitutes proliferation in trafficking were mostly concentrated throughout California, Florida and New York. There are some reports of trafficking throughout Colorado, Pennsylvania and Texas, as well as Kansas, Illinois and Oklahoma.

Geographic Distribution of Targeting the National Information Infrastructure Per Region

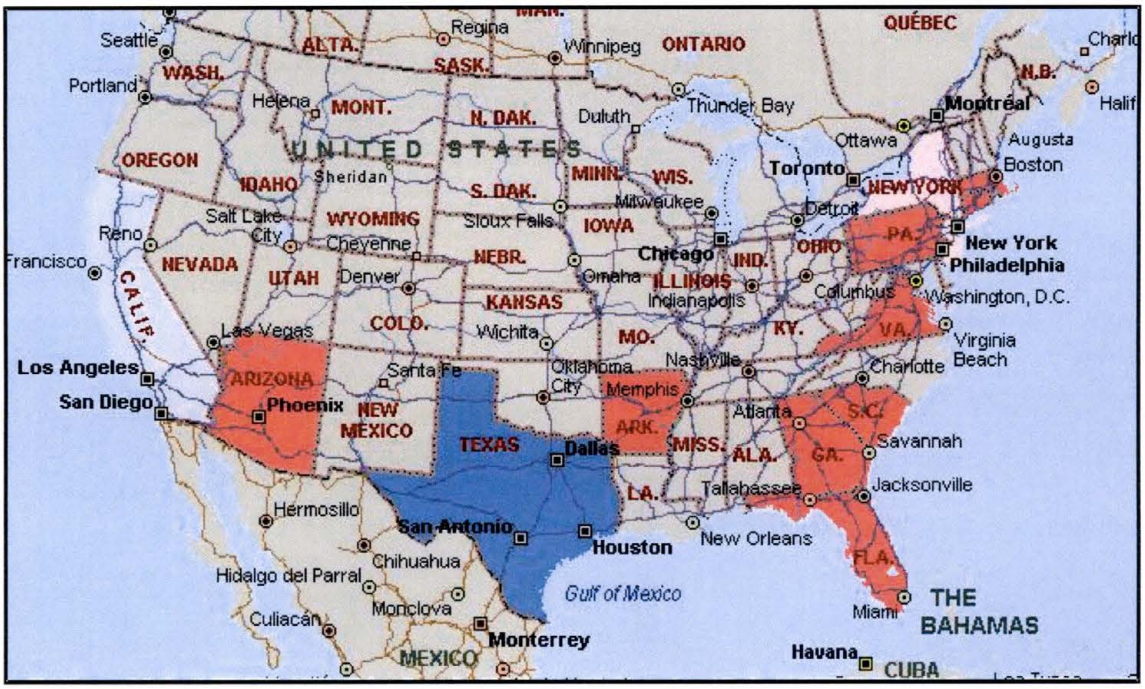
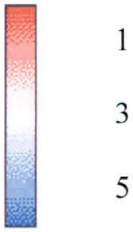


Figure 4.3 Targeting the National Information Infrastructure in the U.S.

Number of Incidences



Reports of high- risk activity that constitutes targeting the national information infrastructure were most common in Texas. There are some reports in Arizona, Arkansas, Florida, Pennsylvania, New Jersey and New York.

Geographic Distribution of Threat Categories

Figure 4.4 National Threats to the U.S. by R.O.C.

- Economic Espionage
- Proliferation in Trafficking
- Targeting the National Information Infrastructure

Overall *reports of all three high- risk activities were most common in California, Florida, New Jersey, New York, Pennsylvania and Texas*

CHAPTER 5

Conclusion and Discussion

Summary of Chapters

The first chapter of this paper gave insight to the threat of international crime groups, and briefly introduced the potential for ROC to cause a significant threat to national security within the U.S.

The second chapter gave an in depth history of ROC, as well as an examination of their activities within the U.S. A review of recent literature summarized the various activates Russian crime groups are domestically and internationally involved with, so as to give an understanding of the threat ROC poses in the U.S. The information in the literature review was be used as framework for this study. Finally, the chapter introduced a previous study that established variables to measure the risk of a crime group, and explained how these variables were used to evaluate ROC as a threat to national security. Chapter three outlined the method for analyzing original data to answer three research questions: (1) Do the activities of ROC groups fit within the pre-defined threat categories (proliferation, economic espionage, and targeting the information infrastructure) and pose a potential security threat to the U.S.?; (2) Are their activities specific to certain geographic areas? (3) If so, are there regions in the U.S. more prone to certain types of high risk activity that fit within the pre-defined threat categories?

Chapter Four provided findings and results that gave indication about the research questions. First of all, data show activities of ROC fit within the pre-defined threat categories (Proliferation, Economic Espionage, and Targeting the Information Infrastructure) and therefore poses a security threat to the U.S. Secondly, data proved that ROC activities are specific to certain geographic areas, and that certain regions in the U.S. are more prone to certain types of high risk activity that fit within the pre-defined threat categories. For instance, cybercrime is common in the south. Moreover, trafficking, fraud, and scams are prevalent in the south, west, and northeast.

Implication of Threat

When reconciling relevant literature with original data from this study, there appears to be a strong indication ROC is a threat to national security. Furthermore, it seems certain areas are more prone to high risk activity such as Texas, Florida, California, New York, New Jersey and Pennsylvania.

Recommendations

Based on the regional distribution of ROC found in this study, several tatical solutions and policy suggestions are particularly useful to examine. For instance, establishing more OCDETF units in regions heavily concentrated with proliferation in trafficking and economic espionage is a potential solution because the primary mission of OCDEFT units is to identify, disrupt, and dismantle the most serious drug trafficking and money laundering organizations (U.S. Drug Enfocement Administration, 2009). However, there should be agents trained to indentify and combat the high-risk activities of ROC groups. Overall, the data in this study show the Northeast and West as concentrated with high-risk activities of proliferation in trafficking and economic

espionage. Those regions should have more OCDETF units with agents trained to identify the activity and structure of ROC groups in their area. Additionally, tactical solutions should be aimed to address the enhanced professionalism of ROC groups. For example, there should be more undercover operations designed to target the legitimate and illegitimate activities of ROC groups. Agents would better understand how ROC groups are able to go undetected, and create better tactical solutions.

Aside from establishing more task forces with agents trained to identify and combat ROC, joint participation among agencies may be helpful. O'Neal (2000) suggests that law enforcement solicit increased participation of local, state, and foreign police agencies in the development of ROC profiles, joint investigations, and task forces. O'Neal explains that the wide variety and to some degree, unknown functions of different ROC groups makes it difficult for law enforcement to investigate without cooperation from other agencies. O'Neal (2000) also suggests money laundering and asses forfeiture laws to attack ROC at its economic source. However, targeting cyber crime remains an issue.

Attacks on the national information infrastructure may possibly be resolved by President Barack Obama's 2009 Cyberspace Policy Review. According to the executive summary the cyber security policy includes:

> Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence

> missions as they relate to the security and stability of the global information and communications infrastructure. (Cyberspace Policy Review, 2009 p. 5)

Data from this study reveals that ROC groups in Texas participate in a wide variety of cybercrime such as network and systems hacking for the purpose of gaining sensitive information. If passed, the 2009 Cyberspace Policy would be useful to monitor and combat attacks on the national information infrastructure from Russian crime groups.

Future Research

American foreign policy has shifted from dealing with Cold-War era threats to combating terrorism. Recently, however, there have been warnings about a new threat from a mix of terrorism and international organized crime transcending the nation-states. Shelley and Picarelli (2002) examine the relationship between terrorism and international organized crime, and conclude that the entities adopt similar methods but strive for divergent ends. Furthermore, they emphasize the importance of scholarly research in this area, and suggest "finding the root causes of organized crime and terrorism in order to tactically respond to the symptoms and outbreaks they generate" (Shelly & Picarelli, 2002, p. 317). This paper could be used to form conclusions about the parallels between terrorism and high-risk activities of international crime groups. Also, the threat-assessment variables could be used in future research as a method to evaluate high-risk activity of international crime groups and determine if they pose a security threat. Ultimately, the effect of ROC on the U.S. will depend upon establishing a comprehensive understanding of its capabilities among researchers and practitioners.

Appendix A

Preliminary Interviews

Interview 9/7/2008

ROC Involvement

3 Most Prevalent of Crime:

- Drugs
- Cars
- Human Trafficking

- Also involved in the exploitation of prostitutes & women

Conduct activities in pockets of the nation, such as:

- Sacramento
- Seattle
- San Diego
- Baltimore
- Phoenix
- Denver
- Pennsylvania
- New York
- New Jersey
- Vancouver, Canada

* "Wherever they can make money"

(perhaps a regional more so than a national threat)

Things to Remember

- There is a research gap between "the sky is falling and ROC or the Mafiya actually existing"
- If organized crime is indeed a threat, why is no one paying attention to it

Things to Look Up

- California DA Report (1996)
- 1990s: laws changed to either decrease or push out of state, not necessarily to eliminate
- April 2008: the need for focus of crime must be shifted from terrorism to organized crime
- FBI Inspector General's report on lack of focus on organized crime
- *Low Intensity Conflict & Law Enforcement* (1993/1994)
- Louis Free "ROC is a threat to national security" (1994-1996) & retraction of statement

Book Suggestions

1. *The Red Mafiya* – Friedman

2. *Godfather of Criminals*

Suggestions for Study

1. Define threats to national security

   - who, what, where, when, why

2. How does organized crime fit in?

- specifically ROC

Interview 10/10/2008

The Evolution of "Scam Blue"

Under the *Contraband Cigarette Trafficking Act,* ATF agent Edward DeRobertis busted an FBI informant for trafficking cigarettes from Virginia to Brighton Beach, New Jersey. The perpetrator informed DeRobertis of his involvement with the FBI, despite this information DeRobertis went forward with the arrest. As the perpetrator's involvement with the FBI as an informant was confirmed, ATF began to collaborate with the FBI & the New Jersey Racketeer Drug Force; in which the FBI was conducting a series of investigations concerning the illegal smuggling of alcohol from the United States to Russia.

Summary of "Scam Blue"

During the early/mid 1990's fewer people in the U.S. were drinking liquor; the choice of alcohol appeared to be wine. With Gorbachev having a monopoly on distilled spirits, American companies, such as the McCormick's Vodka industry took advantage of Russian's desire to consume vodka and went into business with the Russian government as a main distributor of vodka. Taking advantage of this situation paved the way to a number of profitable situations:

- providing of proceeds to the Russian Sports Federation ($ funded Olympic federation)
- vodka in beer cans (12 oz.)
- McCormick's attached a "Russian" tax stamp on all vodka sold in NJ

As profits grew high, the desire to find new and innovative ways to provide Russia with vodka sparked the interests of both Russians and McCormick's. At first McCormick's began to ship 50 gallon drums of vodka to Russia, labeled as ethanol solution (which ultimately voided either party of paying tax on the product). The scam later grew larger to include 300 gallon drums of denatured alcohol (which can not be consumed by humans) that would later be dissolved when citric acid was added on Russia's end.

* The name "Scam Blue" derived from the ability to add blue food coloring to the denatured alcohol as to pass for windshield washer fluid during transportation from U.S. to Russia.

Investigation

Primarily investigations had began under the form of reverse money laundering stings, in which the Russians would provide dirty money to the FBI in exchange for half the amount of clean money (Russians $1,000 dirty → FBI →$500 clean Russians). After the transportation of the 300 gallon drums was discovered, FBI subpoenaed McCormick's for their exportation records. Upon review, the FBI discovered that McCormick's had been involved in exporting millions of gallons of alcohol illegally to Russia. To avoid incarceration, McCormick's cooperated in the investigation to bring the perpetrators within the U.S.'s jurisdiction to justice.

Precedence

U.S. v. Tasquantino (wire & mail fraud statutes involving Canadians)

Terrorism v. Organized Crime

- Since the 1990's and the attack of 9/11 there has been no "legal independence" as far as investigations are concerned

- Post 9/11
    - both ATF & FBI were reassigned to combat possible terroristic attacks
- Beginning to swing back due to a rise in:
    - violent crime
    - murder
- focus needs to be on both O.C. & Terrorism

A Threat to National Security?

"Poses a huge threat…agencies need to work towards prevention"

- In the illegal trafficking of cigarettes alone, $50 billion dollars are lost annually.
- Adverse affect when govt. raises taxes & O.C. sales them cheaper
- "Certain aspects that O.C. is involved in that need to be stamped out"
- Canada loses $5 billion dollars a year

Interview 10/17/2008

ROC in America

- Is ROC a threat to the U.S?
- Yes, however, the threat is very subtle

Evolutionary White Collar Crime in the U.S.

- Insurance fraud
- Scams
- Money laundering
- Attack on economic sectors of the U.S.
- U.S. target of banking institutions (lack of security)
- Computers/Electronic hacking (key issue)

*ROC does not necessarily require big "families"- structure is linear

Recent Russia-Georgia Conflict

- Effect on ROC?

  -more on national security than organized crime

- Recent Project: U.S. Law Enforcement & Russian Law Enforcement on combating ROC

Research Suggestions

- "Durboot": Arms Trafficking
- Use specific cases, look internationally as opposed to only within the U.S.
- Look at the threat of our troops in other nations during wartime

  -any threats posed by former Soviet Union

Interview 10/20/2008

Beginning of Mission: 1990s

- Stolen automobiles transferred to Soviet Union
- Perpetrators asked if Customs Agents if they were interested in weapons
- Presented Agents with Armamex catalog (from former Soviet Union)
- Purchased Stinger missiles (7)

  -met with London undercover

  -were pegged as agents

  -Agents were able to talk their way through the situation, and remain undercover
- Armamex- now the Bulgaria Missile Co.
- St. Petersburg Russia Co.

  -new KGB

Negotiations

- 2 'mafiosos'

  -Bulgarian Armamex

  -Name changes are due to organized crime filter
- Tried a "legal" govt. to govt. trade
- Certificate from Lithuania
- Negotiated to go through San Antonio

  -Our govt. was concerned about the transfer

  -Money trouble: National Security, Department of Justice, CIA

During Case

- Perpetrators offered agents a nuclear device
- Washington called all govt. agents: NSA, DOJ, FBI, & CIA

  -Special Agent in Charge: Raymond Kerr
- FBI provided Russian interpreters

Things to Remember

- A lot has changed since 9/11, the govt. has different agendas
- ROC is ABSOLUTELY a threat to national security
- U.S. major players (Soviet Block)

  -Carlos Kardon (govt. officials)
- Missile transaction in 80s

  -China

  -Chechnya

  -Poland

  -Hungary

  -Iraq

Interview 10/25/2008

ROC and Threats to National Security

- If so, how great of a threat-Feds do not agree
- **Conjecture on ROC- Threat to U.S. National Security 'Three Fold'**
  1.) Abstract- malign influence on Russia, encourages tension between U.S. & Russia
  2.) ROC on U.S. soil: is somewhat undetectable, due to the fact that ROC operates on an underground level
  3.) Byproduct of experienced entrepreneurialism; Russians will make deals with anyone, even dangerous terrorists.
  -Makes terrorism that much more of a threat to national security

Chechens

- Interesting cases: people want to work with the Chechens because of their reputation
- Chechens are the toughest
- Chechens always 'stick to their word', in any event, they get the 'job' done
- Most people who have worked with the Chechens report that they are 'worthwhile' to work with

ROC

- Incredibly post modern/anamorphous
- No specific "families"
- Indirect floor cell gangs that come together when there is an opportunity

- Variety bunch: think of a heist movie, such as Oceans 11; everyone has a specific talent
- Hate Chechens because of the rivalry, however, continue to do business with them

-Chechens pose a threat to power in Russia

International ROC

- Entrepreneurialism
- Russia is a safe haven for people involved in global organized crime

-The Russian banking system is corrupt

-Good home for laundered money

-Having Russia as a 'home base' is key

Specific Activities that Pose National Security Threat

- Money Laundering: embezzled money

-Bank of NY

-Hawlla Banking System

-Used by terrorist organization to move money

-Some have resorted to organized crime

-Key challenge to fight terrorism is to cut their money supplies

-Russians are at the forefront of aiding Al Qaeda more money

-At this point: Organized crime and Terrorism intersect

-Where terrorism fails, organized crime compensates

- Arms Trafficking

-Africa and Latin America, affects guerilla groups because the weapons ROC provides, they have since become more effective

-Durboot: Arms dealer arrested in Thiland; contributed to a dozen militants

Russia-Georgia Conflict\

- Georgians will remain low key in conflict
- Russia is not a good law enforcement partner, and will continue to get worse: due to Russian Policy

  -Makes combating ROC more difficult

  -U.K. v. Russia: Chemical poison in London
- 1996- 1997: Good Russian law enforcement

  -Then: any visa apps with criminal records were tagged

  -Present Day: not as stringently enforced

  -Becoming easier to ship illegal goods out of Mexico

Advice for Project

- Contact Louise Shelley
- Contact Sally Stocker: Human Trafficking
- Contact Phil Williams

  -@ Pittsburg: has security angle

  -researched in 1990s
- Contact Roy Gottdson

  -@Georgetown

  -Has political-criminal nexus

  -Has security angle

Where Research is Lacking

- Most research has investigated ROC from a high perspective: need to look at the nuts and bolts of specific cases
- Russians & other transnational organized crime: how do the two intersect
- Look at micro-level research to build macro-level cases
- Look at the underworld: specific dealings, persons, cases, etc.

Appendix B

Copy of Interview

- What types of activities are linked to ROC groups in your region?
- What is the structure of ROC groups in your region?
- Does your agency experience any barriers when utilizing combative efforts against ROC? If so, please describe
- Please describe the effect of ROC on the communities in your region?
- Do you perceive ROC as a threat to the national security, if so, please explain how?

Appendix C

Coded Interviews

FBI Agent: OC Task Force

Florida

Region: South

Division: South Atlantic

Types of Activities Linked to Russians: Russian enterprises are into fraudulent insurance and financial schemes. For example, they pull off phishing schemes. They attack the financial stability of residents, sending notification of terminated accounts, which request re-registration thru their "institution".

- Coded as: Economic Espionage

Structure of Organization in Region: Does not follow hierarchical structure at all, very loose networks, scattered through southern region of Florida, especially in Miami.

- Coded as: Highly Decentralized

Barriers to Combative Efforts: Law enforcement are unable to locate the networks sending out fraudulent notification of terminated accounts, so they can't stop them. Human trafficking is a big problem, and combative efforts are usually obsolete. "There are few individuals we are able to link to trafficking rings. Participants involved in these rings are usually overseas, and far from our jurisdictional reach."

Effect on Community: Retiring population is especially vulnerable to phishing schemes.

Coded as: Semi-threat to Community

Effect on Nation (National Threat): "Overall, Eurasians are a threat because of their sophistication. The FBI considers Russians as a top priority when targeting organized crime in the state of Florida."

- Coded as: Semi-Threat to the Nation

U.S. Attorney's Office- OCDETF

California

Region: West

Division: Pacific

Types of Activities Linked to Russians: "There are a lot of ROC groups involved in fraud, especially mortgage and healthcare fraud. Also, we have recently uncovered trafficking rings that are linked to Russian crime groups."

The immigration factor contributes to crime overall in the Pacific region, but Russians have always settled in Florida and not California. Recently, however, they have seen an influx of Russian immigrants, coming from the Northwest region (Oregon & Washington).

- Coded as: Economic Espionage and Proliferation in Trafficking

Structure of Organization: There is no structure. "Russians will work with anyone. Lately they have been working with Asian and Mexican crime groups that are already a problem here in California".

- Coded as: Highly Decentralized

Barriers to Combative Efforts: Language is a barrier. They don't have many people who speak Russian, because the primary population is either Asian or Hispanic.

"Collaborative efforts between agencies are difficult because there are a lot of jurisdictional issues in California."

"ROC groups have no geographical anchor, it makes their activities hard to detect"

Effect on Community

Asian crime groups have the biggest effect on the community, they actually give their community what they can't get. Russians are there to defraud, but have a minimal effect on the immediate community. However, their schemes show potential to harm specific regions of California, especially where there is big business.

- Coded as: Semi-Threat to Community

Effect on National Security

"ROC groups pose a threat to national security because they're home base is overseas. They have international relationships, making it easier to commit large scale crimes such as white-collar schemes, drug trafficking and misappropriation of federal funds- the crimes that cause the most economic damage in the U.S."

- Coded as: Significant Threat to Nation

ATF Agent

Colorado

Region: West

Division: Mountains

Types of Activities Linked to Russians: Eurasians are involved in weapons trafficking, but more heavily in drug trafficking. They are also into counterfeiting jewels.

"There are a lot of store fronts here, and the Eurasians are heavily involved in money laundering through the fronts."

Identification fraud is becoming popular among all OC groups

- Coded as: Economic Espionage and Proliferation in Trafficking

Structure of Organization in Regions: Small groups of criminals, as well as individual actors working together

- Coded as: Small Networks

Barriers to Combative Efforts: Jurisdictional issues between state and local law enforcement, the flow of information is top down…when it'd be more effective the other way.

Effect on Community : "They keep to themselves, unless they are involved in business ventures"

- Coded as: Semi-Threat to Community

Effect on Nation: "Eurasians aren't worried about the quantity of jobs they are involved in, they seem to be involved in operations that require the most skill and can make them the most money."

- Coded as: Semi-Threat to Nation

FBI Agent: OC Task Force

New Jersey

Region: Northeast

Division: Middle Atlantic

Type of Activities Linked to Russians: "ROC groups are much more sophisticated than other crime groups here. In the Tri-State area, they are heavily involved with insurance fraud, medical fraud and banking fraud. They are also into stock market manipulation. Russians are billionaires because they are able to blend legitimate and illegitimate activities."

Recently, they have become heavily involved in cyber crime and fuel scams.

- Coded as: Economic Espionage and Targeting the National Information Infrastructure

Structure of Organization in Region: "In New York and New Jersey, ROC used to follow a structural pattern- but now, it's a bunch of different guys from a variety of ethnic backgrounds- specifically, Ukrainians, Uzbekistani, Armenians, and Russians. Now there is no structure".

They operate transnationally and are very mobile

- Coded as: Highly Decentralized

Barriers to Combative Efforts: "Russians aren't afraid of prosecution, they also know they are more sophisticated than other crime groups. It takes a lot of man power, 12-13 squads, to manage their activities. What presents more of a problem is the lack of

resources since 9/11. Criminal enterprises have really been able to thrive since then, especially in white-collar crime."

RICO isn't applicable to their type of operation (due to lack of structure)

Effect on Community: Russian crime groups are violent in the tri-state region. Murder, extortion and arson are common methods to get victims to cooperate.

- Coded as: Significant Threat to Community

Effect on Nation (National Security): "Any criminal organization that can operate like an enterprise poses a security threat. We caught some Armenians who wanted to sell missiles!"

- Coded as: Significant Threat to Nation

U.S. Attorney's Office- OCDETF

Maryland

Region: South

Division: South Atlantic

Type of Activities Linked to Russians: ROC groups are heavily involved in drug trafficking, especially cocaine. They are also involved in weapon trafficking, specifically from the stockpile of weapons from the Cold war.

"Human trafficking is the biggest market for Russians in this region, it's easy for them to bring immigrants here and force them into a vulnerable situation."

- Coded as: Proliferation in Trafficking

Structure of Organization in Region: There are some large networks, but most Russians operate individually or in small groups.

- Coded as: Small Networks

Barriers to Combative Efforts: Interagency cooperation is the method, but it's difficult to get the agencies on the same page with information about ROC.

Effect on Community

Larger networks of Russian crime groups are violent, and frequently use murder and arson as to intimidate local businesses.

- Coded as: Significant Threat to Community

Effect on Nation (National Security): "ROC is embedded in the U.S. underworld, they will deal with anyone, even terrorists."

Coded as: Significant Threat to Nation

FBI Agent- OC Task Force

Texas

Region: South

Division: West South Central

Type of Activities Linked to Russians: Lots of cyber crime!

"Russians are extremely skilled with hacking. With advanced tools at their disposal, they can hack into any website. Mainly, they are interested in are banking and ecommerce websites."

Other crime groups are associated with more traditional organized crime, drug trafficking and money laundering. Some Russian crime groups are involved in arms trafficking, as well as human trafficking.

- Coded as: Cyber Crime, Proliferation in Trafficking and Economic Espionage

Structure of Organization in Region: Mostly small groups of people, with connections overseas

- Coded as: Highly Decentralized

Barriers to Combative Efforts: "The activities Russians are involved in are different than other crime groups, especially the computer hacking. It's difficult to pinpoint exactly where the source of the hacking comes from. Sometimes other hackers will hire the Russians to extort companies."

Effect on Community: It's mainly the Mexican Mafia that has an effect on this region, they traffic drugs and are violent. However, there have been murders and human trafficking rings linked to Russian crime groups in the Houston and San Antonio area.

- Coded as: Significant Threat to Community

Effect on Nation (National Security): "Russian crime groups are involved in so many different scams, and their international reach is what is threatening to the U.S." Hacking poses a substantial security threat in the U.S., especially with the downturn of the economy.

- Coded as: Significant Threat to Nation

FBI Agent: OC Task Force

Washington

Region: West

Division: Pacific

Type of Activities Linked to Russians: "A lot of trafficking…weapons, humans and drugs- all coming from California."

Also, credit card fraud, health insurance fraud, and identity fraud is becoming popular among ROC groups in this region. They conduct schemes in the U.S., and overseas.

- Coded as: Proliferation in Trafficking and Economic Espionage

Structure of Organization in Regions: It's not structured- individuals or small groups of criminals, forming loose networks.

- Coded as: Small Networks

Barriers to Combative Efforts: "Russian crime groups are mobile, they are constantly pushing goods and services between here and California. It takes a lot of inter-agency/inter-jurisdictional cooperation to keep up with their activities. Also, I mentioned earlier that they are into a variety of different fraudulent schemes, here and overseas…that's because Russians have associates all over the place. It's hard to contain their activities when they have so many people working with them."

Effect on Community: Sometimes effects local businesses, and residents if Russian crime groups get involved in store fronts- murders and arson occurs. Most of the time, Russians are more interested in more sophisticated types of fraud and schemes.

- Coded as: Semi Threat to Community

Effect on Nation (National Security): The threat of ROC is becoming more profound, due to the poor condition of the economy.

"Russians have the ability to work with anyone—businessmen, criminals, and even terrorists. That's why they are so successful at pulling off articulate scams, and cause damage to the economy."

- Coded as: Significant Threat to Nation

U.S. Attorney's Office (OCDETF)

Illinois

Region: Midwest

Division: East North Central

Types of Activities Linked to Russians: Tobacco smuggling, and some human trafficking. Very few Russian crime groups here, but most are violent.

- Coded as: Proliferation in Trafficking

Structure of Organization: "There really isn't an organization. Usually, if there is a case involving Russian criminals, it's a small group of people, or one person."

- Coded as: Small Networks

Barriers to Combative Efforts: They have to work with other jurisdictions, because the tobacco is trafficked from Illinois to the Northeast region.

Effect on Community: The violent criminals pose somewhat of a threat to local residents. There have been a few murders linked to Russian crime groups.

- Coded as: Semi Threat to Community

Effect on Nation (National Security): Poses a huge threat…agencies need to work towards prevention, illegal trafficking of cigarettes alone, $50 billion dollars are lost annually. Adverse affect when govt. raises taxes & O.C. sales them cheaper

- Coded as: Significant Threat to Nation

Federal Bureau of Investigations (O.C. Task Force)

Michigan

Region: Midwest

Division: East North Central

Types of Activities Linked to Russians: ROC groups are into a variety of different scams: health insurance, credit card, fuel and scams

Human trafficking (labor & prostitution) is common

- Coded as: Economic Espionage and Proliferation in Trafficking

Structure of Organization in Region: It's not structured like the other crime groups (Italian and Mexican Mafia). The Russians act in small groups, and rarely work with the same people.

- Coded as: Small Networks

Barriers to Combative Efforts: "Russian crime groups come together to pull off a scam, then part ways. Investigation is tedious, and it takes a lot of time to make a case."

Effect on Community: The other crime groups (Italian, Mexican Mafia, and Columbian Cartels) have more of an effect on the community because they are larger in number in this region.

- Coded as: No Threat to Community

Effect on Nation (National Threat): ROC is a national threat due to the variety of scams and fraud they successfully commit. They are attacking the economic structure of the U.S. in many different ways, many times undetected by law enforcement.

- Coded as: Significant Threat to Nation

U.S. Attorney's Office- OCDETF

Pennsylvania

Region: North East

Division: Middle Atlantic

Types of Activities Linked to Russians: "ROC groups smuggle a lot of tobacco, in and out of the Tri-State region. It comes from the Midwest. They also are involved in fuel scams, money laundering and stock market manipulation."

Cyber crime is becoming a problem

Trafficking in arms is commonly linked to Russian crime groups

- Coded as: Proliferation in Trafficking, Economic Espionage and Targeting the National Information Infrastructure

Structure of Organization in Region: There are some large ROC groups that work together, as well as small networks that are internationally mobile.

- Coded as: Large Networks and Small Networks

Barriers to Combative Efforts: "ROC groups are constantly traveling, within the Northeast and overseas. They have international connections…it's a business now. It takes a lot of time and effort to determine their whereabouts."

Effect on Community: Russian crime groups are known for using violence to extort businesses and individuals. Kidnapping, arson and murder are commonly linked to ROC groups in this region.

- Coded as: Significant Threat to Community

Effect on Nation (National Threat): "Russians are very successful in this region. They have underground connections, as well as business connections. They have the ability to compromise enforcement in the U.S., which is something I would consider a security threat."

- Coded as: Significant Threat to Nation

Appendix D

Sources for News Articles

Abel, D. (2005, May 10). ATM cards pirated for plenty, police say. The Boston Globe. Retrieved from http://www.boston.com/news/

Applebaum, A. (2006, December 9). Old KGB lives on in new guises. The Washington Post. Retrieved from http://www.deseretnews.com/

Anastasia, G. (2002, May 7). No bail for alleged Russian mob head. Philadelphia Inquirer. Retrieved from http://nl.newsbank.com/

Anonymous. Bucks man is accused of extortion. (2002, Feburary 2). Philadelphia Inquirer.

Anonymous. Fake websites work of mafia. (2003, July 4). TVNZ. Retrieved from http://tvnz.co.nz/

Anonymous. Last act for the great circus smuggling scheme. (2007, February 5). ABC News. Retrieved from http://blogs.abcnews.com/

Anonymous. Official reactions to newspaper's illegal arms trading allegations. (2005, October 22). BBC News Online. Retrieved from http://www.highbeam.com/

Anonymous. Russian mafia might have ties in the valley. (2005, March 18). Daily News. Retrieved from http://nl.newsbank.com/

Anonymous. Russian mafia internet fraud. (2006, June 27). Computer Crime Research Center. Retrieved from http://www.crime-research.org/news/

Anonymous. Russia Mafia Questioned As church mourns murdered Abbot. (2005, July 31). BosNewsLife. Retrieved from http://www.bosnewslife.com/

Anonymous. Twin businessmen targeted in murder attempt. (2006, March 29). Kyiv Post. Retrieved from http://www.kyivpost.com/

Anderson, J. (2003, May 20). Russian mafia links alleged in fishing industry. Australian Business Intelligence. Retrieved from http://www.sharechat.co.nz/

Baranikas, I. (2003, May 21). The interests of the Russian mafia in the U.S. range from the dating industry to ATM cards. Moscow News. http://www.cdi.org/

Barnes, G. (2004, August 8). Crusader confronts a world of trouble. Fayatteville Observer. Retrieved from http://nl.newsbank.com/

Berkeley, R. (2002, August 19). Code of betrayal, not silence, shines light on Russian mob. The New York Times. http://www.nytimes.com/

Berkeley, B. (2002, August 19). Russian mob's Achilles' heel has been its easy turncoats. Pittsburg Gazette Post. Retrieved from http://news.google.com/newspapers

Blakley, R. (2006, January 18). Hackers hijack homepage. Times Online. Retrieved from http://business.timesonline.co.uk/

Birch, D. (2008, January 26). Suspected crime lord arrested in Moscow. Fox News. http://www.foxnews.com/

Brachear, M. (2002, June 27). Officials alert colleges to ID theft crimes Linked to Russian mafia. The Dallas Morning News. Retrieved from http://www.accessmylibrary.com/

Brick, M. (2006, April 13). 14 years kater, 2 killings Are linked to Russian mob. The New York Times. Retrieved from http://query.nytimes.com/

Brick, M. (2006, July 12). In gas scheme, regular was Sold as premium, prosecutors say. The New York Times. Retrieved from http://query.nytimes.com/

Burkman, O. (2002, August 1). 'Russian mafia kingpin' accused of fixing Olympic skating results. The Gaurdian. Retrieved from http://www.guardian.co.uk/

Chesterton, M. (2006, May 23). Ethical hacking. Radio Netherlands. Retrieved from http://static.rnw.nl/migratie/www.radionetherlands.nl/

Chivers, C. (2004, November 3). Russian gal's seeking comrade an internet scam. The New York Times. http://www.chinadaily.com.cn/

Chu, K. (2004, January 12). Car insurance premiums pushed up by rising fraud organized crime rings getting bigger, bolder, regulators say. The Baltimore Sun. Retrieved from http://www.baltimoresun.com/

Church, L. (2009, July 9). Church gets share of forfeiture. Livingston Daily. Retrieved from http://www.livingstondaily.com/

Cortez, D. (2004, March 17). Man is suspected of ties to Russian mafia. Fort Wayne News Sentinel. Retrieved from http://nl.newsbank.com/

Delacy, T. (2002, March 20). Searchers find fourth body. The Modesto Bee. Retrieved from http://nl.newsbank.com/

Denver inherits global curse. (2005, October 29). Rocky Mountain News. Retrieved from http://nl.newsbank.com/

Diaz, R. (2004, April 14). FBI arrests college official in money-laundering sting. Community College Week. Retrieved from http://www.accessmylibrary.com/

Ellis, M. (2005, June 21). Cops raid Russian mafia ring. The Independent. http://www.highbeam.com/

Elliot, H. (2002, August 11). Harried by the mob?. Los Angeles Times. Retrieved from http://pqasb.pqarchiver.com/latimes/access/

Fendrich, H. (2007, August 27). Davydenko to talk to investigators. The Associated Press. Retrieved from http://www.washingtonpost.com/

Finn, P. (2006, November 26). Probe traces global reach of counterfeiting ring. The Washington Post. Retrieved from http://www.washingtonpost.com/

Finz, S. (2002, March 20). Russian mafia link to bodies in reservoir. San Francisco Chronicle. Retrieved from http://www.sfgate.com/

Fisk, K. (2005, March 30) $28 million forgery ring, smashed. Daily News. Retrieved from http://nl.newsbank.com/

Foster, A. (2002, June 20). Russian mafia may have infiltrated computers at Arizona State and other colleges. The Chronicle of Higher Education. Retrieved from http://chronicle.com/

Gendar, A. (2008, January 21). Bomb-making factory found in Brooklyn apartment of Columbia professor. Daily News. Retrieved from http://www.nydailynews.com/

Getlin, J. (2005, March 16). 18 Charged in plan to smuggle arms into U.S. Los Angeles Times. Retrieved from http://pqasb.pqarchiver.com/latimes/access/

Goodin, D. (2007, June 20). YouTube 'riddled with 40-plus security vulnerabilities'. The Register. Retrieved from http://www.theregister.co.uk/

Grondin, K. (2004, April 7). Computer sleuths take on would-be saboteurs cyber security. Daily Herald. Retrieved from http://nl.newsbank.com/

Harding, L. (2008, January 26). Russians arrest alleged mafia boss by accident. The Guardian. Retrieved from http://www.guardian.co.uk/

Hayward, S. (2003, August 3). Russians co-opt Mexican drug rings, mob takes advantage of arrests, deaths to take bigger role in smuggling. The Charlotte Observer. Retrieved from http://nl.newsbank.com/

Healy, P. (2003, August 13). Investigators Say fraud ring staged thousands of crashes. The New York Times. Retrieved from http://www.nytimes.com/

Herbeck, D. (2004, November 22). Russian criminals active locally. The Buffalo News. Retrieved from http://nl.newsbank.com/

Hersh, P. (2002, July 31). Fix allegedly in as Olympics Russian mafia boss is arrested. Chicago Tribune. Retrieved from http://www.accessmylibrary.com/

Hines, N. (2008, January 25). Semyon Mogilevich, the 'East European mafia boss', captured in Moscow. Times Online. Retrieved from http://www.timesonline.co.uk/

Howlett, K. (2002, February 1). Russian organized crime boss helped launch YBM Magnex. Globe & Mail. Retrieved from http://www.theglobeandmail.com/

Hirschkorn, P. (2005, March 15). U.S. charges 18 in Russian weapons-smuggling plot. CNN.com. Retrieved from http://www.cnn.com/

Kane, F. (2007, October 20). How we survived mafia and banking meltdown. The Observer. http://www.guardian.co.uk/business/

Kelley, M. (2002, October 20) Russian mafia thieves climb into Bill Gates' window. Daily Record. Retrieved from http://www.highbeam.com/

Kirby, C. (2005, May 11). Phishing is big business. San Francisco Chronicle. Retrieved from http://www.sfgate.com/

Kirk, P. (2003, November 20). FBI and Hungarian police arrest leading Russian mafia. AP World Stream. Retrieved from http://www.highbeam.com/

Kline, K. (2008, September 27). Entertainment or exploitation. Chicago Sun Times. Retrieved from http://nl.newsbank.com/

Jesdunun, A. (2004, April 2). Web 'phishing' scams targeted. CBS News. Retrieved from http://guilfoyle.net/

Lashmar, P. (2002, August 2). Police join the FBI in Money laundering investigation. The Independent. http://www.independent.co.uk/

Lee, H. (2008, Feburary 20). Hans Rieser trial. San Francisco Chronicle. Retrieved from http://www.sfgate.com/

Land, T. (2003, May 5) Islamic terrorists and the Russian mafia. Contemporary Review. Retrieved from http://www.accessmylibrary.com/

Landesman, P. (2003, August 17). Arms and the man. New York Times. http://www.nytimes.com/

Lettice, J. (2003, June 20) MS hacked!. The Register. http://www.theregister.co.uk/

Leovy, J. (2007, January 16). Emigres' murder case goes to jury; Organized crime and money laundering are linked to a kidnapping scheme that left five dead, prosecutors say. Los Angeles Times. Retrieved from http://pqasb.pqarchiver.com/latimes/

Lorek, L. (2002, February 2). San Antonio, Texas, firm works to help keep hackers out of U.S. computers. San Antonio Express News. Retrieved from http://www.accessmylibrary.com/

Leyden, J. (2008, October 16). Scammers making $15 million a month on fake anti-virus. The Register. Retrieved from http://www.theregister.co.uk/

Leyden, J. (2007, October 11). U.S. regional bank hacked. The Register. Retrieved from http://www.theregister.co.uk/

Maddox, M. (2004, May 6). Mob retains strong N.J. presence, report says. The Record. Retrieved from http://www.highbeam.com/doc/1P1-94309537.html

Martindale, M. (2008, July 8) Two downriver brothers plead no contest in extortion case. The Detroit News. Retrieved from http://nl.newsbank.com/

Mendieta, A. (2003, October 12). Feds, cops shut social club, alleging ties to Russian mob. Chicago Sun Times. http://nl.newsbank.com/

Milton, P. (2008, June 4). Mob take down by feds. CBS News. Retrieved from http://www.cbsnews.com/

Modern day slavery. (2006, June 15). Daily Herald. Retrieved from http://nl.newsbank.com/

Morse, R. (2005, February 27). Feds investigate odometer rollback scam. The Washington Post. http://www.washingtonpost.com/

Nakaishima, R. (2007, January 26). Hack, pump and dump. Washington Post. Retrieved from http://www.washingtonpost.com/

Naraine, R. (2006, April 16). Cybercrime more widespread, skillful, dangerous than ever. Fox News. Retrieved from http://www.foxnews.com/

Nineteen charged with conspiracy, drug trafficking, gun violations, money laundering. (2006, June 30). US Fed News Service. Retrieved from http://www.fnsg.com/archive

O'Brien, T. (2004, January 10). Banker linked to jailed Russian fighting to stay in U.S. The New York Times. http://www.nytimes.com/

Olsen, L. (2008, November 24). Trafficking victims in visa limbo. Houston Chronicle. Retrieved from http://www.chron.com/CDA/archives/

Paton, J. (2008, May 23). Aurora man, 53, pleads guilty in counterfeit money operation. Rocky Mountain News. Retrieved from http://www.rockymountainnews.com/

Paton, J. (2007, December 19). Funny money operation has link to Denver. Rocky Mountain News. Retrieved from http://www.rockymountainnews.com/

Preston, J. (2005, March 16). Arms network is broken up, officials say. The New York Times. Retrieved from http://query.nytimes.com/

Probert, R. (2002, July 27). Ex spy boss jailed for dollars scam. http://business.timesonline.co.uk/

Rankin, B. (2009, April 2). Singer, producer get prison for identity theft. The Atlanta Journal. Retrieved from http://www.ajc.com/

Ritter, K. (2003, March 11). Jury hears magician's plea for money paid 'Russian mafia'. Associated Press. Retrieved from http://www.highbeam.com/

Ruquet, M. (2003, October 27). New York organized crime arrests rein in auto insurance fraud rings. National Underwriter Property & Casualty-Risk & Benefits Management. Retrieved from http://www.highbeam.com/

Scarborough, R. (2008, August 2). Russian mob plotted attack on Shelton. The Washington Times. Retrieved from http://goliath.ecnext.com/

Scherer, R. (2005, March 16). Arms smuggling sting shows need for vigilance. The Christian Science Monitor. Retrieved from http://www.csmonitor.com/

Schmitt, R. (2008, April 28). AG targets a new type of mobster. The Los Angeles Times. Retrieved from http://www.policeone.com/

Shulas, G. (2004, February 26). Internet scam may be linked to Russian organized crime. Connecticut Post. Retrieved from http://nl.newsbank.com/

Silvester, J. (2004, August 16). Top gangsters targeted on police inquiry list. The Age. Retrieved from http://www.theage.com.au/

Smeler, P. (2002, June 21). The Washington Times. U.S. fugitive rich linked to money laundering. Retrieved from http://www.highbeam.com/

Swartz, J. (2004, October 20). Crooks slither into net's shady nooks and crannies. USA Today. Retrieved from http://www.usatoday.com/

Swift, E. (2002, August 12). An alleged fix at salt lake is the latest link between organized crime and russian athletes. CNN News. Retrieved from http://vault.sportsillustrated.cnn.com/

Tagliabue, J. (2002, June 13). 50 held in European offshoot of bank of New York investigation. The New York Times. http://www.nytimes.com/

Tompson, T. (2002, March 21). Russian mafia targets city. The Observer. http://www.guardian.co.uk/

Townsend, I. (2005, March 1). Police investigate extortion attempt on construction company. The World Today. Retrieved from http://www.abc.net.au/

Tsuruoka, D. (2004, December 21). Net holds attraction for criminal groups; route to cash, secrets. Investors Business Daily. Retrieved from http://www.investors.com/NewsAndAnalysis/

Walsh, P. (2002, June 16). 9 billion dollar money laundering ring broken. The Observer. http://www.guardian.co.uk/

Wartenburg, S. (2009, March 8). Credit-card criminals often strike from afar. The Columbus Dispatch. Retrieved from http://www.columbusdispatch.com/

Wells, T. (2004, June 20). IRA linked to dollar scam. Sunday Mercury. Retrieved from http://www.highbeam.com/

Weinstien, H. (2002, October 31). Tobacco firm colludes with underworld, lawsuit says. San Francisco Chronicle. Retrieved from http://www.sfgate.com/

Welter, G. (2006, April 18). Chico Enterprise Record. Woman allegedly victimized in russian mafia scam. Retrieved from http://nl.newsbank.com/

Whitfeld, F. (2005, July 19). KKK member on trial, 40 Million vulnerable in recent breech of processing company, two unlikely leaders at the U.S. open. CNN News. Retrieved from http://transcripts.cnn.com/TRANSCRIPTS/

Valencia, M. (2008, November 26). Sandwich loses nearly $50k to hacker. The Boston Globe. Retrieved from http://www.boston.com/

Vincent, M. (2005, March 1). Police investigate multiplex extortion attempt. The World Today. Retrieved from http://www.abc.net.au/

Ulin, D. (2002, February 22). A force for good killing fields. LA Times. Retrieved from http://pqasb.pqarchiver.com/

REFERENCES

Albanese, J.S. (1989). *Organized crime in America.* Cincinnati, OH.

Albanese, J.S. (2000). The causes of organized crime: Do criminals organize around opportunities for crime or do criminal opportunities create new offenders? *Journal of Contemporary Criminal Justice*, 16, 409-423.

Albini, J.L., Rogers, R.E., Shabalin, V. (1995). ROC: It's history, structure and function. *Journal of Contemporary Justice. 11, 4,* 213-245.

Carreon, J.R. (2009). An examination of organized crime as a threat to U.S. national security. Unpublished master's thesis, Texas State University, San Marcos, Texas, United States.

Centre for Comparative Criminology & Criminal Justice. (2001). *Russian organized crime and the Baltic states: Assessing the threat.* (Issue Brief No. 1468-4152). Falmer, Brighton: Paddy Rawlinson.

Center for Strategic and International Studies. (1998, March). *Russian organized crime.* Washington D.C.: William H. Webster.

Cyberspace Policy Review (2009). Retrieved from http://www.infoworld.com/d/security-central/obamas-dreamy-plan-cyber-security-290?page=0,0

Department of Homeland Security. (2008). *Homeland security advisory system.* Retrieved May 15, 2008, from http://www.dhs.gov/xinfoshare/programs/Copy_of_press_release_0046.shtm

Federal Bureau of Investigation. (2008, August). *National security threat list.* Retrieved May 15, 2008, from http://www.ntc.doe.gov/cita/CI_Awarness_Guide/T1threat/Nstl.html <http://www.ntc.doe.gov/cita/CI_Awarness_Guide/T1threat/Nstl.html

Finckenauer, J.O. (2004, July). The Russian "Mafia". *Society Abroad*, 61-64.

Finckenauer, J.O. & Waring, E.J. (2001). *The Russian Mafia in America: Immigration, Culture, and Crime.* Boston, MA: North Eastern University Press.

Fickenauer, J.O. & Voronin, Y.A. (2001). The threat of Russian organized crime. *Issues in International Crime,* 1-33.

Friedman, R. (2000). *Red Mafiya.* Boston, MA: Little, Brown & Company.

Frisby, T. (1998). The rise of organised crime in Russia: Its roots and social significance. *Europe-Asia Studies*, 50, 27-49.

Galeotti, M. (2002). *Russian & Post- Soviet Organized Crime.* Aldershot, England: Ashgate Publishing Company.

Galeotti, M. (2005). The Russian 'mafiya': Consolidation and globalisation. In Galeotti, M. (Ed.), Global crime today: The changing face of organised crime (pp. 54-69). New York, NY: Routledge Taylor & Francis Group.

Handleman, S. (1995). *Comrade criminal: Russia's new mafiya.* Binghamton, NY: Vail-Ballon Press.

Hagan, F. (1997). *Research Methods in Criminal Justice & Criminology.* Needham Heights, MA: Allyn & Bacon Inc.

Leitzel, J., Gaddy, C., Alexeev, M. (1995). Mafiosi and matrioshki: Organized crime and Russian reform. *The Brookings Review,* 13, 26-29.

Lorek, L. (2001). Russian Mafia Net Threat. *Newsfront.* Retrieved March, 18, 2008 from http://www.zdnetasia.com/news/business/0,39044229,30089685,00.htm

Mays, N. & Pope, C. (1995). Rigour and qualitative research. *British Medical Journal,* 311, 109-112.

Mcillwain, J.S. (1999). Organized crime: A social network approach. *Crime, Law & Social Change*, 32, 301-323.

O'Neal, S. (2000, May). Russian Organized Crime: A criminal hydra. *FBI Law Enforcement Bulletin*, 69, 1-5.

Pickering, S. (2007). Transnational crime and refugee protection. *Social Justice*, 34, 47-61.

Rawlinson, P. (1998). Mafia, media, and myth: Representations of Russian organised crime. *The Howard Journal*, 37, 346-358.

Schwartz, C.A. (1979). Corruption and political development in the U.S.S.R. *Comparative Politics,* 11, 424-443.

Serio, J.D. (2008). *Investigating the Russian Mafia.* Durham, NC: Carolina Academic Press.

Shelley, L.I. & Picarelli, J.T. (2002). Methods not motives: Implications of the convergence of international organized crime and terrorism. *Police Practice and Research,* 3, 305-318.

Shelley, L.I. (2001). Transnational organized crime: An imminent threat to the nation state?. *Journal of International Affairs,* 48, 464-489.Sterling, C. (1994). *Thieves World.* New York, NY: Simon & Schuster.

U.S. Department of Justice. (2005). *National gang threat assessment* (BJA Publication No. 2003-DD-BX-0311, pp. 37-46). Washington, DC: National Alliance of Gang Investigators Associations.

U.S. Department of Justice (2007, October). *National drug threat assessment* (Product No. 2007-Q0317-003). Washington, DC: National Drug Intelligence Center.

U.S. Department of Justice. (2009). *President's budget.* Retrieved May 15, 2008, from http://www.whitehouse.gov/omb/rewrite/budget/fy2009/justice.html

Varese, F. (2001). *The Russian Mafia.* Oxford, NY: Oxford University Press.

VITA

Valerie E. Hollier was born in Lafayette, Louisiana on August 1, 1984, the daughter of Susan Gail Hollier and Gregory Martin Hollier. After completing her work at San Marcos High School, San Marcos Texas, in 2002, she entered Sam Houston State University in Huntsville, Texas. During the summer of 2004, she attended Texas State University- San Marcos. She received her degree of Bachelor of Science from Texas State University- San Marcos in May 2007. In August 2007, she entered the Graduate College of Texas State University- San Marcos and was employed as a graduate assistant.

Permanent Address: 4103 Hilliard Rd.

San Marcos, Texas 78666

This thesis was typed by Valerie E. Hollier