WHERE POLITICAL EXTREMISTS AND GREEDY CRIMINALS MEET:

A COMPARATIVE STUDY OF FINANCIAL CRIMES AND CRIMINAL NETWORKS IN THE UNITED STATES

by

Roberta Belli

A dissertation submitted to the Graduate Faculty in Criminal Justice in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York

2011

This manuscript has been read and accepted for
the Graduate Faculty in Criminal Justice in satisfaction of the
dissertation requirement for the degree of Doctor of Philosophy.

Joshua D. Freilich, Ph.D.

_____ _____

Date Chair of Examining Committee

Joshua D. Freilich, Ph.D.

_____ _____

Date Executive Officer

Kirk Dombrowski, Ph.D.

Amy Adamczyk, Ph.D.

James P. Lynch, Ph.D.
Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK

ABSTRACT

Where political extremists and greedy criminals meet: A comparative study of financial crimes and criminal networks in the United States

by

Roberta Belli

Advisor: Joshua D. Freilich, Ph.D.

Financial crime poses a serious threat to the integrity and security of legitimate businesses and institutions, and to the safety and prosperity of private citizens and communities. Experts argue that the profile of financial offenders is extremely diversified and includes individuals who may be motivated by greed or ideology. Islamic extremists increasingly resort to typical white-collar crimes, like credit card and financial fraud, to raise funds for their missions. In the United States, the far-right movement professes its anti-government ideology by promoting and using a variety of anti-tax strategies. There is evidence that ideologically motivated individuals who engage in financial crimes benefit from interactions with profit-driven offenders and legitimate actors that provide resources for crime in the form of knowledge, skills, and suitable co-offenders. This dissertation sheds light on the nexus between political extremism and profit-driven crime by conducting a systematic study of financial crime cases involving Islamic extremists, domestic far-rightists, and their non-extremist accomplices prosecuted by federal courts in 2004. Attribute and relational data were extracted from the *U.S. Extremist Crime Database* (ECDB), which is the first open-source relational database that provides information on all extremist crimes, violent and non-violent, ideological and routine crimes, since 1990. A descriptive analysis was conducted comparing schemes, crimes, and techniques used by far-rightists, Islamic

extremists, and non-extremists, before moving into an in-depth social network analysis of their relational ties in co-offending, business, and family networks. The descriptive findings revealed considerable differences in the *modus operandi* followed by far-rightists and Islamic extremists as well as the prosecutorial strategies used against them. The subsequent exploratory and statistical network analyses, however, revealed interesting similarities, suggesting that financial schemes by political extremists occurred within similarly decentralized, self-organizing structures that facilitated exchanges between individuals acting within close-knit subsets regardless of their ideological affiliation. Meaningful interactions emerged between far-rightists and non-extremists involved in business ventures and within a tax avoidance scheme, indicating that the crime-extremism nexus was more prevalent within far-right settings compared to Islamic extremist ones. The findings were discussed in light of their implications for criminological theories, criminal justice and crime prevention policies, and methodological advances.

ACKNOWLEDGMENTS

I would like to express my deepest gratitude to my advisor, Dr. Joshua D. Freilich, who started mentoring me during my first year as a PhD student and encouraged me to fully explore the whole range of my research interests. Over four years ago we started talking about a possible study on financial crimes and terrorism. No longer after that we embarked on this incredible project together, and that is how the *U.S. Extremist Crime Database (ECDB) - Financial Crime* from an idea became reality. For believing in me and giving me the chance to create something so meaningful and ambitious, I will be forever grateful.

I am greatly obliged to my examination committee: Dr. Dombrowski, who sparked my interest in social network analysis and offered invaluable feedback and guidance; Dr. Adamczyk, who agreed to join this project at the last minute without hesitation; and Dr. Lynch, whose challenging questions undoubtedly contributed to make this a more rigorous empirical study. I must also thank the National Institute of Justice (NIJ), the National Consortium for the Study of Terrorism and Responses to Terrorism (START), and the U.S. Department of Homeland Security (DHS) for funding this research.

This dissertation would have not been possible without the amazing team of research assistants who worked on the ECDB: William, Catherine, Ashmini, Yvette, Rebecca, Kevin, Tarra, Celinet, Johnny, and many others. I met a few colleagues at work, and I found many good friends. Thank you for all your help and support.

I owe everything to my family back in Italy and here in the United States.

Mamma e papa': veni vidi vici! Thank you for your endless faith and trust. Even when the road ahead was not clear, you never stopped encouraging me and giving me the strength to pursue my dreams. I am who I am today because of who you are.

Simone, the "real" scientist: you have been a great friend, amazing listener and supporter throughout my life. Thank you to the best brother any big sister could wish for. Soon there will be not one, but three doctors in the family.

Fabio: thank you for your love, support, patience and understanding. You made me laugh when I needed it most, and comforted me when I was almost ready to give up. I took each and every word you said at heart and look where it brought me.

Benito: it's amazing what a little furry friend can do to preserve a PhD student's mental sanity. Grazie Gigi!

My grandparents, here and in the afterlife: nonna Beppa e nonna Natalia, nonno Livio e nonno Silvio. We have come a long way from that sunny mountain region of ours.

My experience as a doctoral student at John Jay College would have not been the same withouth the many talented and inspiring people whom I shared with all the good and bad moments: Besiki, Meredith, Andrea, Crystal, Anna, Younoh, Gipsy. Thank you!

To all the wonderful people I met since I moved to New York City, who helped me in so many ways, knowingly or unknowingly. You are too many to mention, but you all have a special place in my heart.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1. INTRODUCTION

1.1 Problem Statement

Financial crime poses a serious threat to the integrity and security of legitimate businesses and institutions, as well as to the safety and prosperity of private citizens and communities (Biagioli, 2008; Levi, 2003; Nelken, 2002). The United States, as a leading economic power, is especially vulnerable to this type of crimes. US stock markets, financial institutions, large and small businesses and their consumer bases are all possible targets of fraud, identity theft and other financial crimes. The risk is heightened when unscrupulous actors such as terrorists and organized criminals penetrate the legitimate economy to pursue their political or criminal agenda (Berdal & Serrano, 2002; Bovenkerk & Chakra, 2007; Nardo, 2004; Rollins & Wyler, 2010).

Experts have warned against the possibility that the financial sector become fertile ground for new criminal ventures thanks to lax security mechanisms, the existence of numerous offshore tax havens, and the relative easiness to commit these crimes (Beare, 2003; Bequai, 2002). The result is that the profile of financial offenders today is extremely diversified, so that it has become increasingly difficult to distinguish between "ordinary" criminals and "atypical" financial offenders, such as international terrorists or domestic political extremists (Dishman, 2005; Horgan & Taylor, 1999 & 2003; Shapiro, 2007; Shelley & Picarelli, 2005).

Recent studies reveal that financial crimes, traditionally considered the realm of white-collar offenders and organized crime groups, today attract an increasing number of militant Islamic activists and domestic far-right extremists. There is evidence that Islamic extremists increasingly resort to crime, including typical white-collar offenses like credit

card and financial fraud, to raise funds for their missions (Biersteker & Eckert, 2008a; Compin, 2008; deKieffer, 2008; Ehrenfeld, 2003; Gallant, 2007; Giraldo & Trinkunas, 2007; Hamm, 2007; Hamm & Van de Voorde, 2005; Kane & Wall, 2005; Napoleoni, 2005; Passas, 2003; Picarelli & Shelley, 2007; Raphaeli, 2003; Rollins & Wyler, 2010; Smith & Damphousse, 2003; Williams, 2008).

The significance of this problem is evidenced by the direction counterterrorism strategies have taken in the wake of the 9/11 attacks. The disruption of financing methods used to support terrorist activities has become a top priority in the United States and all over the world (Biersteker, Eckert, & Romaniuk, 2008). More than 130 countries signed the "UN International Convention for the Suppression of the Financing of Terrorism", requiring legislative action and financial supervision to detect illegal money flows. The Financial Action Task Force (FATF) based in Paris, France, has published several recommendations designed to fight terrorist finance and improve financial transparency, including new regulations for financial institutions such as "know-your-customer" and suspicious transactions reporting. In the United States, the USA Patriot Act has introduced exceptional measures against money-laundering and other terrorism-related financing activities (Eckert, 2008). Unfortunately, it is unclear whether these initiatives have actually had any impact on the financing of terrorism. As the 9/11 Commission Report and other experts pointed out, these policies were often based on misconceptions on the nature of terrorism financing and the general propensity to believe in "facts by repetition" rather than evidence-based studies (Biersteker & Eckert, 2008b; National Commission on Terrorist Attacks Upon the United States, 2004; Passas, 2007; Warde, 2007).

The American far right has recently become center of attention in the criminological debate (Belli & Freilich, 2009; Chermak, 2002; Chermak, Freilich, & Shemtob, 2009; Freilich & Chermak, 2009; Freilich, Chermak, & Caspi, 2009; Freilich, Chermak, & Simone, 2009;

Freilich & Pridemore, 2006; Gruenewald, Freilich & Chermak, 2008; Hewitt, 2003; Dugan, LaFree, & Fogg, 2006). Over the past few decades, far-right members have engaged in a variety of violent and non-violent criminal behaviors, including actual terrorist attacks like those carried out by Timothy McVeigh and Eric Rudolph. A specific segment of the domestic far right – linked to the tax protest movement – professes its ideological opposition to the government by using and advocating tax evasion and other fraudulent practices devised to purportedly allow people to avoid paying income taxes (ADL, 2003 & 2005; Sanger-Katz, 2006; SPLC, 2001 & 2007). The press has sometimes referred to this phenomenon as "paper terrorism", i.e. the filing of bogus property liens, warrants, writs and other documents, which results in considerable administrative and judicial backlog and has sometimes escalated to violent threats and harassment against public officials (Corcoran, 1990; Levitas, 2002; Pitcavage, 1996, 1999 & 2001). Oftentimes, these behaviors appear to have a clear ideological orientation, like in the case of ideologically motivated tax refusal (Belli & Freilich, 2009). In other instances, it is unclear whether the motivation is ideological, profit-driven, or both (McNab, 2006; Sanchez, 2009).

Despite the seriousness of these problems, there is a lack of empirical research in this study area. Journalistic accounts tend to "fill in the gaps between facts in order to create a better narrative" rather than accurately investigate the extent of the problem (Sageman, 2004, p. 67). This has created a number of "myths" – like the idea that Al-Qaeda profited from speculations in the stock markets after the 9/11 attacks, subsequently debunked in the 9/11 Commission Report –that have led to the implementation of ineffective and even counterproductive policy choices (National Commission on Terrorist Attacks Upon the United States, 2004; Levi, 2008a; Passas, 2007; Warde, 2007). This research attempts to fill this literature gap and shed light on the relationship between political extremism and

profit-oriented crime in the financial arena with a view to the implications for crime prevention and criminal justice purposes.

1.2 Project's goals

This dissertation advances a systematic study of financial crime cases involving political extremists (i.e., Islamic extremists and American far-rightists) and profit-oriented individuals prosecuted by US federal courts in 2004 by conducting a quantitative analysis of attribute and relational data obtained through open sources. The purpose was to investigate whether and to what extent these various criminal actors converge in the financial arena, and what can be done about it.

Four main goals were pursued in this research:

1. Understanding the *financial schemes* and *techniques* used by political extremists prosecuted in the US, as well as the *crimes* they are charged and convicted with;
2. Comparing similarities and differences between *ideologically motivated* and *non-ideological, profit oriented* offenders;
3. Investigating the nature and structure of their relational ties to determine how contacts and interactions with criminal and legitimate actors may provide valuable resources for crime;
4. Producing useful knowledge for U.S. policy-makers and justice officials involved in counterterrorism strategies.

Given the lack of criminological research in this study area, this dissertation serves first of all as an exploration into the financial criminality of political extremists in the United

States, focusing specifically on two ideological movements that seemingly engage in non-violent, financial crime, i.e. the domestic far right and Islamic-related extremism. To understand the different aspects of these crime types, this dissertation provides an in-depth descriptive analysis of judicial cases focusing on (a) the financial scheme, intended as the overall illicit financial operation involving one or more suspects over a period of time, (b) financial crimes, which refer to the specific offenses suspects are charged and convicted with (i.e., legal component), and (c) the techniques used by the suspects to carry out the scheme (i.e., behavioral component). Importantly, this descriptive analysis was conducted in a comparative way to highlight similarities and differences between far-rightists, Islamic extremists, and profit-driven offenders. Although academics and criminal justice professionals tend to consider terrorism and profit-oriented crime as substantively different phenomena, there appear to be similarities and connections that have long been overlooked. In the words of Jacobs (2007), "money is the nexus of everything".

To further shed light on the nexus between political extremism and profit-driven crime, this dissertation employed social network analysis exploring the nature and structure of the relational ties between far-rightists, Islamic extremists, and non-extremist accomplices, and testing four hypotheses using a sophisticated statistical method especially developed to model network data, i.e. Exponential Random Graph (p*) Modeling (ERGM). The goal was to improve our understanding of the relational dynamics between financial scheme participants who appear to be variously motivated, focusing in particular on how legitimate and criminal actors interact, and possibly discover hidden behavioral patterns and vulnerabilities that could provide useful knowledge for US policy-makers and criminal justice officials to devise more effective counterstrategies, prioritize among different crime problems, and better allocate the available resources.

Chapter 2 provides a review of criminological studies on financial crime, starting with a brief overview of research on white-collar and organized crime, followed by an examination of financial criminal behaviors associated with international terrorism and domestic far-right extremism, and concluding with a synopsis of studies on the convergence between these social phenomena.

Chapter 3 introduces the theoretical framework driving this exploratory study, which combined opportunity theories with the social network perspective, and poses the research questions and hypotheses.

Chapter 4 outlines this dissertation's methodology, including a detailed description of research design and data collection procedures, which followed the open-source searching and coding protocol developed for the *Extremist Crime Database – Financial Crime* (ECDB). A section of this chapter is devoted to definitions and principles pertaining to social network analysis, since this is the primary method used in this research.

Chapter 5 presents the descriptive findings, starting with a comparison of financial schemes, crimes, and techniques, before focusing on suspects' characteristics comparing between far-rightists, Islamic extremists, and their non-extremist accomplices. In conclusion of this chapter, an analysis of open-source materials used to collect attribute and relational data is provided.

Chapter 6 deals with financial extremist networks, describing the results of our exploratory and statistical network analyses, which are further discussed in Chapter 7 in light of their theoretical, practical, and methodological implications, concluding with a discussion of research limitations and future directions.

CHAPTER 2. BACKGROUND AND SIGNIFICANCE

Political extremism and profit-driven crime are usually considered distinct social phenomena and, therefore, studied separately in criminology (Bovenkerk & Chakra, 2007). While they undoubtedly have some distinctive features, there may be similarities and connections that have long been overlooked because of this preconceived notion. This section begins with a brief background on the extant literature concerning financial crime in the criminology literature to subsequently focus on the involvement of political extremists, more specifically supporters of the American far right and Islamic-based extremism, and lastly addresses the issue of their convergence.

2.1 Financial crime in the criminology literature

In the criminology literature, there is no universally accepted definition of financial criminality. Sometimes equated with white-collar and corporate crime, in the public view financial crimes are often associated with profit-oriented individuals, groups and corporations (Croall, 2001; Hobbs, 1994; Ruggiero, 1997; Levi 2003). Until recently, the public and academic interest in these crime types has been notably low compared to other crime problems, such as gangs and violent crime. Except for some high-profile scandals, like those started in 2001 with Enron and including WorldCom, Global Crossing, Adelphia, and Tyco, and the recent decades-long Ponzi scheme by Madoff, criminal trials involving financial offenses have been seldom publicized (Friedrichs, 2004). Financial offenders are considered less blameworthy compared to conventional criminals who engage in, for

example, burglary or robbery, and this is reflected in the punishing treatment, which generally involves lower sentences (Wright, 2006).

The term “white-collar” crime was first coined by Sutherland in 1939, and described as a “crime committed by a person of respectability and high social status in the course of his occupation” (1983, p. 7). Since then, criminologists have tried to measure the pervasiveness and impact of this problem, and developed ways to classify offense and offender types (Croall, 2001; Doig, 2006; Gill, 1994; Levi, 2003; Nelken, 2002; Weisburd, Wheeler, Waring, & Bode, 1991; Taylor, 1999).There is, however, a substantial disagreement on how to define and interpret the various criminal behaviors falling under this overarching crime category. In particular, the tendency to identify financial and white-collar crime with ‘elite crime’ or ‘crimes of the powerful’ has been criticized because it creates stereotypes about offenders that do not always represent the reality accurately (Weisburd et al., 1991).

Some studies focus on specific financial crime types to grasp the motives and profile of financial offenders. Croall (2001) distinguishes between “occupational” and “organizational” crimes. The former refers to individuals or small groups who offend for personal gain, and includes crimes like embezzlement, tax evasion, insurance fraud, whereas the latter involves illegal activities that are not necessarily conducted for personal profit but rather in the interests of the corporation. A number of surveys conducted in the UK among the general population revealed that insurance and benefits fraud were commonplace, and that people considered it as an acceptable behavior under certain circumstances (Gill, 1994). Both economic necessity and grievances against insurance companies and the government were identified as predominant reasons (Dean & Melrose, 1996). According to Rowlingson, Whyley, Newburn, and Berthoud (1997), people from disadvantaged areas become fraudsters to make extra-money for their families.

On the other hand, other studies argue that the majority of financial offenders are not marginalized populations but rather people who live in affluent areas and are self-employed, small entrepreneurs, or work within a company (Levi & Reuter, 2006). A study of convicted fraudsters found that greed, the position of trust, and the skills and knowledge learned at work played a central role in their criminal decision-making process (Gill, 1994). Top-level managers and executives are attracted by the extra benefits that derive from economic profit obtained by illegal means, such as power, the drive to control their and other people's lives, expensive lifestyles and the desire for social respectability (Levi, 1994).

Taylor (1999) argues that different forms of financial crimes can be found at all societal levels today as a result of the liberalization of financial markets and the lessening of the regulations for private businesses. According to Croall (2001), the concept of "need and greed" best explains the question of criminal involvement, because "financial crime is related to different levels of constraint or inducement – for those at higher levels, constraints or pressures focus on demands for continuing capital accumulation, whereas, at lower levels, pressures are related to survival where full-time employment is no longer a realistic option" (2001, pp. 92-93).

A portion of the literature on financial crime deals with organized crime, which is conventionally classified as non-ideological, profit-oriented criminality (Abadinsky, 2006). Organized crime is a complex and hard-to-define phenomenon (Vander Beken, 2004). There is no consensus among academics and experts in the field on the current situation of organized crime and its impact on our society. The reality comprises a myriad of clandestine, diverse and complex aspects of the social universe, including a broad and miscellaneous category of criminal actors who are variously organized (Fijnaut & Paoli, 2004). Recently, scholars have pointed to major changes in the structure and functioning of

modern criminal organizations, which today often involve loose networks of individuals that undertake particular criminal ventures for profit (Klerks, 2003; Levi, 2008b).

Hobbs (1994) describes organized crime groups operating in the financial crime sector as "professionals" who infiltrate the legitimate economy to reinvest the proceeds of their criminal activities. There are several ways in which criminal organizations exploit financial businesses and operations (Levi & Reuter, 2006; Williams, 1999; Wright, 2006). Successful crime trade leads to the accumulation of money. Part of this money is destined to pay accomplices, like couriers, truck drivers, lawyers and other executives. Another part of the money consists of a chain of transformations, which ends in laundered surplus capital and enters the legitimate world (Reuter & Truman, 2004). Crime-money shows up invested in some tax haven or in legitimate activities, like the catering business (pubs, restaurants), gambling (casinos), transportation services, the real estate market, and construction industry. Fraud, money laundering, tax evasion and other financial crimes are therefore a constant theme and often a side consequence of the criminal enterprise (Beare, 2003; Doig, 2006; Levi, 2003).

Other criminologists point to underlying connections between legitimate and illegitimate businesses (Albanese, 1995; Block & Griffin, 2002; Di Nicola & Zoffi, 2005; Kelly, 1999; Levi, Nelen, & Lankhorst, 2008; Middleton & Levi, 2005; Van Duyne & Von Lampe, 2002). Findings from the "Organized Crime Notification Scheme" (OCNS), a survey collecting data from UK police agencies, reveal that 43 percent of organized crime groups identified had established "shell" corporations for their illicit activities, and 20 per cent had actually invested in the financial market (Gregory, 2003). Ruggiero (2003) argues that organized and white-collar crime should be studied conjointly, as the 'upperworld' tends to be increasingly involved in the 'underworld' in a relationship of "mutual entrepreneurial

promotion" (2003, p. 35). The result is what Ruggiero calls "dirty economies", a concept that highlights how illegitimate and legitimate environments often intermingle.

2.2 Terrorism and financial crime

The relationship between terrorism and financial crime is a relatively new topic. *Terrorism financing* is the general rubric used to refer to activities aimed at providing financial support to terrorism operations. According to the UN International Convention for the Suppression of the Financing of Terrorism, a person engages in terrorism financing "if that person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

a. An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex; or
b. Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act".

This definition is clearly broad and vague both in terms of what specific activities are prohibited and with respect to what constitutes a terrorist act for the purposes of the law. The extant literature details various fund-raising methods that have been pursued by militant activist groups. Historically, typical sources of funding came from supportive

countries, wealthy individuals, domestic population and ethnic Diasporas in the form of voluntary contributions or extortion (Giraldo & Trinkunas, 2007). Today, however, terrorist organizations tend to diversify their sources of income depending on the available opportunities to increase their independence of action. Recent societal developments, such as globalization and the decline of state-sponsored terrorism, have been indicated as primary factors in the decision of terrorist groups to turn to crime (Hamm, 2007; Passas, 2007).

A growing body of literature supports the hypothesis of a crime-terror nexus, especially as a result of the post-9/11 alarm on terrorism financing. According to Hamm (2007), terrorists engage in a wide range of criminal activities to raise funds for their missions. Regardless of the specific political objectives and the methods employed to achieve them, they all need logistical support in the form of cash, materials, personnel, training, communication systems, travel, and so forth. Unfortunately, this area is surrounded by inaccurate information mostly based on unempirical and anecdotal evidence (Biersteker & Eckert, 2008b; McCulloch & Pickering, 2005; Passas, 2007; Warde, 2007).

The study of terrorism presents several problems, including the lack of reliable and accessible data compared to conventional crimes, the reluctance of law enforcement agencies to share their information with academic researchers, and the underground nature of terrorist organizations and their members (Hamm, 2007; LaFree & Dugan, 2004). The recent creation of terrorism databases, like the Global Terrorism Database (GTD), the American Terrorism Study (ATS) and the Extremist Crime Database (ECDB), is therefore of paramount importance for terrorism researchers. Using ATS data, Smith, Damphousse, and Roberts (2006) found that terrorists engage in a variety of non-terrorist planning activities and “antecedent” criminal conduct prior to the commission of any terrorist act. These “preparatory crimes” also include crimes to procure funding for the group. Hamm (2007)

used ATS data to compare methods used by domestic and international terrorists for financing purposes, and found that right-wing terrorism in the US is more likely to engage in mail fraud, racketeering and other financial crimes than international jihad groups.

A recent NIJ-sponsored study (Kane & Wall, 2005) explored the links between white-collar crime and terrorism financing in the US by examining a sample of 100 defendants indicted in federal court between 2001 and 2003 for terrorist-related activities. Interestingly, most cases involved white-collar offenses, like ID theft, money laundering, fraud, and intellectual property crime. Credit card and financial fraud appeared to be most directly related to funding terrorist activities.

Picarelli and Shelley (2007) argue that terrorists today rely more increasingly on crime as both a source of financial support, i.e. to obtain funds and services needed to run their operations, and for logical support, i.e. to fulfill specific operational and logistical goals. In particular, certain situational factors – like the available criminal opportunities, contacts with criminal groups or individuals, organizational capabilities, and entry costs – play a significant role in terrorists' decision-making process. Financial crimes, like credit card theft and fraud, seem to be popular among terrorist groups such as al Qaeda, Hezbollah, and Hamas, because they require relatively little expertise and involve low costs and few barriers (Shapiro, 2007). Terrorist funding may also involve high-status individuals or institutions as money is moved through banks, high-priced real estate, and offshore tax havens (Picarelli & Shelley, 2007). To better understand the complexities of the terrorism-financial crime nexus, it is therefore important to also consider the role of legitimate actors, such as bankers, lawyers, accountants, and discover the points of intersection between legitimate and illegitimate economy (Block & Griffin, 2002; Di Nicola & Zoffi, 2005; Levi, Nelen, & Lankhorst, 2005).

Some experts argue that much of the US anti-terrorism strategy adopted after 9/11 is the product of conventional wisdom rather than informed decision-making (Passas, 2007; Warde, 2007). In 2001, the US government launched the "war on terror", which was aimed to disrupt the financial systems that allegedly supported terrorist activities (Williams, 2008b). The USA Patriot legislation expanded investigative and prosecutorial powers to tackle money laundering and other financial related crimes (Eckert, 2008).

According to Warde (2007), the money-laundering approach was ill founded because it was based on a misinterpretation of the law. Money laundering by definition involves hiding and "cleaning" the proceeds of crime in the financial system. Terrorism financing, on the contrary, often involves "soiling" clean (or even dirty) money, which will be used for illegal purposes (Compin, 2008). Masciandaro, Takats, and Unger (2007) coined the term *money dirtying* to refer to terrorism financing activities that do not necessarily originate from predicate crimes. In this sense, money dirtying (also called the "reverse" of money-laundering) refers to the process of using money raised legitimately (e.g. through donations or legitimate investments) for illicit purposes (i.e. funding of terrorist operations). In some instances, money laundering and money dirtying overlap, for example when illegally obtained capital is used for terrorism financing purposes (i.e. money from drug trafficking activities). Oftentimes, however, money-laundering and money-dirtying are distinct criminal phenomena as they pursue different goals, involve different activities, and require different levels of financial sophistication: "in money-laundering, capital from illegal channels is repatriated in order to be used 'freely', whereas in money dirtying, the aim is to commit a crime and therefore all traces must be destroyed" (Compin, 2008, p. 599). This distinction bears significant implications for law enforcement and crime prevention purposes.

Other financing methods targeted by the "war on terror" include the alleged involvement of Islamic charities, accused of acting as legitimate fronts for terrorism financing activities, and the use of informal value transfer systems (IVTS), such as "hawalas", which originated from traditional money-transmitting practices common among certain ethnic groups in Asia, the Middle East and parts of Africa.

According to Gunning (2008), the number of charities directly involved in terrorism financing activities is quite small compared to what public opinion might think. In addition, their investigation and prosecution both in the United States and Europe has taken a politicized and antagonistic turn (Warde, 2007). One of the biggest problems authorities face is to prove the link between charitable activities and terrorism. To overcome this problem, a common strategy has been to simply label as "terrorist" charities that are believed to be affiliated with U.S. Specially Designated Terrorist Organizations (e.g. Hamas and Hezbollah) and implement preventative (but also punitive) measures, such as the freezing of assets. As it has been pointed out, the "freezing of assets has become controversial because of the inevitable freeze of charitable assets along with those assets supporting terrorism" (Hardister, 2003, p. 610). This may bring stigmatization and further compromise the network of humanitarian interventions in areas where foreign help is much needed. As a result, NGOs and human rights organizations who may be even remotely connected to one of these black-listed actors run the risk of being penalized because of this "crime by association" (Gunning, 2008).

Informal value transfer systems are "mechanisms or networks of people facilitating the transfer of funds or value without leaving a trail of entire transactions or taking place outside the traditionally regulated financial channels" (Passas, 2003, p. 14-15). This expression was coined to replace "underground banking" and "alternative remittance systems", and refers to a variety of techniques ranging from sophisticated trade diversion

schemes and Internet-based gift services to cash smuggling and "door-to-door" transfers. Some of these, such as *hawala* (which means "transfer" in Arabic and "reference" in Hindu), *hundi* (from Sanskrit for "to collect") and *fei chien* ("flying money" in Chinese), are community-based practices which provide a cost-effective alternative to formal banking systems in countries where these are not easily available (Grabbe, 2002). Experts argue that any attempt to strictly regulate or even suppress these trust-based methods should take into account their important societal function, and may in fact not be a viable option (Passas, 2007).

On the other hand, there is also evidence that, in some instances, similar methods were used for criminal goals. Trade diversion, for example, has been indicated as "one of the most sophisticated methods of laundering large amounts of money" used by terrorist groups to collect and hide funds (deKieffer, 2008, p. 150). The US State Department defines trade diversion as "the use of trade to legitimize, conceal, transfer and convert large quantities of illicit cash into less conspicuous assets or commodities", which in turn […] "are transferred worldwide without being subject to financial transparency laws and regulations" (US Department of State, 2003). These schemes involve various criminal activities, e.g. theft to procure high-value commodities (e.g., pharmaceuticals, infant baby formula, and computer hardware) and smuggling operations to transport them in countries or states where they can be sold at higher prices. Incidents involving contraband cigarette trafficking have put trade diversion under the FBI radar, which recently identified a large network of tobacco shop owners who were smuggling low-taxed cigarettes from North Carolina and NY Indian Reservations to the Detroit area. Revenues from the sale of black-market cigarettes in high-taxed jurisdictions were then transferred to Hezbollah sites in Lebanon (Shelley & Merzel, 2008).

After the 9/11 attacks, *hawalas* came under public scrutiny for a number of publicized cases that connected them to terrorism financing. A *hawala* is a trust-based value transfer system which involves the transfer of money without the actual movement of money (Passas, 2003). The sender gives money to a *hawaladar,* i.e. an intermediary, in her country for transfer to another country. The *hawaladar* instructs her contact in the destination country by fax, phone call, or email to make the requested payment to the recipient, and notes the transfer in her books. The *hawaladar* in the origin country usually charges a commission for the transfer, while the other *hawaladar* keeps a record of the receivable in her books. At some point, the two *hawaladars* regulate the balance by either settling it up or through other transactions (Manning, 2005).

One of the first post-9/11 investigations involved "Al-Barakaat", a group of companies based in Somalia providing *hawala* services for the Somali Diaspora in over forty countries. Despite the lack of evidence regarding the alleged terrorism connection and long protest campaigns, the companies' and its members' assets were frozen. Al-Barakaat eventually fell in ruin and was forced to close. This in return caused a serious financial crisis in Somalia, which did not have a formal banking system since 1993, and cuts in international aid programs. In 2009, the organization's name was finally removed from the UN terrorist list (Öhlén, 2009).

Finally, the use of "shell companies" has also been flagged (Kane & Wall, 2005). These business entities exist on paper but transact either no business or minimal business. Some people use nominees (i.e., a person designated to act for another as an agent or trustee) and form domestic or offshore shell corporations for the purpose of disguising the ownership of a business or financial activity. These can be used to facilitate underreporting of income, non-filing of tax returns, engaging in listed transactions, money laundering, financial crimes and terrorist financing (IRS, 2008). Oftentimes, the nominees are close

relatives or professionals such as corporate stakeholders, employees, attorneys, accountants, etc. (Reuter & Truman, 2004).

2.3 The American far right and financial crime

The American far-right is a neglected topic that has only recently attracted the attention of criminology scholars despite what experts say is a significant threat to public safety (Chermak et al., 2009; Freilich, et al., 2009b; Freilich & Chermak, 2009; Freilich & Pridemore, 2006; Levitas, 2002; Pitcavage, 1996, 1999 & 2001). Data shows that, in fact, domestic terrorist attacks outnumber international ones 7 to 1 in the United States (Dugan et al., 2006; LaFree & Dugan, 2007). Furthermore, a recent survey of state police agencies found that 92 percent and 89 percent of responding agencies reported the presence of far-right Neo-Nazis and militia groups respectively, whereas only 76 percent and 62 percent pointed to environmental and Islamic jihadi groups respectively (Freilich, et al., 2009). Unfortunately, the literature on far-right criminality lacks methodologically sound research (Gruenewald et al., 2008).

The Extremist Crime Database (ECDB), created by Frelich and Chermak in 2006, is the first database on all violent and non-violent crimes committed by domestic far-rightists between 1990 and 2010. The ECDB Codebook defines far-right members as individuals or groups who display the following characteristics: "they are fiercely nationalistic (as opposed to universal and international in orientation), anti-global, suspicious of centralized federal authority, reverent of individual liberty (especially their right to own guns, be free of taxes), believe in conspiracy theories that involve a grave threat to national sovereignty and/or personal liberty and a belief that one's personal and/or national 'way of life' is under

attack and is either already lost or that the threat is imminent (sometimes such beliefs are amorphous and vague, but for some the threat is from a specific ethnic, racial, or religious group), and a belief in the need to be prepared for an attack either by participating in paramilitary preparations and training and survivalism".

The domestic far right has a long history of ideologically motivated financial crimes that originated in the context of the so-called tax protest movement, one of the oldest and most active anti-government movements existing in the country (ADL, 2003 & 2005; Hewitt, 2003). After the end of World War II, two major anti-tax movements emerged with opposite political inclinations (Barkun, 1996; Levitas, 2002). The first one was part of a left-wing movement that formed as a reaction against the Vietnam War. A number of pacifist "war tax resisters" declared it was immoral, and consequently refused, to pay federal taxes that would support what they believed was an imperialistic military strategy adopted by the American government in South-East Asia. However, the movement started to lose strength after the end of the war. Today anti-war tax resisters still exist, although in much reduced number.

The second movement began in the 1950s and 1960s and has been growing steadily since as a key component of the extreme right-wing activism, often referred to as the "Patriot" movement. Unlike its left-wing counterpart, the ideology proposed by this archconservative movement lies in the belief that either income tax laws are in some way invalid or do not apply to most citizens. Promoters have been known to make a number of claims to justify their decision not to pay taxes (McNab, 2006; Sanger-Katz, 2006; Pitcavage, 1999). The following are some popular far-right anti-tax arguments:

- Income tax is merely voluntary, because of the language used on Form 1040 instruction booklet;
- State citizens are not US citizens under the Constitution but "sovereign citizens",

therefore need not pay;

- Labor cannot be taxed because wages are not income;
- Federal reserve notes do not count as income because US currency is not backed by gold or silver;
- The Sixteenth Amendment concerning congressional power to lay and collect income taxes was never ratified;
- Being required to file Form 1040 violates the Fifth Amendment right against self-incrimination or the Fourth Amendment right to privacy;
- Paying taxes is a form of slavery which is banned by the 13th Amendment.

The term "tax protester" has since then been applied to people who refuse to file returns or pay taxes because of dubious arguments against the validity or application of tax laws (although some have recently argued that they should be called "tax deniers" because of their absolute denial regarding the existence of any tax liability; McNab, 2006; Pitcavage, 2001). This belief is generally supported by conspiratorial theories about how the government is cheating on its citizens by covering up the truth concerning the money owed in the form of income taxes. Both the IRS and US courts have rejected such claims as "frivolous arguments", stating that while taxpayers have the right to contest their tax liabilities in court, no one has the right to disobey the law (IRS, 2006 & 2008). Far-right tax protesters therefore differ from common tax cheaters and other ideologically driven protesters because they believe they have a legal right as well as a moral duty not to pay federal (and sometimes state) taxes (Belli & Freilich, 2009).

Although it is hard to estimate the size of the movement, experts agree that it is growing, especially as a result of the efforts of prominent tax protesters – who include accountants, business owners, former IRS agents, doctors, lawyers, etc. – that have been

extremely vocal in their opposition to the income tax, and their ability to recruit a large number of people (ADL, 2003 & 2005; McNab, 2010; Sanchez, 2009; SPLC, 2001 & 2007). Tax protest rhetoric is promoted in live seminars, which are being held regularly all over the country, books, tapes, DVDs, and on the Internet, and it is not cheap. For example, Irwin Schiff, who is considered one of the fathers of the movement, has written several books (e.g. "The Great Income Tax Hoax: Why You Can Immediately Stop Paying This Illegally Enforced Tax") that are available for purchase online as well as in his Las Vegas bookstore. Similarly, an Iranian immigrant who founded the "Freedom Law School" in 1992 presented and sold his "Freedom Packages" – which range from $4,000 to $6,000, plus $2,000 a year in maintenance fees – to more than 200 people attending the "Health and Freedom" conference in Irvine, CA, in March 2006 (Sanger-Katz, 2006).

Over time the tax protest movement has given rise to a number of illegal behaviors that are both violent and non-violent. Although the majority of tax-related crimes committed by far-rightists include some form of tax evasion, there have been incidents since the 1970s involving threats, harassment and violence against people or property related to the enforcement of tax laws. Members of the most radical groups have sometimes engaged in serious acts of violence against the IRS and other governmental targets (Barkun, 1996; Flynn & Gerhardt, 1995; Levitas, 2002). A notorious case is that of Gordon Kahl, a fervent tax protester and state coordinator for the Texas section of the anti-tax Posse Comitatus, who was convicted of tax charges but refused to surrender to the authorities. When the marshals stopped him at a roadblock in 1983 in an attempt to bring him in, he opened fire, killing two of them and injuring several others before fleeing. The four-month manhunt ended with a second fatal shootout where he killed a local sheriff before being killed (Corcoran, 1990).

Despite exceptional cases, however, tax protesters tend to be involved in non-

violent activities, employing and advocating different tax evasion strategies that range from simple tax refusal to more complicated fraud schemes. Recently, several tax protesters have used the "Zero Return" strategy, a financial scheme created by anti-tax far-right groups like "We The People" (SPLC, 2001). Promoters instruct taxpayers either to enter all zeros on their federal income tax filings or to enter zero income, report their withholding and then write "*nunc pro tunc*"–– Latin for "now for then"––on the return. This and other tax evasion strategies have been included in the "Dirty Dozen", a list of the most popular financial scams published by the IRS annually (IRS, 2006 & 2008).

People involved in the tax protest movement have also made ample use of bogus trusts, bogus liens, "untax" kits or other devices that purportedly allow people to avoid paying income taxes. For example, promoters of "tax avoidance schemes" urge their clients to transfer assets into trusts, promising a variety of benefits, such as the reduction of income subject to tax, deductions for personal expenses paid by the trust and reduction of gift or estate taxes (IRS, 2006). High-profile bogus tax purchasers include Hollywood celebrities, such as film actor Wesley Snipes, who was sentenced to three years in prison in 2008 for willfully failing to file tax returns in the amount of $17 million (Browing, 2008; SPLC, 2007). Other schemes, based on a misinterpretation of Section 861 of the U.S. Tax Code, instruct employers not to withhold federal income tax or other employment taxes from wages paid to their employees.

Currently, a new theory has started circulating among tax protesters giving rise to the so-called "redemption movement". Members believe that the US government is using its citizens as collateral against foreign debt, and that they can get access to funds from this secret government account by using special monetary instruments without being criminally prosecutable (ADL, 2003; Sanchez, 2009). For example, in Ohio eighteen people were indicted following a two-year multi-agency investigation involving the local police

department, the FBI, the CIA and US Postal Inspectors. Their leader wrote checks on a bogus account to get $40,000 in computer equipment, swindle $119,000 from two banks and then helped file liens and involuntary bankruptcy claims against a local judge, police officials and a Cleveland area car dealer. He was convicted in 2003 of charges of intimidation, theft, forgery, uttering, possession of criminal tools and tampering with records, but continued to threaten officials from jail. This is an example of a phenomenon that experts have, quite accurately, defined as "paper terrorism" (Pitcavage, 1999).

In some cases, tax protesters have also made use of tax-exempt organizations to improperly shield income or assets from taxation using the Corporation Sole argument. In this scheme, participants apply for incorporation under the pretext of being a "bishop" or "overseer" of a one-person, phony religious organization or society with the idea that this entitles the individual to exemption from federal income taxes as a nonprofit, religious organization. When used as intended, Corporation Sole statutes enable religious leaders to separate themselves legally from the control and ownership of church assets, but the rules have been twisted at seminars where taxpayers are charged fees of $1,000 or more and incorrectly told that Corporation Sole laws provide a "legal" way to escape paying federal income taxes, child support and other personal debts (IRS, 2008). A famous evangelist minister, anti-evolution activist and businessman in Florida was recently sentenced with his wife to 10 years imprisonment on 58 counts of tax fraud, including failure to pay $845,000 in employee-related taxes, and threatening investigators. According to the defense, the couple considered themselves "workers of God", and did not believe they were subject to taxation for their theme park (the "Dinosaur Adventure Land and Creation Science Ministries"), which grossed more than $2 million dollars a year (SPLC, 2007).

Freilich and Chermak (2009) suggest a possible radicalization process or "escalation" effect, where tax-related offenses might become a gateway to more violent

forms of ideological commitment. For example, a couple from New Hampshire was recently convicted on several charges, including tax evasion and fraud, for millions of dollars (McNab, 2010). Investigations subsequently revealed that the couple owned an arsenal of weapons and explosives stored in their basement together with far-right literature, anti-government and warfare materials. It is important to understand these issues in order to provide more effective crime control and prevention.

2.4 The convergence hypotheses: where do political extremists and greedy criminals meet?

Recently, criminologists have become interested in exploring the possible areas of convergence of profit-oriented crime and political extremism. The traditional separation based on the preconceived notion that typical financial offenders (such as white-collar and organized criminals) commit crimes for personal profit whereas political extremists aim to a higher cause, like political upheaval or ideological commitment, appears to be rather simplistic and possibly misleading (Picarelli & Shelley, 2005).

In their study on the Provisional IRA, Horgan and Taylor (1999 & 2003) noticed how the Irish terrorist group progressed from violent and property crimes in the 1980s – e.g. bank robberies, burglaries, etc. – to more sophisticated financial operations involving money-laundering, tax evasion, and construction fraud in the late 1990s. Dishman (2005) describes this converging trend in terms of either a terrorist group's transition into organized crime or as collaborations between terrorists and criminal syndicates. This convergence can also be noted with respect to the groups' internal organization, which increasingly resembles that of fluid and dynamics networks of individuals who join for

short-term, opportunistic ventures. According to Hamm (2007), certain terrorist groups have made a clear transition into organized crime, like the Colombian leftist group, M-19, that entered a strategic alliance with Pablo Escobar's drug cartel, providing transportation and protection services in exchange of conspicuous funding from the cocaine trade.

Shelley and Picarelli (2005) distinguish different levels of convergence between terrorists and conventional criminals, namely: (1) "activity appropriation", defined as a shared approach where terrorists imitate criminals, and *vice versa*, by borrowing their techniques without however interacting with them; (2) "business relationships or nexus", that tend to involve individual short-term transactions; (3) "symbiotic relationship", where the two groups begin working together and sharing their methods more regularly; and (4) "transformation", where a hybrid form is created involving individuals who belong to both terror and organized crime groups.

Hutchinson and O'Malley (2007) argue that "while there is evidence of cooperation between terrorist and organized crime groups, this generally occurs in contexts where terrorists are forced to ally with organized crime (for example because organized crime already controls the relevant illicit markets), and the relationships are temporary and/or parasitical rather than symbiotic" (Hutchinson and O'Malley, 2007, p. 1096). In other words, terrorists' ideological commitment will preclude fully symbiotic cooperation with organized crime. Similarly, Morselli (2009) found substantial differences in the way terrorist groups are organized and operate compared to drug smuggling organizations as a result of different "efficiency-security" trade-offs. Short-term objectives, such as immediate monetary pay-offs (which are typical of organized crime groups), require greater efficiency at the expenses of security, whereas long-term operations (like those involving the planning and execution of terrorist attacks) favor greater protection and security for the group's members while assuring as much efficiency as possible.

According to Williams (2008), cooperation between organized crime and terrorism "is often circumstantial and has rarely been buttressed by empirical evidence" (p. 134). On the other hand, appropriation of organized crime techniques by terrorist actors (and *vice versa*) is more likely to happen, and possibly more dangerous as this may eventually lead to the creation of a wider network of criminal and terrorist contacts. For example, behind the 2004 Madrid bombing investigators discovered a drug trafficking organization whose leader, Jahmal Ahmidan ("El Chino"), became radicalized while in prison.

Some argue that not only methods, but sometimes also motives converge, especially when focusing on micro-level variations. Shapiro (2007) found that low-level terrorists involved in fund-raising activities would sometimes divert funds for personal gain rather than follow the terrorist leadership goals. Similarly, it has been noted that far-right extremists sometimes orchestrate scams to capitalize on the beliefs of other tax protesters and the greed of ordinary citizens by marketing bogus trusts and "untax" kits to avoid paying income taxes (Belli & Freilich, 2009; Sanger-Katz, 2006). Naylor (2000) holds that factors other than profit can influence common financial criminals in their decision to offend, including jealousy, prestige, and status.

Makarenko (2004) provides one of the most interesting conceptualizations of these trends emphasizing the dynamic and evolving nature of this phenomenon, which is described as an expression of the "crime-terror continuum" theory. Accordingly, crime and terrorism can be "placed on a continuum precisely because it illustrates the fact that a single group can slide up and down the scale – between what is traditionally referred to as organized crime and terrorism – depending on the environment in which it operates" (p. 130). Specifically, four general stages can be identified on this continuum line, i.e. (1) alliances; (2) operational motivations; (3) convergence; and (4) the "black hole" syndrome.

As others previously noted, alliances occur when either criminal or terrorist groups reach out to fill an operational or expertise gap, similarly to what happens in a legitimate business context. Examples include joint ventures involving Russian criminal groups and Colombian Revolutionary Armed Forces (FARC), trading arms for drugs, and the mutual entrepreneurial relationship between the Albanian mafia and the Kosovo Liberation Army (KLF) during the Kosovo conflict. Although there is evidence that such alliances have taken place in the past, Makarenko argues that they are less likely to happen than the second type, which involves "acquiring in-house capabilities" […] "to ensure organizational security, and to secure organizational operations" (2004, p. 133).

The second point on the continuum line, therefore, involves criminal entities exploiting typical terror tactics, and terrorist groups using criminal methods. For example, the Sicilian Mafia engaged in a terror campaign in Italy in the early 1990s, which included bombings and assassinations, to intimidate the public opinion and the government into abrogating a recently adopted anti-Mafia law. On the other end of the spectrum, terrorist groups have engaged in criminal activities, especially related to international drug trafficking, since the 1970s (e.g., FARC in Colombia, Sendero Luminoso in Peru, the PKK in Kurdistan).

The third type, "convergence", hypothesizes a deeper transformation involving methods and motives, and creating new hybrid entities. In this scenario, criminals become involved in the political process by either penetrating legitimate state institutions or controlling some parts of the economic sector, whereas terrorists become so engaged in criminal activities that their focus slowly shifts from ideological to monetary, maintaining "their political rhetoric as a façade" (p. 136).

The last stage on the continuum ("black hole theory") portrays a situation where weak or failed states are taken over by these hybrid groups, which can find optimal ground

to carry out their convergent agenda of political and profit goals through criminal activities. According to Makarenko, Afghanistan provides a good example of a "black hole" country. After the 1989 Soviet withdrawal, the country was left in a state of anarchy and chaos, which allowed trafficking of opiates, arms smuggling, and terrorism to flourish at the hands of transnational organized crime groups, warlords, and Al Qaeda.

Unfortunately, these categorizations and theoretical constructs are the mere product of abstract conceptualizations and speculations about how the reality possibly is based on a sometimes simplistic analysis of single case studies. More systematic research is needed to determine whether any of these typologies captures the true nature of this complex phenomenon. In this research, we propose a new analytic framework exploring and comparing organizational structures by conducting an empirical study of financial networks involving political extremists and profit-driven offenders prosecuted in the United States. It is our biggest hope to contribute at least in part to this important debate with evidence-based knowledge in this and future works.

2.5 Significance of the proposed study

This study has important theoretical, methodological, and practical implications. From a theoretical perspective, it provides a significant contribution to the criminology field, as it is the first empirically based study that focuses on financial crimes committed by ideologically motivated and non-ideological, profit-driven offenders in the United States, comparing similarities and differences. As noted, this research sheds light on the relationship between political extremism and profit-driven criminality in the financial crime sector, and questions the validity and usefulness of this distinction. This is important, given

that the extant literature on these "gray areas" of crime consists for the most part of atheoretical conceptualizations based on case studies.

From a methodological perspective, this study is innovative because it introduces a pioneering methodology to examine financial crime cases by breaking them down in three major components, i.e. (a) financial schemes, (b) financial crimes, and (c) techniques. As will be discussed more in depth in the following chapters, this methodology has enormous potential not only for researchers interested in the study of non-violent extremist crime, but also for those focusing on typical white-collar and organized crime.

Importantly, this dissertation is the first attempt of exploring the organizational structures of financial extremist networks as well as the nature of network members' relational ties to understand types and degrees of convergence. The potential of social network analysis for the study of criminal behaviors has already been acknowledged in the academic world (Coles, 2001; Krebs, 2002a & 2002b; Klerks, 2003; Natarajan, 2006; McGloin, 2005; Morselli & Giguere, 2006; Morselli & Roy, 2008; Sparrow, 1991; Van der Hulst, 2009; Van Duijn & Vermunt, 2006). However, only few studies have employed this method with respect to the crime-terror nexus (see for example Morselli, Giguere & Petit, 2007), and as of today no research has investigated the connections between Islamic extremists, far-rightists, and profit-oriented criminals.

This project is also of considerable value to policymakers and practitioners. As Van der Hulst (2009) maintains, "systematically accumulating knowledge about the structural 'blue print' of criminal activity increases our understanding of their functioning and flaws, and may lead to effective ways to counteract and disrupt those networks" (p. 102). Additionally, it adds important knowledge to terrorism research, which is still largely unempirical, and possibly provides useful information for counterterrorism strategies. Despite the massive number of terrorism-related publications, only five percent of

terrorism studies are based on empirical research (Merari, 1991; Silke, 2001). Furthermore, financial crime is a neglected topic despite its often crucial, instrumental role in the preparation and furtherance of violent attacks (Smith, Cothren, Roberts, & Damphousse, 2008). This is unfortunate, as acquiring a better understanding of the crimes committed by political extremists, violent and non-violent, ideological and routine, should become a top priority among investigators as well as policy-makers (Hamm, 2007; Horgan & Taylor, 2003; Chermak et al., 2009).

Routinized preparatory behaviors may serve as pre-incident indicators for law enforcement interventions aimed at the early interdiction and prevention of terrorist incidents (Smith & Damphousse, 2003). Focusing on terrorism financing has great potential for understanding the complexities within terrorist groups, because money is the ultimate link or "connection between known and unknown parts of terrorist networks" (Williams, 2007, p. 81). Moreover, "limiting access to lucrative profits from illicit activities simultaneously eliminates the operational capacity, and subsequent political influence, of both criminal and terrorist groups" (Makarenko, 2004, p. 141). As Horgan and Taylor (2003) maintain, finance rather than the personal or ideological commitment of its active members is "one of the most important long-term, fundamental, limiting factors for the development of a large, sophisticated terrorist group (and its political wing)" (p. 53).

Finally, this study highlights the role of financial investigators and prosecutors as active agents in governmental counterterrorism strategies. The use of financial investigations to tackle criminal enterprises has many advantages (Van Duyne & Levi, 1999). First of all, it allows authorities to deprive them of the means to act, and second, by "unraveling the web of their financial networks and financing methods, to gain knowledge of how better to combat them" (Thony, 2002, p. 1). Criminal investigations and prosecutions have tremendous potential for preventing terrorism through a "creative" use of relatively

minor laws, such as tax and immigration legislations (Breinholt, 2005; Chesney, 2005). Referencing to the famous Al Capone case, Gallant (2007, p. 457) argues that "whether moneys are destined for terrorism or are the product of tax offenses, both are criminal offenses. If the pursuit of terrorism exposes dirty tax dollars, so much better".

CHAPTER 3. RESEARCH QUESTIONS, THEORETICAL FRAMEWORK, AND HYPOTHESES

3.1 Research questions

As discussed in the literature review, scholars argue that an increasing number of political extremists engage in criminal behaviors that have traditionally been associated with profit-driven crime (Shelley & Picarelli, 2005; Dishman, 2005; Hamm, 2007; Hutchinson & O'Malley, 2007; Makarenko, 2004; Williams, 2008). Some point out that criminal and terrorist groups, despite diverging motives, have come to use similar methods to achieve their goals. In some cases this may be the result of a simple imitation process supported by existing situational opportunities. In other cases, it is hypothesized that contacts and collaborations have occurred, which may have strengthened this process further. Some go even further and argue that not only methods, but also motives sometimes converge as part of a transformation process from ideology to profit, and *vice versa*. None of these studies, however, is based on empirical and systematic research.

In an attempt to fill this gap, this study addresses the following core question: to what extent does political extremism converge with profit-oriented crime in the U.S. financial crime sector, and what should be done about it? The main question can be broken down into a number of sub-questions:

1. What are the characteristics of financial schemes involving political extremists and profit-driven offenders in the US, and what criminal offenses are they associated with?
2. What are the characteristics of prosecuted individuals, and are there any differences or similarities between political extremists and non-extremist offenders?

3. What are the techniques used to carry out these schemes, and are there any differences or similarities in the *modus operandi* followed by political extremists and profit-driven individuals?
4. How are the suspects related to each other, and how are they connected to other non-prosecuted individuals who took part in the scheme?
5. What are the properties of these financial criminal networks, and how do they vary taking into account schemes and suspects' characteristics?
6. What types of relational ties exist among network members, and how do these vary taking into account schemes and suspects' characteristics?
7. How can we use this knowledge to improve government responses?

To answer these questions, we systematically examined judicial cases involving political extremists, i.e. American far-rightists and Islamic extremists, and profit-driven offenders prosecuted by US federal courts in 2004 for their involvement in a financial scheme. The purpose was to first illustrate the characteristics of financial schemes and suspects by comparing and contrasting similarities and differences, before moving into a social network analysis of their relational ties to detect meaningful structural and behavioral patterns. The research findings were discussed with a view to the possible policy implications for criminal justice and crime prevention purposes.

3.2 Theoretical framework

The theoretical framework used in this dissertation combines opportunity theories with the social network perspective. In this section, we first present the basic tenets of

opportunity theories as defined in the criminology literature. We then introduce key concepts of social network analysis and explain how a combined theoretical model could be useful to study financial criminal networks. Although this research does not aim at explaining the criminal phenomena under study in terms of causal mechanisms, this model provides the theoretical foundation driving our exploratory and descriptive analyses. Future studies may be able to build more sound theoretical arguments in the light of this and future studies' findings.

3.2.1 Opportunity theories

Opportunity theorists argue that crime results from an interaction between a motivated offender and a set of available opportunities (Clarke & Felson, 1993). The rational choice approach, the first one to apply the concept of criminal opportunity, defines crime as the outcome of an individual's decision-making process in response to situational circumstances (Cornish & Clarke, 2008; Newman, Clarke, & Shoham, 1997). Considerations of risks, efforts and rewards provide the basis for the decision-making process that will possibly lead a potential offender to crime (Clarke, 1997).

Clarke (1980) mentioned the idea of rationality in an early critique of situational crime prevention, where he portrayed offenders as well-aware rational thinkers. This idea was subsequently developed in a more sophisticated theory, which partly borrowed from economic theories of crime (see, for example, Becker, 1968). Accordingly, criminals are seen as rational individuals who choose to act in certain ways in order to maximize their profits while minimizing the risks. Cornish and Clarke (1986) also acknowledged that people sometimes act in accordance with "standing decisions", i.e. "habitual responses or

dispositions which govern the individual's response to opportunities for crime in ordinary circumstances" (Trasler, 1986, p. 20). They developed the concept of "limited" or "bounded" rationality to explain crime incidents that are not the outcome of a full rational process, but are rather committed in the heat of the moment, such as most homicides and rapes. Crime is seen as purposive behavior, aimed at satisfying the offender's needs, and "involves the making of (sometimes quite rudimentary) decisions and choices, constrained as these are by limits of time and the availability of relevant information" (Clarke, 1997, p. 10).

Routine activity theory identifies three minimal elements for a crime to occur: a likely offender, a suitable target, and the absence of a capable guardian (Cohen & Felson, 1979). Crime is, therefore, more likely to happen when a ready offender finds a target in the absence of a capable guardian. The routine activity approach emphasizes the role played by societal changes (e.g., technological progress) in creating new opportunities for crime that are independent of individual motivations. In particular, changes in routine activities are believed to play a significant role in crime causation. Felson (2002) applied this approach to the study of white-collar crime. He argued that no specific motivation is needed to commit a white-collar offense, whether this is a trivial (e.g., cheating overtime) or a very serious one (e.g., embezzlement). The key factor is the specialized access granted by the individual's professional position. When there are changes in routine activities (e.g., the absence of a boss on sick-leave, the "capable guardian"), it becomes easier for potential offenders to reach their target, and it is therefore more likely that a person will take advantage of the situation for personal profit.

Both rational choice and routine activity theories focus on the criminal event rather than the criminal agent, and more specifically on the situational factors that may facilitate the commission of a crime. These principles provide the theoretical foundation of situational crime prevention, which employs strategies aimed at manipulating situational

circumstances to reduce crime (Clarke, 1997). Situational crime prevention has been used extensively for the prevention of a wide range of criminal activities, including property crime (e.g. car-theft, burglary, vandalism, etc.), white-collar crime (e.g. tax fraud, corporate fraud, insurance fraud, etc.) and recently also political extremism (Belli & Freilich, 2009; Burrows & Hopkins, 2005; Freilich & Chermak, 2009; Clarke, 1997; Clarke, 1999; Clarke & Newman, 2006; Hamilton-Smith & Kent, 2005; Webb, 2005). The advantage of this approach is that it does not require an in-depth understanding of the offender's ultimate motive. All criminals, like terrorists, have one immediate goal: the successful completion of their task at hand (Clarke & Newman, 2006). Following this perspective, this research focuses on objective criminal behaviors rather than subjective offenders' perspectives to understand *how* – and not *why* – financial crimes are committed.

In addition to external opportunities, recent studies have emphasized the role of certain resources that are necessary to commit a crime and can be acquired in various ways (Ekblom & Tilley, 2000; Gill, 2005; Levi, 2008; Newman et al., 1997; Niggli, 2007). As Ekblom and Tilley (2000, p. 382) explain: "some resources are part of the offender – whether acquired congenitally, learned through socialization or education or picked up more casually as items of knowledge. Together these could be regarded as the offender's core competences for crime. Other resources relate to facilitators – tools, weapons, etc. that the offender can pick up and down – and to the scope of collaboration with others."

In rational choice terms, the offender not only estimates the relative weight of anticipated efforts, risks and rewards; she will also ponder whether she is sufficiently and adequately equipped for crime (Ekblom & Tilley, 2000; Gill, 2005). Interactions with criminal associates as well as legitimate contacts play a crucial role as they may provide access to know-how and a pool of accomplices that are often necessary to engage in certain illegal activities (Haller, 1990; Tremblay, 1993). In this sense, "how potential offenders

obtain the relevant knowledge or material resources is determined by their access to various networks, subcultures and suppliers" (Ekblom & Tilley, 2000, p. 386).

This argument finds support in a common finding in criminological research, i.e. that more than half of all crimes involve two or more co-offenders (Reiss, 1986; Warr, 2002).Co-offending patterns can take many different forms: offenders may exchange knowledge and skills; one person may induce another one to participate in a criminal venture; an accomplice can provide network ties to other accomplices, etc. (Gill, 2005). According to Felson (2003), opportunities for co-offending emerge in "offender convergence settings" where potential offenders find one another in the context of their routine activities (e.g. school, bar, office, etc.). In other words, it is more likely that two people who "converge" in common routine settings become "partners in crime" rather than two strangers (e.g. neighbors, co-workers, friends, etc.).

Levi (2008b) examined the opportunity structure of different types of financial frauds, focusing on the variety of criminal actors involved and their collaborating patterns. In his discussion, he noted that, although some frauds may be committed by "transnational" organized crime groups, "others are merely mobile small groups or individuals who can transplant techniques wherever they go; and others still commit very large one-off frauds without a need for long-term or any involvement in 'organized crime'" (p. 1). Different skill sets and statuses are needed for different fraud offenses. Collaboration among motivated individuals may therefore emerge as a response to these needs.

Studies on the nature and duration of criminal collaborations among juveniles found that these are usually short-lived, although there are variations depending on the size of the co-offending group (McGloin, Sullivan, Piquero, & Bacon, 2008). Interestingly, the greater the number of offenses and the larger the co-offender group, the more likely the offenders will collaborate again in the future. From the perspective of opportunity theories, Tremblay

(1993) maintains that, to truly understand the nature of co-offending, one needs to take into account not only offenders who collaborate in a specific venture, but also all others who "the offender must rely on before, during and after the crime event in order to make the contemplated crime possible or worthwhile" (1993, p. 20).

These considerations raise three important points that will be explored more in depth in the course of this dissertation: (a) potential offenders may benefit from contacts and interactions with key individuals who provide various opportunities for crime; (b) such opportunities may come from interactions that occur in the context of daily routine settings; and (c) these criminal networks expand beyond the immediate co-offenders' group and include other meaningful relationships that are instrumental to the crime-commission process.

3.2.2 Social network theory

Social network analysis focuses on relationships among actors, such as individuals, groups or organizations, and on the patterns and significance of these relationships (Wasserman & Faust, 1994). This approach has attracted considerable attention from the social and behavioral science community as a set of methods for the study of social structures and their relational aspects (Scott, 2000). In this sense, the network paradigm is not a theoretical framework *per se*, but rather an analytic approach that facilitates the study of relational patterns and network structures among sets of actors (Morselli, 2009). The basic assumption proposed by network researchers is that every person is involved in a web of connections with many other persons, and that they all influence each other in the way they conduct their lives (Coles, 2001). Some even argue that the success or failure of

social entities and organizations may be dependent on the patterning of their internal structure (Freeman, 2004).

Although some researchers have noticed the potential of social network analysis for the study of crime, especially when considered in its associational forms, there are still very few studies in the criminology field that have employed this method (Coles, 2001). The number is in fact marginal if compared to applications in other disciplines, such as public health, anthropology, social psychology, and organizational studies. Despite the paucity of studies, some interesting works have been conducted on "covert" networks, such as street gangs, organized crime, and terrorist groups, to understand how they originate and function (Klerks, 2003; Krebs, 2002a & 2002b; Malm, 2007; McGloin, 2004 & 2005; Natarajan 2006; Morselli & Giguere, 2006; Morselli & Roy, 2008; Morselli, 2009; Sageman, 2004; Sarnecki, 2001; Van Meter, 2002; Xu, Byron, Siddhart, & Chen, 2004; Xu & Chen, 2008).

For example, Natarajan (2006) examined the structure of a large heroin-trafficking organization active in the New York City area by analyzing wiretaps and other official data. Interestingly, the network structure she identified was partially different from the picture presented by the prosecution in court. Specifically, she argued that the prosecutor might have simply identified a segment of the New York City drug market rather than an actual criminal organization with a hierarchical structure. This clearly highlights the usefulness of social network analysis not only in academic but also public policy settings.

Sageman's (2004) seminal study on the global Salafi jihad examined the network of over 170 individuals who joined this extremist movement by using their biographical data. His research focused on understanding the social and psychological dynamics that may explain recruitment and radicalization processes. Among the many interesting findings, he identified the role of social bonds (such as friendship and kinship) as a "bridge" between

potential recruits and terrorist cells. In conclusion, the author suggests that targeting social hubs that facilitate these contacts may constitute an effective counterterrorism strategy.

The study of "covert" networks presents unique challenges. From a methodological perspective, access to reliable network data and issues related to identifying network boundaries can be especially problematic. As Morselli points out, "criminal networks are not simply mirror images of non criminal networks" (2009, p. 5). In other words, "it is not sufficient to simply transpose theories and models from general social life to crime settings. Criminal phenomena require their own explanations." (2009, p. 8). The necessity to remain "underground" influences the way such networks are structured and operate, limited as they are by internal and external controls. Internally, constraints come from the necessary interaction among different participants, whose possible conflicts cannot be resolved using traditional legitimate methods. Externally, social controls from the government, public services, and the community force a "covert" network to constantly adjust to changing circumstances.

Because of these limits, trust is often a key component in the functioning and survival of illicit conspiracies (Erikson, 1981). Relational ties that can guarantee the permanence of trust among network members (e.g., kinship, friendship, business partnerships) are therefore paramount (Hutchinson & O'Malley, 2007; Krebs, 2002a). In some cases, concerns for concealment and security may even override economic interests and efficiency. Baker and Faulkner (1993) studied three collusive operations in the electronic equipment industry, and found that security concerns influenced the way the company was organized, so to protect the illegal business (and its promoters) at the expenses of profit and production. Therefore, it appears that "efficiency drives the structure of legal networks, but secrecy drives the structure of illegal networks" (p. 856).

Krebs (2002a) mapped the links between the 19 hijackers who were behind the 9/11 attacks and added nodes and links as information became publicly available. The identified network resembled the shape of a "snake", i.e. it was sparsely distributed and showed how hijackers from different cells were at considerable distance from one another. Krebs hypothesized that the hijacker network may have "traded efficiency for secrecy", by keeping cell members distant from one another and the other cells, to minimize the impact to the network if one of the members were to be captured before time.

Morselli, Giguere, and Petit (2007) explored the "efficiency-security trade-off" further by comparing Krebs' hijacking network (Krebs, 2002a) with a drug-trafficking network investigated by the police in Montreal, Canada (see also Morselli, 2009). The authors found that the need to balance security and efficiency not only distinguishes covert networks from legal ones; variations may also occur *within* covert networks, which can be attributed to other important factors, e.g. the long-term ideological objective pursued by terrorists as opposed to the short-term monetary goal pursued by conventional criminals.

In conclusion, to better understand the structural characteristics of a covert network, it is necessary to take into consideration a variety of factors that may be related to the specific needs and objectives pursued by the network's members (van der Hulst, 2009). This point has special relevance for this study as we compare networks composed of individuals who engage in illegal activities aiming at different goals (e.g. financing of a terrorist mission, fund-raising for maintenance purposes, anti-government economic sabotage, etc.) and who may be variously motivated (i.e. some purely driven by their ideological commitment, others motivated by greed, and others by a combination thereof).

The table below summarizes the theoretical framework proposed in these dissertation derived from opportunity theories as applied to the social network perspective.

Table 3.1. Theoretical framework	
Opportunity theories	**Relevance for Social Network Analysis**
➢ Rational Choice ➢ Routine Activity ➢ Conjunction of Criminal Opportunities	➢ Security/efficiency trade-off, presence/absence of trusted network ➢ Specialized access and accomplices in converging routine settings ➢ Available resources for crime (personal, cognitive, collaborative, etc.)

3.3 Hypotheses

One of the biggest advantages of social network analysis is that it investigates structure rather than assuming it (Morselli, 2009). In this research, we argue that the social network approach offers a useful perspective to study financial criminal networks composed of political extremists and profit-driven offenders. More specifically, it is argued that political extremists who engage in financial crimes are embedded in networks of various sizes and structures, composed of legitimate and criminal actors who provide opportunities for crime in the form of personal, cognitive and collaborative resources.

Based upon the previous sections, this dissertation advances four hypotheses that are examined using exponential random graph modeling (ERGM), a sophisticated technique that is based on computer simulation and allows for analyzing network data without violating its primary assumption of relational interdependence. We remand to the next chapter for a more in-depth discussion of this analytical method.

1. *Political extremists who engage in financial crimes will be associated with each other and other non-extremist accomplices through three types of relational ties, namely criminal, family, and business ties. Additionally, there will be significant variations in the structure of their criminal, family, and business networks.*

Recent studies suggest that individuals who commit crimes together are also linked through other relational ties, such as kinship or legitimate business partnership (Krebs, 2002b; Malm, Bichler, & Van de Walle, 2010; McGloin, 2004; Sageman, 2004; Sarnecki, 2001). Unfortunately, the literature on *multiplexity*, i.e. the presence of multiple types of ties between pairs of actors, within covert networks is still very sparse. This dissertation aims to advance this body of knowledge by examining and comparing co-offending, family, and business networks involving political extremists, i.e. American far-rightists and Islamic extremists, and their non-extremist associates.

As mentioned, relationships that can be trusted are essential for the functioning and survival of covert networks (Baker & Faulkner, 1993; Erikson, 1981; Morselli, 2009). Trust is a key component of any type of business relationship; it makes, therefore, sense to assume that it will have a significant impact on illegal financial operations, too. In accordance with the routine activity perspective (Felson, 2003), we therefore argue that political extremists who engage in financial criminal activities will find co-offending partners and opportunities among individuals who belong to their circle of trusted relationships, such as relatives and business associates, and that these ties will shape the structure and characteristics of their financial criminal networks (Williams, 1999).

A recent study conducted by Malm, Bichler, and Van De Walle (2010) suggests that individuals who are connected by more than one tie type may form cohesive clusters that may be more resilient to external attacks. The authors examined a large network of

individuals who had been investigated for their involvement in a criminal enterprise, and collected information on four types of relationships among network members, i.e. co-offending, kinship, legitimate business, and formal organization. They subsequently analyzed and compared network characteristics by tie classification and found that there were significant structural variations across the four sub-networks. Interestingly, kinship and formal organization networks appeared to be more cohesive than co-offending networks, suggesting that "blood is thicker than water", and therefore relationships based on trust (such as kinship and gang membership) are a stronger "glue" than mere criminal association, which can be unstable and opportunistic.

These findings are critical from a policy perspective. First of all, they highlight the importance of gaining insight into the different types of links existing among criminals, especially as it relates to legitimate relationships, such as family or business ties. In addition, they suggest that targeting different types of networks may yield different results. If co-offending networks are less cohesive, it may be useful to focus on selected key individuals who link the loosely connected parts of the network. On the other hand, cohesive networks of co-offenders who are also bound by kinship and other legitimate ties may be more difficult to dismantle, and therefore require other types of interventions.

2. *Suspect status as extremist or non-extremist will be an organizing factor within co-offending, family, and business networks involving far-rightists and Islamic extremists. Specifically, we expect homophily (i.e., the tendency of political extremists to associate with each other) to be more prevalent within family and co-offending networks, whereas business networks will display more significant*

heterophily effects (i.e., political extremists will be predominantly associated with non-extremists).

Social network formation is a complex process that can be explained as the emergence of relational ties between individuals who display certain characteristics (Leenders, 1997). Some maintain that network ties form through a process of "social selection", which occurs when "actors consciously or unconsciously structure their networks on the basis of other actors' attributes" (Robins, Elliott, & Pattison, 2001, p. 1). Others argue that sometimes the opposite happens, i.e. relationships transform people who modify their behavior or attitude as a result of this relationship, a process called "social influence". For the purposes of this research, we will focus on the first approach, and test two competing theories that have been developed by researchers interested in this topic.

The first one is based on the concept of *homophily,* which is exemplified by the saying "birds of a feather flock together" (Glueck & Glueck, 1950; McPherson, Smith-Lovin, & Cook, 2001). Accordingly, relational ties based on social selection (e.g., friendship) are more likely to form between individuals who share similar traits (e.g. same race, same gender, same age, etc.; see: Goodreau, Kitts, & Morris, 2009; Knoke, 1990; Wimmer & Lewis, 2010; Young, 2010). The second one refers to the opposite phenomenon, *heterophily¸* i.e. the tendency for a network to form based on actors' differences, which has also been observed within social settings. In a heterophilous environment, including people who think and act differently, innovative ideas spread more easily, making changes and progress easier to achieve (Rogers, 1962). Being part of a heterophilous group is also considered an important factor in social capital studies because, for example, it increases the likelihood that people will find out about new employment opportunities (Burt, 2001 & 2005; Lin, 2008).

Although these theories have traditionally been applied to legitimate social settings, selection processes based on specific actor attributes can provide an interesting and useful framework to better understand tie formation within covert networks, too (Kleemans, 2007; Morselli, 2009; Stohl, 2008). In the criminology field, social selection was discussed by Gottfredson and Hirschi (1990), who argued that juveniles with deviant tendencies have low self-control and tend to associate with similar peers. Among opportunity theory scholars, Tremblay (1993) argued that "the search for co-offenders […] involves complicated mating processes by which potential co-offenders select themselves as mutually suitable or unsuitable for crime purposes" (pp. 33).

In this dissertation, we hypothesize the existence of both homophily and heterophily effects within far-right and Islamic financial extremist networks. Homophily effects will be prevalent within familial and criminal settings. Specifically, among financial scheme participants who are linked by kinship or commit crimes together, we expect to find political extremists to be more prevalently associated with other extremists rather than non-extremists because of the focus on trusted relationships (Malm et al., 2010; Krebs, 2002a; Sageman, 2004). Familial networks are described as typical homophilous settings, and have the advantage of providing strong and lasting relationships (Cook et al., 2001). Social selection processes based on homophily have also been noted by researchers studying juvenile delinquency, who found that ties between delinquent peers form more frequently among adolescents with similar attitudes and behaviors (Gottfredson & Hirschi, 1990; Glueck & Glueck, 1950; Tremblay, 1993; Warr, 2002).

Heterophily effects, on the contrary, will be predominant among business associates to facilitate professional services and exchanges that are instrumental to the execution of the financial scheme (Ekblom & Tilley, 2000; Gill, 2005). According to the "strength of weak ties" theory, first developed by Granovetter (1973), criminal networks whose members

share similar characteristics and are strongly and exclusively connected with each other are at a disadvantage compared to those that are more diversified and have loosely connected members ("weak ties"). The latter are, in fact, more isolated from distant parts of the social system compared to the former, and may therefore suffer from a lack of information exchange (Coles, 2001; Granovetter, 1973). As Levi (2008b) noted, financial crimes sometimes require specialized knowledge and skill sets that political extremists do not possess, pushing them to venture out searching for new connections beyond their familiar settings. Therefore, we argue that business relationships will provide an ideal setting where heterophilous interactions between extremist and non-extremist associates occur most frequently.

3. *Islamic and far-right extremist networks will exhibit different structural characteristics as a result of different ideological goals pursued through financial schemes. More specifically, we expect far-right extremist networks to be more cohesive and centralized than Islamic networks based on different efficiency-security trade-offs.*

Covert networks can usually be partitioned into smaller subgroups involving co-offenders who collaborate closely with each other for the completion of specific objectives (Xu & Chen, 2008). Their structures vary greatly depending on a variety of factors, including the type of criminal activities, long-term and short-term objectives, actors' characteristics, and so forth (Krebs, 2002a; Morselli, Giguere & Petit, 2007; van der Hulst, 2009). This argument is in tune with rational choice theory, which defines crime as goal-oriented

behavior aimed at maximizing benefits while containing costs under specific situational constraints (Clarke, 1980; Cornish & Clarke, 1986).

In particular, the need to balance security with efficiency appears to be a significant factor in covert networks (Baker & Faulkner, 1993; Erickson, 1981; Morselli, 2009). In fact, "the efficiency-security trade-off is presented as the interplay between the need to act collectively and the need to individually assure trust and secrecy within these sensitive collaborative settings" (Morselli, 2009, p. 64). In this respect, criminal and terrorist networks are self-organizing structures that follow a "flexible order" investing in either more security or efficiency depending upon the specific network's objective or, in other words, adapting the number and type of interactions depending on the specific "time-to-tasks".

Morselli (2009, p. 65) maintains that covert networks pursuing ideological causes have longer time-to-tasks, "because they are less often in action than are criminal enterprise networks", and put therefore more emphasis on security rather than efficiency. From a social network perspective, these variations are reflected in different structural patterning. A covert network that favors security over efficiency is likely to be dispersed and decentralized (e.g., the 9/11 hijackers network described by Krebs, 2002a), whereas one where efficiency is more important than security will present a denser and more centralized structure, where information flows more easily and prominent actors are more clearly visible (e.g., the drug trafficking network described by Morselli, Giguere & Petit, 2007).

In this dissertation we argue that structural variations occur not only between criminal and terrorist networks, but also *within* different types of ideologically driven covert networks. More specifically, we argue that the different ideological goals pursued by far-rightists involved in tax avoidance schemes (i.e., non-violent, anti-government protest) compared to Islamic extremists engaging in terrorism financing activities (i.e., pro-violence)

will affect the structure of the networks they are embedded in. In particular, the lesser risk associated with non-violent criminal goals strengthened by tax protesters' ideological convictions will result in a centralized structure that favors efficiency over security in the form of increased information sharing, shorter distances between members, and the presence of prominent figures that function as reference points, or "hubs". On the other hand, Islamic extremist networks aiming at raising funds for future violent activities, similarly to terrorism cells that are in a dormant phase preceding action, will display a more dispersed and decentralized structure, including smaller cohesive subsets for enhanced security and insulation from outside threats.

4. *Suspect non-extremist status will be an organizing factor within Islamic and far-right financial criminal networks aiming at different ideological goals. Specifically, we expect homophily effects to be prevalent within Islamic networks aiming at violent ideological goals (i.e., terrorism financing), whereas heterophily effects will be prevalent within far-right settings aiming at non-violent ideological goals (i.e., anti-government protest).*

Similarly to what we hypothesized as regards suspect status within networks based on different relational ties, we argue that social selection processes based on suspect status will shape far-right and Islamic extremist networks aiming at distinct ideological goals. Specifically, we hypothesize a prevalence of heterophilous effects within far-right financial extremist networks compared to Islamic ones, which will be characterized by significant homophilous effects.

As noted in the literature, collaborations between individuals who differ in their motivation, i.e. political extremists pursuing ideological goals on one hand and profit-driven criminals on the other, have occurred in the past in a variety of forms (Makarenko, 2004; Shelley & Picarelli, 2005). Criminologists view these collaborations as mostly erratic and opportunistic, aiming for example at facilitating short-term criminal ventures or enhancing security (Hutchinson & O'Malley, 2007; Williams, 2008). However, in the context of financial schemes involving political extremists and profit-driven individuals, variations in these collaborations may occur as a result of the different goals pursued through such schemes.

Tax avoidance schemes promoted by the American far right attract a diverse crowd of financial offenders, ranging from highly committed tax protesters to more mundane white-collar criminals (Belli & Freilich, 2009; Cornish & Clarke, 2003). Their criminal networks are, therefore, likely to comprise heterophilous ties between ideologically motivated individuals and greedy citizens (Pitcavage, 1999; Sanchez, 2009). On the contrary, fund-raising operations on behalf of terrorist organizations such as Hamas and Hezbollah are likely to be composed primarily of homophilous links between individuals who share various characteristics, including the same ethnic and religious background, and similar ideological perspectives (Stohl, 2008; Williams, 1999; Sageman, 2004). In these networks, "growth and preferential attachment are turned inward", and new connections outside a trusted circle are likely to be minimal (Stohl, 2008, p. 67).

To provide further insight into the role of non-extremist associates within financial extremist networks, we will also look at their structural position to identify key figures. In social network analysis terms, we will conduct an actor-centered analysis comparing centrality measures. One type of centrality measure (i.e. *betweenness centrality*) is particularly important in the study of criminal networks as it focuses on brokerage positions. Similarly to their legitimate counterpart, brokers are pivotal within illicit

networks as they maintain “flexibility, integration, and creativity” (Morselli & Roy, 2008, p. 72). In addition, brokers control information asymmetries and guarantee continued access to resources for crime, such as people with specialized knowledge, skills, or contacts (Burt, 2005; Ekblom & Tilley, 2000). This analysis will have important policy implications as it highlights the potential utility of strategies aiming at the elimination of selected network members (“brokers” or “bridges”), who are not necessarily at the top of the criminal hierarchy, for the disruption of the whole network (McGloin, 2005).

CHAPTER 4. METHODOLOGY

This dissertation advances an empirical study of judicial cases involving political extremists (i.e., American far-rightists and Islamic extremists) and profit-driven offenders involved in a financial scheme prosecuted by US federal courts. The purpose was to determine whether and to what extent political extremism and profit-driven crime converge in the financial crime sector.

The research strategy consisted of four stages. The first two stages involved data collection and the creation of a relational database on US financial crime. This dissertation is part of a larger project directed by Freilich and Chermak, whose initial goal was to build the most comprehensive database on all crimes committed by the domestic far right between 1990 and 2010 (*Extremist Crime Database – ECDB*). The first phase of the project (2006-2009) consisted in collecting and coding information on all violent crimes committed by individuals or groups who adhere to a far-right ideology. The project's scope was subsequently expanded to include non-violent, ideologically motivated crimes (i.e., financial crimes) and other types of political extremists prosecuted in the U.S. (i.e. left-wing radicals and Islamic extremists). This dissertation supported the project during this transition. The new database on extremist financial crime was modeled after the ECDB, which was modified and expanded further as described below.

In the third stage, the collected data were analyzed quantitatively to address the questions proposed in this research. Specifically, we first provided a descriptive analysis of financial schemes and offenders prosecuted in the United States, before moving into an in-depth study of financial extremist networks using social network analysis (SNA). The descriptive analysis provided us with a basis to identify and compare similarities and differences across suspect categories. Social network analysis allowed us to explore the

structure of networks involving individuals who engage in financial crimes in the US, examine the patterns of their interactions and relational ties, and test this study's hypotheses. Theoretical, practical, and methodological implications based on the study's findings, including recommendations concerning criminal justice and crime prevention strategies, are discussed in the final chapter.

The following sections outline the proposed research design, procedures for data collection, creation of the relational database, and data analysis plan. As social network analysis is the primary method used in this dissertation, one section is devoted to describing basic concepts and issues related to network data collection and measurement as they apply to this study.

4.1 Research strategy

This section deals with definitional issues and inclusion criteria before outlining the different stages of the data collection process, explaining how we identified our study population and describing open-source searching and coding procedures. We also describe how the new relational database, the *Extremist Crime Database – Financial (ECDB),* was created and define key concepts, such as the distinction between financial scheme, crimes, and techniques. In conclusion, we discuss methodological challenges and how we proposed to address them.

4.1.1 Definitional issues and inclusion criteria

Before we outline the different stages of the data collection process, it is important to clarify some key issues regarding our inclusion criteria, i.e. the rules we followed to identify relevant cases to be included in our database.

As mentioned, this is a study of criminal behaviors by individuals who adhere to an extremist ideology, which we broadly defined as "political extremists". We purposefully decided not to describe them or their actions as "terrorist" because of the ambiguity associated to this label. Research shows that terrorism is hard to define, and in fact there is no consensus among both academics and practitioners (Schmid, 2004; Weinberg, Pedahzur, & Hirsch-Hoefler, 2004). Furthermore, existing definitions appear to be either too broad or too narrow, failing to capture important aspects of political extremists' criminality. For example, the FBI definition, which law enforcement agencies appear to use most frequently, defines terrorism as "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives" (Freilich et al., 2009b). Thus, non-violent but ideologically motivated crimes (such as those here examined) would fall out of the FBI universe, to the detriment of effective counterstrategies which should instead adopt a holistic approach and consider all known crimes involving political extremists (Chermak et al., 2009).

In this research, we followed two basic criteria to identify incidents (or more specifically "schemes", as defined below) and suspects to be coded in our database. The first one (*behavioral criterion*) focused on the crimes committed by the suspect. To be included in our data set, at least one financial crime as defined in the U.S. Criminal Code must have been committed and an official investigation leading to a federal criminal indictment must

have been initiated. The second one (*attitudinal criterion*) referred to the suspect's ideological affiliation, and it required that at least one of the suspects be a far-rightist or Islamic extremist at the time of the scheme. Importantly, we also coded non-ideologically motivated suspects who participated in the financial scheme, as long as at least one of those involved was either a far-rightist or Islamic extremist[1].

The ECDB Codebook defines the domestic far right as "composed of individuals or groups that subscribe to aspects of the following ideals: they are fiercely nationalistic (as opposed to universal and international in orientation), anti-global, suspicious of centralized federal authority, reverent of individual liberty (especially their right to own guns, be free of taxes), believe in conspiracy theories that involve a grave threat to national sovereignty and/or personal liberty and a belief that one's personal and/or national "way of life" is under attack and is either already lost or that the threat is imminent (sometimes such beliefs are amorphous and vague, but for some the threat is from a specific ethnic, racial, or religious group), and a belief in the need to be prepared for an attack either by participating in or supporting the need for paramilitary preparations and training or survivalism. The mainstream conservative movement and the mainstream Christian right are not included".

The ECDB Codebook defines the Islamic extremist movement as "composed of individuals or groups that subscribe to aspects of the following ideals:

- only acceptance of the Islamic faith promotes human dignity as well as affirms God's authority;

[1] The ECDB Project includes crimes by other political or ideological movements, e.g. secular Arab nationalists and environmental rights extremists. However, a preliminary examination of the existing data revealed that no financial crime was committed by these extremists' types during the study period under consideration. Hence, they were excluded from this dissertation.

- rejection of the traditional Muslim respect for "People of the Book," i.e., Christians & Jews;
- "Jihad" (defined as to struggle in the path of God in the example of the Prophet Muhammad & his early companions)" is a defining belief in Islam. This belief includes the "lesser Jihad" that endorses violence against a corrupt other;
- the Islamic faith and or one's people are oppressed and under attack in both "local and nominally Muslim" Middle-Eastern/North African/Asian governments that are corrupt & authoritarian, as well as in non-Islamic nations (e.g., Israel/Palestine, Russia/Chechnya; India/Kashmir, etc) that occupy indigenous Islamic populations (an argument for political & military mobilization);
- the West in general & the U.S. in particular supports the corruption, oppression & humiliation of Islam, and exploits the region's resources;
- the culture of the West in general & the U.S. in particular (e.g., gay-rights, feminism, sexual permissiveness, alcohol abuse, racism, etc) has a corrosive effect on social & religious values;
- the people of the West in general and the US in particular are responsible for the actions of their governments and culture;
- it is a religious obligation is to promote a violent Islamic revolution to combat this assault on Islam, oppression, corruption & the values of the West by targeting nonbelievers (both Muslims and non-Muslims);
- Jihad will remain an individual obligation until all lands that were once Muslim (e.g., Andalusia- Southern Spain, Palestine, Philippines, etc.) are returned & Islam again reigns supreme in those countries;

- Islamic law- Sharia- provides the ideal blueprint for a modern Muslim society and should be implemented in all "Muslim" countries by force".

As discussed more in detail in the sections below, we referred to federal investigations and prosecutions as the starting point to identify our study universe. Because financial crimes often involve multiple jurisdictions within the United States and abroad, we deemed the federal system would constitute an optimal venue for this research. Importantly, this database continues on the line of the American Terrorism Study by Brent Smith and colleagues, which includes federal judicial cases involving individuals indicted as a result of investigation under the FBI's Counterterrorism Program.

For reasons of availability and manageability of open-source data, we decided to focus on a 12-month period (January to December 2004) and provide a snapshot of all financial crime cases involving political extremists indicted in that specific timeframe. Additionally, prosecutions started in 2004 should now be completed or in the final phases of the criminal proceedings. We remand to the ECDB Codebook (Appendix A) for a more in-depth description of our inclusion criteria with practical examples.

4.1.2 Identification of study population

This study aims at investigating how political extremists (i.e. American far-rightists and Islamic extremists) who engage in financial criminal activities associate with non-ideological profit-driven offenders. In other words, our study population consists of all individuals who participated in a financial scheme, provided that at least one of them was either a far-rightist or Islamic extremist at the time of the scheme. In this sense, the identification process is very different from those commonly used in conventional social

science research. The basic rules of random sampling and independence of observations do not apply, given that by definition network members are connected with each other through some form of relational tie (e.g. kinship, friendship, gang membership, etc.; Wasserman & Faust, 1994). We will return to this important point in the next section when discussing network data collection and analysis methods.

Keeping these issues in mind, we followed a multi-step procedure to identify our study population. First, we created a list of all publicly available judicial cases involving at least one far-rightist or Islamic extremist indicted by federal courts in 2004. Each judicial case was treated as a case study, and used as a starting point to identify relevant incidents ("financial schemes") and all suspects involved. Because financial crimes are often committed in the context of large criminal operations that may span over an extended period of time and involve many perpetrators and jurisdictions (think about the Madoff case and his decades-long Ponzi scheme as an example), investigations tend to be lengthy and complicated. The identity of all individuals involved in such schemes may come up at different stages of the criminal investigation. Therefore, to provide a comprehensive picture of financial extremist networks, we supplemented the initial list of political extremists indicted in 2004 with any other person who was prosecuted for the same scheme regardless of indictment date or ideological affiliation.

Various sources were consulted to identify relevant judicial cases, including: (a) official records; (b) existing terrorism databases; (c) watch-group reports; and (d) media publications. We started by searching through the press releases' sections of governmental agencies websites (e.g., US DOJ Office of Public Affairs, Tax Division, Criminal Division, National Security Division, etc.), which publish judicial cases investigated and prosecuted federally on a monthly basis. These websites contain a gold mine of publicly available information, and provide direct links to press releases and other relevant documents

(including indictments, civil injunctions, private motions, decisions, appeals, etc.) regarding each newly prosecuted case for over ten years.

After reviewing official government sources, we systematically searched existing terrorism databases to locate additional relevant cases. Specifically, we reviewed the American Terrorism Study (ATS) and Global Terrorism Database (GTD). Brent Smith and colleagues' American Terrorism Study (ATS) is one of the most important domestic terrorism data collection efforts (Smith, 1994). This project, conducted in cooperation with the FBI's Terrorist Research and Analytical Center, includes persons indicted federally as a result of an investigation under the FBI's Counterterrorism Program. The data have been used to investigate the prosecution and punishment of international and domestic terrorists (Smith, Damphousse, Jackson, & Sellers, 2002), test models of sentencing outcomes and prosecutorial strategies (Smith & Damphousse, 1998), and examine geospatial characteristics of violent incidents and preparatory behaviors (Smit, et al., 2008). LaFree and colleagues created the Global Terrorism Database (GTD) from the Pinkerton Global Intelligence Services (PGIS) data that identified and coded all terrorism incidents from wire services, State Department reports, other U.S. and foreign government reporting, newspapers, information from PGIS offices, and data furnished by PGIS clients (LaFree & Dugan, 2007).

There are various watch-groups that provide chronological and incident information via the web, reports, and press releases. To identify far-right cases, we searched through the following watch-groups websites: the Southern Poverty Law Center, the Anti-Defamation League, the Militia Watchdog Organization, the Center for Democratic Renewal, and Quatloos. Many scholars, law enforcement personnel, watchdog employees, and reporters belong to a listserv affiliated with the militia watchdog website. Members circulate newspaper clippings, reports, and documents about militia group and other far

right activities across the country almost daily. For Islamic extremist cases, we searched through the following websites: the NEFA Foundation, Investigative Project, Human Rights First, the Center on Law and Security, and Jihad Watch. Finally, media publications, such as newspaper stories, Internet websites, blogs, and so forth, provided additional important open source materials.

4.1.3 Data collection process

As mentioned, this dissertation is part of a larger data collection effort, the Extremist Crime Database (ECDB) project led by Freilich and Chermak, which aims at creating the most comprehensive open-source dataset on the suspects, victims, event, and group characteristics of all known crimes committed by far-rightists in the United States since 1990. The ECDB significantly expands the universe of cases relevant to the study of domestic terrorism because it includes federal and state cases, violent and non-violent, terrorist and non-terrorist, and ideological and non-ideological crimes committed by both groups and lone wolves.

The data collection process used in this study followed the protocol established for the ECDB project and consisted of two stages: (1) open-source searching; and (2) coding relevant data in a Microsoft Access relational database[2]. During the first stage, each relevant case was assigned to a searcher (i.e., an undergraduate or graduate research assistant) who conducted systematic searches over the Internet using key words from the original source

[2] Please refer to Appendix A, ECDB Codebook, for a detailed description of searching and coding procedures.

information (e.g. suspect name and residence, prosecuting jurisdiction, etc.) to compile as much information as possible on the case. Searchers used 26 web engines to retrieve all publicly available open-source materials, i.e.: Lexis-Nexis (News & Legal); Proquest; Yahoo; Google; Copernic; News Library; Westlaw; Google Scholar (both articles & legal opinions); Amazon; Google U.S. Government; Federation of American Scientists; Google Video; Center for the Study of Intelligence; Surf Wax; Dogpile; Mamma; Librarians' Internet Index; Scirus; All the Web; Google News; Google Blog; Homeland Security Digital Library; Vinelink; The inmate locator; Individual State Department of Corrections (DOCs); Blackbookonline.info

Following this process, searchers were able to uncover and gather all publicly available documents on each case, compiling them in separate folders. The information uncovered includes media accounts, government documents, court records, videos, blogs, books, watch-group reports, movement produced materials and scholarly accounts. When searching for relevant information, priority was given to court documents (i.e. indictments, private motions, injunctions, decisions, appeals, etc.), which were obtained through government agencies' websites (e.g. US Department of Justice, FBI, etc.), legal databases (e.g., Westlaw and Lexis-Nexis) and, when possible, through PACER (Public Access to Court Electronic Records), which is an electronic public access service of the United States Judiciary that allows users to obtain case information from federal courts. Court documents are considered the most reliable sources according to empirical terrorism research, because they are subjected to in-depth judicial screening and, in the case of court decisions, to cross-examination (Sageman, 2004).

The next stage involved coding the open-source materials in a relational database in Microsoft Access format, created by integrating the original *Extremist Crime Database (ECDB) – Violent Crimes* with several new attribute and structural variables, as described in the section below. To make sure that the previous searches accurately identified all

available open-source information and improve the quality of our data, each case was assigned to a different person (in this case a graduate research assistant) who reviewed the search materials and conducted follow-up searches to update search materials and clarify possible inconsistencies between sources. When coders found multiple sources containing conflicting information (e.g., date of birth was differently specified in criminal indictment and newspaper article), greater weight was granted to the more "trusted" type as defined by the empirical terrorism literature. Following Sageman (2004, p. 65) "in decreasing degrees of reliability" […], coders favored "court proceedings subject to cross examination, followed by reports of court proceedings, then corroborated information from people with direct access to information provided, uncorroborated statements from people with that access, and finally statements from people who had heard the information secondhand". Similarly, court records were favored over media reports and media reports were favored over watch group reports. The table below describes the various types of sources in decreasing degrees of reliability.

Table 4.1 Open sources hierarchy in decreasing degrees of reliability

1	Court proceedings subject to cross examination; and Appellate Court decisions
2	Corroborated information from people with direct access to information provided (i.e., key informants)
3	Corroborated information from people with direct access to information provided (i.e., key informants)
4	Uncorroborated statements from people with that access (i.e., key informants); Indictments; and other court documents not subject to cross examination; and law enforcement documents
5	Other Media reports
6	Watch-group Reports
7	Personal views expressed in blogs, websites, editorials or Op-Ed, etc.

To control for possible inter-coder discrepancies, once the data set was complete, we reviewed each single coded case, and conducted follow-up searches using the abovementioned 26 web engines. This second round of targeted follow-up searches was conducted to fill out missing data on key variables, correct data entry errors, and update the database. This process was extremely important as it allowed us to prevent possible selectivity biases, which may affect research based on open sources as discussed in the following section. We remand to future research endeavors the important task to consider these methodological issues from a measurement perspective.

4.1.4 The Extremist Crime Database (ECDB) – Financial Crimes

The complexity of financial crime cases, which are often committed in the context of larger criminal operations involving many perpetrators and jurisdictions over an extended period of time, makes them a difficult topic to study. To simplify the analysis of complex crime scenarios and capture the nuances inherent in financial crime cases, we developed a pioneering methodology that borrows from opportunity theories and the "script approach". As discussed, opportunity theorists argue that crime is goal-oriented behavior resulting from an interaction between a rational, decision-making offender and a set of available opportunities (Clarke & Felson, 1993; Cohen & Felson, 1979; Cornish & Clarke, 1986). The "script approach", developed by Cornish (1994), simplifies crime analysis by breaking down the crime-commission process in a sequence of steps to identify opportunity structures and intervention points for the development of situational prevention measures.

By combining these theoretical and analytic frameworks, we developed three key concepts that provide the foundation of the *Extremist Crime Database (ECDB) – Financial Crimes*:

- Financial scheme. The financial scheme is the database main unit of analysis, and is defined as an illicit financial operation involving a set of activities (i.e. *techniques*) carried out by one or more perpetrators to obtain unlawful gain or other economic advantage through the use of deliberate deception. Example: a money-laundering scheme in which perpetrators attempt to "clean" money from illegal activities (e.g. drug smuggling) to fund a terrorist mission abroad.
- Criminal offenses. These refer to the specific provisions in the U.S. Criminal Code which the perpetrators may be charged and convicted with in relation to their scheme involvement. Notice that these crimes do not necessarily reflect the financial scheme or techniques used by the offenders. Sometimes prosecutors may decide to charge alleged terrorists "strategically", for example, with "material support to a foreign terrorist organization" (FTO), under Title 18, section 2339A, of the US Criminal Code. Therefore, these represent the *legal component* of financial schemes.
- Techniques. To carry out the scheme, perpetrators engage in a variety of specific activities, or techniques, which constitute the *modus operandi* followed by different perpetrators, and therefore describe the *behavioral component* of the financial scheme. Example: one person may be in charge of sending money abroad via wire transfer, another one may be smuggling U.S. currency across borders, another one may open and manage offshore bank accounts, etc.

The *Extremist Crime Database (ECDB) – Financial Crimes* comprises four codebooks with more than 500 variables on: (1) Scheme, (2) Suspect, (3) Business Entity, and (4) Quality of the Data Assessment[3]:

- Scheme Codebook contains incident-level variables (e.g. factual narrative, time period, geographic location, scheme type, scheme relevance, link to other incidents, number of perpetrators, amount of government financial losses, etc.) as well as criminal justice variables (e.g. indictment information, criminal offenses charged, investigating and prosecuting agencies, court type, etc.).
- Suspect Codebook includes a variety of suspect-level variables, e.g. demographic and socio-economic characteristics, ideological commitment and strength of association to an ideological movement, group membership and role, personal motivation in the scheme, prior criminal history, investigation and trial result, etc. Importantly, this codebook comprises structural variables especially developed to collect network data.
- Business Entity Codebook focuses on collecting basic information concerning companies involved in the scheme. The role of business entities in the execution of financial schemes is, in fact, quite relevant, and although the analysis in this study is limited, future studies should provide more insight on this topic.
- Data Assessment Codebook provides a summary of the number, type, and quality of open sources used in our database. This codebook is especially important as it provides a measurement of open sources validity and reliability, and allows for monitoring open-ended issues that need to be resolved.

[3] Please refer to the ECDB Codebook, Appendix A, for a more detailed explanation of specific variables.

To sum up, the *ECDB – Financial Crimes* contains several variables of interest for the study of financial crimes by political extremists. However, this dissertation focused on selected variables that allowed us to answer our research questions, as described in the analytic method section. Upon completion of the data collection process, we exported the data into SPSS software program and created three data files (on scheme, suspect, and data quality assessment) for statistical analysis. Network data files were also created using UCINet and Pajek, two popular software programs for social network analysis, and PNet, which is a software package for statistical network modeling (Huisman & van Duijn, 2005).

4.2 Social network analysis

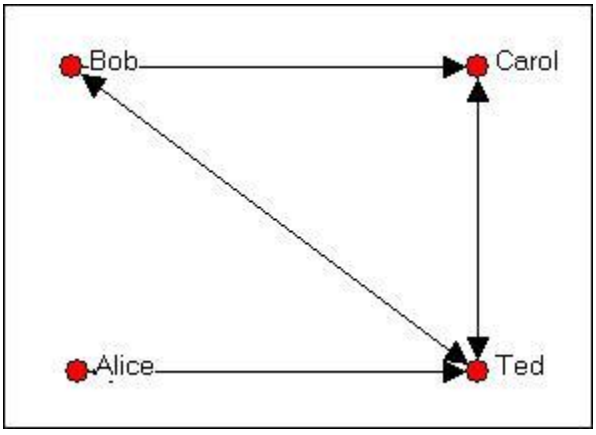
Social network analysis focuses on structural patterns among interdependent individuals (Wasserman & Faust, 1994). Network researchers have developed a specific terminology to define key concepts as well as a variety of methods to measure and model network data (Carrington, Scott, & Wasserman, 2005; Hanneman & Riddle, 2005; Huisman & van Duijn, 2005). In the following sections, we introduce the social network analysis method and describe how it is applied in this research.

4.2.1 Defining and measuring social ties

A social network is defined as a finite set of actors and the relations that exist among them (Wasserman & Faust, 1994). The terms "actor", "node", "vertex", and "agent" are used interchangeably to refer to social entities (like persons, organizations, cities, countries, etc.)

which compose a social network. "Tie", "link", "edge", and "arc" are used to describe relationships among actors. A "dyad" consists of two actors and the (possible) tie(s) between them, a "triad" involves three individuals, and a "subgroup" includes a larger subset of actors and all ties among them. These simple local structural configurations can be used to advance hypotheses about the global structure of the network (Robins, Pattison, Kalish, & Lusher, 2007). We remand to the following sections for a more in-depth discussion of these concepts and how they apply to this research.

Relational data can be represented through *sociograms*, which provide a graphical display of network members as a set of points (i.e., "nodes" or "vertices") and their relational ties as a set of lines (called "arcs" if directional, or "edges" if undirected), or *sociomatrices*, which use mathematical algebraic representations of network ties (Wasserman & Faust, 1994; Knoke & Yang, 2008). The figures below are two examples of a sociogram and its corresponding sociomatrix representing a directed network of friendship between four people (Hanneman & Riddle, 2005).



	Bob	Carol	Ted	Alice
Bob	---	1	1	0
Carol	0	---	1	0
Ted	1	1	---	1
Alice	0	0	1	---

Figure 4.1. Sociogram (left) and sociomatrix (right) of friendship network between Bob, Carol, Ted, and Alice (Source: Hanneman & Riddle, 2005).

Another important concept in the study of social networks is that of "level" or "mode" (Wasserman & Faust, 1994). Most network studies focus on *one-mode* networks, involving a specific set of actors and their relationships at an individual level. The social reality, however, is often better represented by *multi-modal* networks, which include additional sets of actors and their relationships (Hanneman & Riddle, 2005). For example, in the study of financial criminal networks, one could first examine the ties among individual offenders (one mode) as well as the relationships between criminal organizations and terrorist groups where these offenders operate (two modes).

The structural properties of a network can be measured and analyzed at different levels, e.g. at the level of the individual actor, link, dyad, sub-group, or network as a whole. In fact, "the unit of analysis in network analysis is not the individual, but an entity consisting of a collection of individuals and the linkages among them" (Wasserman & Faust, 1994, p. 5). Importantly, models and methods developed by social network researchers vary depending on the specific level of analysis chosen by the researcher. As we explain in the following section, this study focuses on individual, sub-group, and whole-network measures to examine and compare the structural characteristics of financial extremist networks.

Structural variables are the cornerstone of social network data sets and measure ties between pairs of actors (Wasserman & Faust, 1994). Network data may display various types of relationship, e.g. kinship (brother of, father of), social roles (boss of, teacher of, friend of), affectivity (likes, respects, hates), actions (talks to, has lunch with, attacks), transfer of material resources (business transactions, lending), and so forth. Connections among individuals can be *directed*, when for example information flows from one node to another one but not vice versa, like in the case of someone lending money to someone else (i.e. exchanges between sender and receiver), or *non-directed*, when the relational variable indicates a symmetrical relationship between nodes (e.g., relatives).

Social network analysts have identified four possible scales for measuring relational variables: (1) *binary measures*, where 0 denotes the absence and 1 the presence of a tie; (2) *multiple-category nominal measures*, where each category identifies a specific relationship type among actors (e.g., 1=friend, 2=husband/wife, 3=colleague); (3) *full-rank ordinal measures*, which involve ranking nodes with a strength of association measure (e.g., asking respondents to rank in order their best friend, second best friend, etc.) ; and (4) *interval measures*, which involve assigning an interval measure of association strength (e.g., recording how many times criminal associates have been arrested together). Substantive concerns and theoretical propositions determine which structural variables to measure as well as the techniques that are most appropriate for their measurement (Hanneman & Riddle, 2005; Malm, 2007).

At the very minimum, network studies include one structural variable which describes a specific type of relationship between actors in the population of interest, e.g. the exchange of professional services between lawyers and their clients. When the focus is on a multiplicity of relational ties, network studies are considered *multi-relational*. Although the majority of network studies, for simplicity reasons, usually focus on one type of relationship, the existence of multiple ties better represents the complexity of social phenomena (Hanneman & Riddle, 2005; Garton, Haythornthwaite, & Wellman, 1997; Koehly & Pattison, 2005). For example, two co-workers may also be friends and seek advice from each other. *Multiplexity*, as network researchers call it, may also characterize social ties in criminal settings, e.g. two gang members who are brothers and were both incarcerated (Malm et al., 2010; McGloin, 2004; Sarnecki, 2001).

In this study, we examined one-mode financial criminal networks collecting information on three types of relational ties between suspects and their associates, i.e.:

- Criminal tie. Two actors are linked through a criminal tie if they commit a crime together (Reiss, 1986; Warr, 2002). Studies on co-offending patterns suggest that criminal networks are often loose and opportunistic. In other words, it is unlikely that the same two persons will reoffend multiple times (McGloin et al., 2008). In this dissertation, we considered being prosecuted in the same judicial case (i.e. co-defendants) or in separate but related cases (i.e. co-suspects) as a proxy for criminal tie between two suspects.
- Family tie. Criminal association presupposes the existence and permanence of trust among its members to function efficiently and enhance security (Krebs, 2002a & 2002b; Sageman, 2004; Van der Hulst, 2009). Kinship ties between criminals often fulfill these needs, especially for complex organized crime activities that require a higher level of sophistication (Zhang, Chin, & Miller, 2007). In this dissertation, we included suspects' immediate family ties (e.g., spouse, parents, siblings) as well as more distant ones (e.g., cousins, in-laws, etc.) to describe the network of family contacts involved in financial crime activities.
- Business tie. Previous studies show that criminal networks often include individuals who provide professional services that facilitate and are sometimes crucial for the crime commission process (Malm et al., 2010; Morselli & Giguere, 2006; Ruggiero, 1997). This study operationally defines business tie as a legitimate business relationship (e.g., shared financial investment, co-ownership, etc.) or work relationship between two individuals (e.g. co-workers, employer and employee, etc.).

Consistently with previous research on multiplex networks, we used dichotomous variables to identify the presence or absence of a tie (Koehly & Pattison, 2005; Malm, et al.,

2010). In our data set, dyadic ties were symmetrical and non-directed. In other words, relationships between pairs of actors were reciprocal, i.e. two suspects prosecuted in the same criminal trial, two persons related by marriage or kinship, or two individuals exchanging financial services.

The role of multiplexity within financial extremist networks, comparing co-offending, family, and business settings involving far-rightists, Islamic extremists, and profit-driven offenders, was examined in Hypotheses 1 and 2. To explore and compare structural and attribute characteristics of two Islamic and far-right subsets testing Hypotheses 3 and 4, we aggregated the three separate relational ties into a single linkage, which can be operationalized as the exchange of goods (e.g., money, products, etc.) or services (e.g., labor, legal advice, etc.) in furtherance of an illegal financial scheme.

4.2.2 Network data collection and analysis

For a better understanding of social network research and the methodological challenges faced by network researchers, it is important to describe how network data are collected and analyzed. The populations that network researchers study are remarkably diverse, ranging from the members of a certain organization to nations in the world system. In each case, the elements of the population studied are defined by some boundaries. Population boundaries are usually decided by the specific design and data collection method chosen by the researcher (Laumann, Marsden, & Prensky, 1992; Marsden, 2005).

Most network studies employ either "whole-network" or "ego-centric" designs (Hanneman & Riddle, 2005). "Whole-network" designs involve collecting data from every member of a population whose boundaries represent naturally occurring clusters or

networks. Network studies often draw the boundaries around a population that is already known to be a network, like the members of a classroom, organization, club, neighborhood, or local community.

In many cases, however, it is not possible to track down complete or whole-networks, especially when dealing with very large or hard-to-reach populations (Morselli, 2009; Krebs, 2002a; Xu & Chen, 2008). "Ego-centric" designs provide an alternative method for network data collection by focusing on a set of focal actors (*egos*), who may be sampled from a larger population, and the selected actors' ties with neighboring individuals (*alters*) through a "snowball" approach (Kossinets, 2008). The relational system is then assumed to be composed of the sampled *egos*, reported *alters,* and their reciprocal ties, including possible additional actor and tie information (Van Duijn & Vermunt, 2006). This method is often used by researchers who decide to take a more "demographic" or "ecological" approach to defining population boundaries, which are usually set during data collection (Hanneman & Riddle, 2005). Although from a macro-structure perspective this type of data provides a more fragmented picture of the overall social universe compared to whole-network studies, it is still possible to examine the characteristics of micro-level networks or local neighborhoods in which individuals are embedded. In addition, if *egos* are sampled densely, whole networks may be constructed using egocentric network data (Marsden, 2005).

In this study, we aimed to construct a whole network by following a contextual ego-network expansion process using suspects coded in our database as primary nodes (or *egos*). Primary suspects were used as "seeds" to identify additional individuals (*alters*) who belonged to their financial criminal network but were not prosecuted (e.g., relatives or professionals, like businessmen, lawyers and accountants). In other words, we collected information on each coded suspect and the relational ties with any individual she associated

with in the context of the financial scheme. The goal was to detect the composition and structure of the overall network of criminal associates who participated in the scheme, as well as their ties to non-criminal actors similarly involved.

What makes network data unique and fundamentally different from conventional social science data is their focus on relationships among actors rather than on the attributes of actors (Pattison & Wasserman, 1999; Wasserman & Pattison, 1996). To say that network data are relational simply means that study participants are dependent on one another. If we select one actor for inclusion in our network study, then we need to include all of the actors that are connected to the first one. Network studies, therefore, do not rely on traditional random sampling and statistical modeling procedures, which require independence of observations.

These differences bear consequences for both the question of generalization of findings and for the mechanics of hypothesis testing. Most of the times, network researchers are not interested in testing any specific hypothesis concerning their study population. As Hanneman and Riddle (2005) point out, "in many cases, they are studying a particular network or set of networks, and have no interest in generalizing to a larger population of such networks (either because there isn't any such a population, or we don't care about generalizing to it in any probabilistic way)".

More recently, network analysts have experimented with hypothesis testing procedures by using a variety of methods based on precise probability distributions, such as Quadratic Assignment Procedure (QAP) correlation, exponential random graph models (p1, p2, p*), generalized blockmodeling, etc. (Doreian, Batagely, & Ferligoj, 2005; Valente, 1995; Wasserman & Robins, 2005; see Huisman & van Duijn, 2005, for a summary of statistical procedures and available software packages). Statistical advances in network modeling techniques offer a more rigorous approach to the study of network structures and allow for

uncovering and comparing relational patterns in a more systematic way. These issues will be discussed more in depth in the following section.

For the purposes of this study, structural and attribute data were collected from open-source materials and coded in the *Extremist Crime Database (ECDB) – Financial Crimes*[4]. The use of archival records for social network analysis is not uncommon among social network researchers (Alexander & Danowski, 1990; Hargens, 2000; Podolny, 1993; Podolny & Stuart, 1995). Archival network data provide unobtrusive measures of social ties because they allow for tracing relationships of actors who may be reluctant to grant interviews. Additionally, they are inexpensive and may support longitudinal network studies (Marsden, 2005). Population boundaries in our study were determined by the available information collected from open sources and coded in our database. Exploratory and statistical modeling techniques were used to analyze this data, as described in the sections below.

To conclude, we provide a summary of key terms discussed in this section (Hanneman & Riddle, 2005; Scott, 2000; Wasserman & Faust, 1994).

[4] See Appendix A – ECDB Codebook for a detailed description of network data collection and measurement.

Table 4.2 Glossary of key terms for social network analysis (SNA)

Name	Definition
Social network	A finite set of actors and all the ties among them
Nodes	Social entities that compose the network, e.g. persons, companies, countries, etc. (*aka* actor, vertex, agent, point)
Edge	A specific type of relationship between two actors that is reciprocated or symmetrical, e.g. kinship, co-offending (*aka* tie, link)
Dyad	A pair of actors and the relationship(s) between them
Triad	A subset of the network including three actors and all ties among them
Subgroup	A subset of actors and all ties among them
Component	A maximal connected subset involving two or more actors and all ties among them
Clique	A maximal complete subset of three or more nodes that are all adjacent to one another (i.e. every actor is connected to all other actors)

4.3 Analytic method

In this study, we investigated the extent to which political extremism converges with profit-oriented crime in the financial crime sector, and advanced possible recommendations based on our research findings. Seven sub-questions and four research hypotheses were developed to further specify the core question.

The dataset was analyzed using various quantitative techniques. First, we conducted a descriptive analysis to provide an overview of the financial criminality of American far-rightists, Islamic extremists, and profit-driven individuals, and to compare similarities and differences. Next, we focused on suspects' financial extremist networks by exploring

structural and attribute characteristics. Finally, we tested our research hypotheses using an innovative statistical network modeling routine called Exponential Random Graph Modeling (ERGM, or p* class models; Robins et al., 2007a). The next sections describe each of these three analyses more in detail.

4.3.1 Descriptive analysis

A descriptive analysis of the data was conducted to illustrate basic characteristics of the financial criminality of American far-rightists, Islamic extremists, and profit-driven individuals. Descriptive statistics provided us with a baseline for comparing and contrasting differences and similarities across the three offender categories. This analysis, although purely descriptive, was very informative, considering the lack of empirical research in this study area. In addition, it helped direct the subsequent exploratory and statistical network analysis. Frequencies and prevalence rates were calculated for various scheme- and suspect-related variables. At the scheme level, we focused on the following variables from our database:

- Scheme type. As mentioned, the ECDB defines a *financial scheme* as an illicit financial operation involving a set of activities aiming at a specific economic and unlawful objective through the use of deception. At present, there is a wide variety of financial scheme types that target citizens, businesses, financial markets, and government institutions, and are subject to federal investigation and prosecution. A

preliminary typology was created based on the most popular fraudulent schemes identified and described by the FBI, CIA, IRS, and other governmental agencies[5]. In this analysis, we examined frequencies of scheme types comparing far-right with Islamic extremist cases.

- Length and geographic scope. Financial schemes were examined with regard to their time duration and geographic scope. Temporal and spatial attributes are important situational factors in the analysis of crime and routine activities (Cohen & Felson, 1979; Felson, 1998 & 2002). For example, Smith et al. (2008) found that there are significant temporal and spatial differences across extremist groups (e.g. U.S.-based environmental extremist group act more quickly than international terrorists when planning and executing preparatory activities).
- Single/multiple suspect. Although organized crime and terrorism are usually viewed as collective activities, "lone-wolf terrorism" is nowadays considered a reality and a serious threat to public safety both in the US and overseas (Johnston & Risen, 2003; Dishman, 2005). Such issue, however, has never been considered with respect to non-violent criminal behaviors, such as financial crimes. Here we examined the incidence of single suspects involved in financial schemes by comparing between far-right and Islamic jihad cases.
- Scheme relevance. Financial schemes were examined with regard to their macro-level function or purpose served. Research shows that political extremists pursue various goals by engaging in criminal activities (Belli & Freilich, 2009; Horgan & Taylor, 1999 & 2003; Kane & Wall, 2005; Makarenko, 2004; Picarelli & Shelley,

[5] See ECDB Codebook for a more detailed explanation of the various sub-categories.

2005; Pitcavage, 2001; Smith & Damphousse, 2003; Williams, 2008). For example, some may resort to financial crime to raise funds for violent missions (i.e. violent ideological goal). Others may engage in this type of crime as a form of anti-government, non-violent protest (i.e. ideological, non-violent goal). It was also noticed that some schemes might help achieve multiple goals (i.e. "hybrid" schemes aiming at ideology and profit). Finally, there could be instances where political extremists have no ideological goal at all (i.e. pure profit).

- Criminal offenses. Each financial scheme involves criminal activities that may amount to a variety of federal offenses punishable under the provisions of the U.S. Criminal Code (e.g., money-laundering, Title 18 U.S.C., sections 1956-1957; material support to terrorists, Title 18 U.S.C., section 2339A, etc.). When the suspects are apprehended and brought to justice, the prosecutor may decide, for strategic purposes, to charge them with criminal offenses which may not necessarily reflect the "techniques" used (e.g. suspects are charged with the general formula "material support to a designated terrorist organization", Title 18 U.S.C., section 2339A).

  Therefore, we decided to examine criminal charges that were mentioned in the criminal indictment and investigate prosecutorial strategies used.

At the suspect level, the following variables were statistically analyzed for comparison purposes:

- Demographics. Gender, age, and occupation were examined and compared to identify differences and similarities between political extremists (Islamic extremists and far-rightists) and non-extremists financial offenders.
- Motive. This variable captures motives from a micro-level perspective focusing on the specific goals suspects aimed at by initiating or participating in a financial

scheme (i.e., ideological, profit, mixed ideological and profit, or other goal). In this way, we were able to differentiate between the overall scheme function (as previously discussed) and single individuals' involvement.

- Group affiliation. To gain further insight into political extremist movements that engage in financial crimes, we examined suspects' extremist group affiliation.
- Trial outcomes. Here we compared trial decisions (i.e. convictions, acquittals, plea-bargaining, etc.) and sentencing outcomes (i.e. imprisonment time) between far-rightists, Islamic extremists, and profit-driven offenders.
- Techniques. Lastly, we compared techniques used by extremists and non-extremists in the context of specific scheme types to better understand their *modus operandi* and identify similarities and differences.

Finally, we measured the strength of ideological association for schemes and suspects using a 4-point scale, which was initially developed by Gruenewald (2009) in his ECDB study of far-right homicides and subsequently used by Freilich et al. (2009). At the scheme-level, this variable provided us with a measure of the role of ideology in the scheme-commission process. As financial schemes may be committed by political extremists for various reasons, we thought it be important to find out how strong the ideological motive was compared to other factors.

At the suspect-level, the strength of ideological association allowed us to measure the intensity of suspects' affiliation to an ideological movement based on an evaluation of multiple sources rather than relying on single subjective interpretations (e.g. prosecutorial evidence labeling suspects as terrorists without proving their terrorism link). In this way, each political extremist in our database received an ideological affiliation score from 1 to 4. The table below describes the criteria used to measure this variable.

Table 4.3. Strength of Ideological Association

Category		Criteria
Scheme	**Suspect**	
4=Undisputed established ideological motive to further far-right or Islamic extremist goals	4=Undisputed established present or past adherence to far-right or Islamic extremist ideology	1) Multiple (2 or more) far-right/Islamic extremist indicators found, and 2) No evidence found contrary to far-right/Islamic extremist association
3=Clear established ideological motive to further far-right or Islamic extremist goals	3=Clear established present or past adherence to far-right or Islamic extremist ideology	1) Only single far-right/Islamic extremist indicator found, and 2) No evidence found contrary to far-right/Islamic extremist association
2=Disputed established ideological motive to further far-right or Islamic extremist goals	2=Disputed present or past adherence to far-right or Islamic extremist ideology	1) Multiple (2 or more) far-right/Islamic extremist indicators found, and 2) Evidence found contrary to far-right/Islamic extremist association
1=Disputed established ideological motive to further far-right or Islamic extremist goals	1=Disputed established present or past adherence to far-right or Islamic extremist ideology	1) Only single far-right/Islamic extremist indicator found, and 2) Evidence found contrary to far-right/Islamic extremist association

4.3.2 Exploratory network analysis

In social network analysis, structure is not assumed but it is searched (Morselli, 2009). Different analysis routines were used to explore patterns of interaction among political extremists and profit-driven offenders who engage in financial criminal activities, and examine the structural characteristics of far-right and Islamic extremist networks. These analyses were performed using two software packages, i.e. UCINet, the most popular social network analysis program developed by Borgatti, Everett and Freeman (2002), and

Pajek, which was created to improve analysis and visualization of large scale networks (de Nooy et al., 2005).

As a rule of thumb, the first step in exploratory network analysis is to determine whether the data display any interesting patterning at all (Freeman, 2005). This can be done by using a systematic "principled procedure" which combines visualization techniques with mathematical algorithms to search for an optimal arrangement of actors and links[6]. The goal is to find optimal layouts to position nodes on a graph in a way that accurately represent the structural patterning of the network "by depicting pairs that are socially closest in a data matrix as closest in a graphic image" (Knoke & Yang, 2008, p. 79). *Multi-dimensional scaling (MDS)* is one of the methods used to visualize data structures taking into account meaningful distances between actors, and it is especially useful to explore complex network structures and detect cohesive sub-groups. For this routine, we used the software package *Pajek,* which is equipped with sophisticated visualization techniques that utilize two spring-embedding algorithms, i.e., Kamada-Kawai and Fruchterman-Reingold algorithms (Huisman & van Dujin, 2005).

Similarly to crime mapping, visual representations of illegal networks can provide useful directions for researchers, and a starting point to develop subsequent quantitative analyses (McGloin, 2005). As the literature suggests, the structural patterning of a "covert network" is dependent upon a variety of factors, such as the type of illegal activities carried out (e.g. political violence, drug-trafficking, financial fraud, etc.), the "security-efficiency trade-off", long-term and short-term goals, etc. (Baker & Faulkner, 1993; Krebs, 2002a; Levi, 2008b; Morselli, 2009; Van der Hulst, 2009). In this analysis, we examined and compared

[6] See Freeman, 2006, at p. 49: "procedures that are specified in exact terms and that will produce the same results when they are applied repeatedly or by different investigators".

structural properties of financial extremist networks involving far-rightists, Islamic extremists, and profit-driven offenders at the network-, sub-group, and actor-level to identify similarities and differences.

At the network-level, we examined four measures that allow for comparing complete networks (Wasserman & Faust, 1994):

- Density. Density is a measure of social cohesion and estimates the degree of connectedness among network members as a proportion between the number of observed ties and the maximum number of possible ties (Freeman, 1979). Density values range from 0, indicating that the network is empty, i.e. no ties are present, to 1 when the network is complete, i.e. all individuals are connected with each other.
- Average nodal degree. Because density is inversely related to network's size and therefore tends to naturally decrease when the sample is large, it may not always be a reliable measure of social cohesion (deNooy et al., 2005). As an additional measure of connectedness, we examined the network's average degree, which is estimated by calculating the average number of lines incident with each node, or in other words the average number of neighbors each actor has (Wasserman & Faust, 1994).
- Components. Complete networks are frequently made of smaller cohesive sub-groups consisting of actors connected through many direct ties that allow them to share information and collaborate (Knoke & Yang, 2008). In social network analysis terms, these local concentrations of ties are called components, which are maximal connected sub-groups that look like large areas broken off from other elements of the network (Malm, 2007).
- Centralization. Network researchers associate centrality with power and control as a function of certain relational characteristics (Hanneman & Riddle, 2005). Centrality can be measured as a characteristic of the overall network, in which case

it is called *centralization*, as well as an actor-level property. Network centralization explains "how variable or heterogeneous the actor centralities are"; […] "the larger it is, the more likely it is that a single actor is quite central, with the remaining actors considerably less central" (Wasserman & Faust, 1994, p. 176). The centralization index, which ranges from 0 to 1, provides a measure of variation around a central tendency, similarly to the standard deviation (Knoke & Yang, 2008). Three measures of centralization are commonly referred to, i.e. *degree*, *closeness*, and *betweenness* centralization, which are described in the following paragraph together with their corresponding actor-level measures (Freeman, 1979).

Studies investigating network's topology (i.e. structural properties) usually focus on the network's largest component for more in-depth analysis (Albert & Barabasi, 2005; Xu & Chen, 2008). Similarly, we extracted two large maximally connected components (i.e. one per ideology) from our overall network of far-rightists, Islamic extremists, and profit-driven offenders to examine macro- and micro-level characteristics.

Research shows that individuals who participate in a criminal enterprise or a terrorist cell play different roles that are instrumental to the functioning and survival of their organizational structure (Krebs, 2002b; Morselli, 2009; Natarajan, 2006). In social network analysis, there are a variety of techniques that can be used to study the position and prominence of specific actors in the network. Our analysis focused on three popular centrality measures to identify and compare key players across financial extremist networks (Freeman, 1979). Actor centrality analysis is very common in network research, as it allows researchers to discover key players by summarizing structural relations among all nodes (Knoke & Yang, 2008). To carry out meaningful comparisons across networks

eliminating the effect of different network sizes, we used normalized centrality measures with values ranging from 0 to 1 (Wasserman & Faust, 1994), i.e.:

- Degree centrality. *Node degree centrality* in an undirected network is measured as the number of actors adjacent to it, or in simpler terms, the number of actors each node is connected to within the network (Wasserman & Faust, 1994). Degree centrality is a simple but informative actor-level measure, providing an indication of prominence and visibility. *Degree centralization,* mentioned above, measures the network tendency to be more or less centralized taking into account variations within all actors degree centralities.
- Closeness centrality. *Node closeness centrality* characterizes actors who have a central position in the social network because they are "closer" to a higher number of people estimating the *geodesic distance* between nodes, i.e. the length of the shortest path connecting a dyad, or pair of actors (Knoke & Yang, 2008). Accordingly, an actor with high closeness centrality can reach a second actor in very few steps, i.e. by interacting with very few intermediaries. On the contrary, an actor with low closeness centrality is more distant from the second actor, and needs to go through various intermediate steps. Closeness centrality differs from degree centrality because it highlights the position of actors who have better access to other network members thanks to indirect rather than direct ties. *Closeness centralization* refers to the variation of all actors closeness centralities within a network.
- Betweenness centrality. *Node betweenness centrality* reveals actors who lie on the geodesic path (i.e., shortest distance) between pairs of actors in the network (Knoke & Yang, 2008). Actors with high betweenness centrality are mediators connecting a large number of other actors. *Betweenness centralization* is a dispersion measures

indicating the extent to which actors differ in their betweenness centralization. Betweenness centrality has a pivotal role in the study of covert networks, as it allows for detecting brokers, i.e. individuals who are major links in the chain of contacts between other network members and control the network's flow of information (Freeman, 1979; Morselli, 2009; Sparrow 1991). It has particular relevance for government policies, as it has been suggested that targeting "cut-points" who have a strategic position instead of traditional gang or organized crime leaders may have a positive impact on containment and disruption strategies (Malm et al., 2010; McGloin, 2005).

To sum up, cohesion, centralization, and centrality measures are used by network researchers to understand the distribution of power and control within a specific social setting (Freeman, 1979; Hanneman & Riddle, 2005). For example, an actor that has many direct ties, i.e. is high in degree centrality, can be considered powerful because she has more options to pick from when, for example, deciding whom to ask for help. Power can also be related to distance between actors or, from a network analysis perspective, actor closeness centrality. In this sense, individuals who can immediately reach out to many actors within a network may be considered more influential players because they have a larger audience than individuals who are difficult to get a reach on. Finally, individuals who are positioned between many other actors, i.e. they are high in betweenness centrality, are also considered powerful actors, but in a different way because they control the flow of information within the network and can manipulate such interactions by creating or cutting connections.

Although these interpretations are valid for most social networks, they are not necessarily applicable to covert networks. In fact, previous studies on criminal and terrorist networks have come to equate degree centrality with visibility and vulnerability. Think

about, for example, an organized crime leader who knows all his subordinates, but is also known by the police because of these many connections. Betweenness centrality, on the other hand, is considered a crucial quality in covert networks, because it highlights the existence of strategic players who are not immediately visible, but control information asymmetries and provide a bridge between otherwise unconnected network subsets (i.e., brokers; see: Baker & Faulkner, 1993; Malm et al., 2010; Natarajan, 2006; Morselli, 2009).

To better understand these concepts in view of the following analysis, in the tables below we illustrate three simple graphs displaying different structural patterns (source: Hanneman & Riddle, 2005).

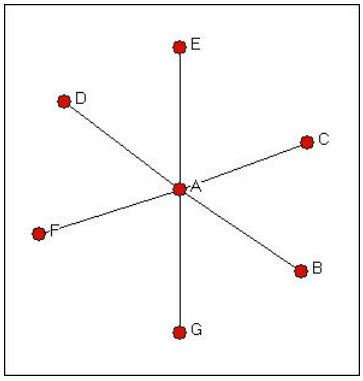


Figure 4.2. "Star" network

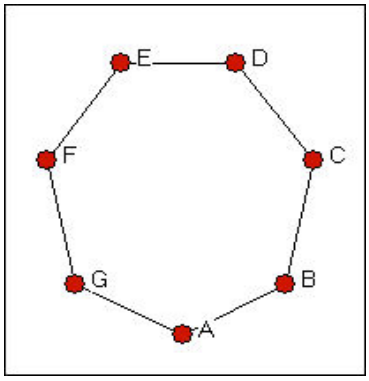


Figure 4.3. "Circle" network

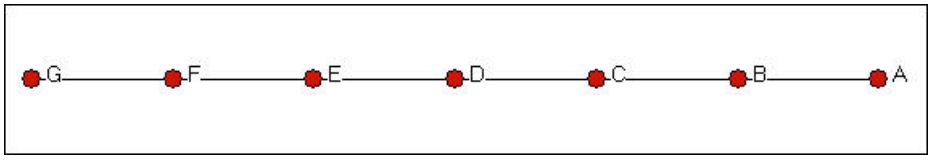


Figure 4.4. "Chain" network

The "star" network is the most centralized: the actor in the middle (actor A) clearly dominates the other actors on all levels of centralization (i.e. degree, closeness, and betweenness centralization indexes are equal to 1). More specifically, actor A in the "star"

network has highest degree centrality (equal to 6, which is the number of her neighbors) because she has direct access to everyone else in the network, but also highest closeness and betweenness centrality, which means that she is not only closer to all other actors (she is at a geodesic distance of 1 from each one), but she is also the cut-point everyone has to go through to communicate with each other. As mentioned, depending on the type of relational tie, being in the position of actor A may be good, because she has most choices and can manipulate relationships at her advantage, or bad, because she is most visible and easier to be reached. Additionally, elimination of the central node would cause the network's disruption, as the remaining members would be disconnected.

Figure 4.3 illustrates the "circle" network, which is the least centralized of all three structures: there is no prominent actor and, in fact, all nodes are equal in terms of their structural position. Each actor is directly connected to two actors (degree equal to 2), and although each one has a different geodesic distance from all others (e.g., A is at geodesic distance of 1 from B, 2 to C, 3 to E, etc.), the closeness centralization index is 0, i.e. all actors have identical distributions of closeness. Similarly, betweenness centrality is equal for everybody, as each actor lies on the path between two different actors. A decentralized structure is less efficient in the short-run than a centralized one, because it is more difficult for information to flow within the network. However, it provides increased security and efficiency in the long-run: even if one of the nodes were to be eliminated, information would still flow in the opposite direction of the missing node.

The "chain" network in Figure 4.4 presents a more diversified situation. Degree centrality is equal for all except for the two actors at the extremes (i.e., actor A and G who have a degree of 1 instead of 2). The middle node (actor D) lies on the shortest path between pairs of actors with similar positions (C-E, B-F, and A-G), and is also a broker between the two sets A-B-C and E-F-G. Therefore, if this were a communication exchange

network, we could argue that nodes A and G are at a more disadvantaged position compared to node D. However, if this was a terrorist network instead, we could see the advantages of such a configuration or shape, which allows for keeping members separate and insulating actors who need enhanced protection (e.g., the hijackers in Kreb's reconstruction of the 9/11 attacks network).

4.3.3 Statistical network modeling

Although a large number of network studies are exploratory and aim to simply visualize underlying structures or algebraically compute network properties, recent advances in statistical modeling allow for a more in-depth approach to the study of network characteristics (Knoke & Yang, 2008). As previously mentioned, conventional statistical methods are not appropriate with network data because these are not normally based on independent observations (Pattison & Wasserman, 1999; Robins & Pattison, 2005; Wasserman & Pattison, 1996). Previous studies applying conventional inferential formulas (e.g., regression analysis) using network properties, such as density or actor centrality, as predictor or outcome variables are likely to be inaccurate as they violated or, at the least, openly ignored basic statistical assumptions (Shumate & Palazzolo, 2010). Drawing conclusions from such analyses is dangerous "because the non-independence of network observations will usually result in under-estimates of true sampling variability – and hence, too much confidence in our results" (Hanneman & Riddle, 2005).

Exponential random graph models (ERGM), also called p* class models, were developed to provide reliable modeling techniques taking into account the unique characteristics of social networks and explaining the presence of interdependent dyadic ties

as a function of structural and attribute factors (Robins et al., 2007a; Robins & Pattison, 2005; Wasserman & Pattison, 1996). As pointed out, "social behavior is complex, and stochastic models allow us to capture both the regularities in the processes giving rise to network ties while at the same time recognizing that there is variability that we are unlikely to be able to model in detail" (Robins et al., 2007a, p. 174).

The logic behind these statistical models is that network ties between pairs of actors form through a stochastic (i.e. probabilistic) process as a result of the presence or absence of other relational ties as well as certain network or actor attributes (Wasserman & Robins, 2005; Robins & Pattison, 2005). In this sense, relational ties between actors are considered random variables that are modeled based on certain assumptions concerning their dependencies. In other words, "the network is conceptualized as a self-organizing system of relational ties. Substantively, the claim is that there are local social processes that generate dyadic relations, and that these social processes may depend on the surrounding environment (i.e. on existing relations)" (Robbins et al., 2007, p. 177).

All exponential random graph models can be described by the following formula:

$$Pr\,(Y = y) = \left(\frac{1}{k}\right) \exp\ \{\sum_A nA\ gA(y)\}$$

which estimates the probability that a given network y is a function of the summation of non-zero parameter nA with corresponding network statistic $gA(y)$ over all configurations , where $1/_{\mathrm{k}}$ is a normalizing factor that ensures that the probabilities sum to 1 (for more details on the mathematic explanation of this formula see: Robins et al., 2007a; Snijders, 2009).

ERGM models allow to test whether certain structural characteristics are significantly more prevalent in an observed network than it would occur by chance (Shumate & Palazzolo, 2010). In a certain way, this procedure resembles that of logistic

regression, as the model estimates the probability to observe the represented graph with certain network statistics and non-zero parameters chosen using a "plausible and theoretically principled" process (Robins et al., 2007a, p. 175; Wasserman and Pattison, 1996).

In the past two decades, statisticians have proposed various methods for random graph models estimation (Frank & Strauss, 1986; Pattison & Wasserman, 1999; Wasserman & Pattison, 1996). Currently, the preferred option involves the use of Markov Chain Monte Carlo Maximum Likelihood Estimation (MCMCMLE), because it produces more reliable standard errors than pseudolikelihood estimations (Wasserman & Robbins, 2005). The procedure involves running computer simulations that produce a distribution of random graphs from a starting set of parameter values (decided by the researcher) and subsequently estimating and refining the parameters by repeating these simulations until the model is stabilized (for a detailed description of mathematical procedures, see: Robins et al., 2007a; Snijders, 2009). To conduct this statistical analysis, we used PNet software program, which was developed by Wang, Robins, and Pattison (2004 & 2009) for simulation and estimation of Exponential Random Graph (p*) Models.

The choice of parameters, which can represent both structural and attribute characteristics found in a social network, is an important step in positing an exponential random graph model (Robins, Snijders, Wang, Handcock, & Pattison, 2007). Parameters can be as simple as a single tie (i.e., arc in a directed network, edge in an undirected network), used to estimate the role of connectivity or density in a social network, to more sophisticated structural configurations, as described below. Recent studies modeling complex graphs suggest the use of so-called higher-order parameters, i.e. resulting from a combination of simpler configurations, to fit empirical network data (Robins et al., 2005; Snijders, Pattison, Robins, & Handcock, 2006). One of the major benefits of including higher-

order parameters in a random graph model simulation is that it may help overcome the problem of model *degeneracy* or *near degeneracy*, which occurs when the model estimation can only find networks that are nearly complete (i.e., density is nearly 1, which means all nodes are connected) or nearly empty (i.e., density is almost 0, indicating that no ties are found; for more detailed information on these issues, see: Handcock, 2003; Harrigan, 2009).

To test our research hypotheses, we selected four structural parameters, i.e.:

- Edge. At the very minimum, an exponential random graph model for non-directed graphs must include this parameter, which indicates the likelihood that a tie exists between pairs of actors and provides a measure of density and cohesion (Shumate & Palazzolo, 2010). If the *edge* parameter is significant and positive, it may be interpreted as a tendency of the network to display more relational ties than observed by chance. On the opposite, a significant and negative parameter indicates lower connectivity among network members than expected by chance. With regard to criminal networks, a negative parameter would indicate that suspects cooperate with only a few of the potential accomplices in the network (Malm et al., 2010).
- Alternating *k*-stars. This is one of the new higher order parameters (i.e. including configurations of more than three nodes) developed by Snijders et al. (2006) to prevent model degeneracy, and is used to measure degree distributions. In Markov Chain Monte Carlo maximum likelihood estimation models, *k*-star refers to an undefined possible number of star values (e.g. 2-star, 3-star, 4-star, etc.). If the alternating *k*-star parameter is positive and significant, it indicates the presence of some higher degree nodes ("hubs") and the tendency to display centralized or "core-periphery" structures as a result of the popularity of these hubs. On the opposite, if the parameter is significant and negative, this suggests the absence of centralized actors and the tendency to have less variance in node degree distribution (Robins et

al. 2007b). In other words, the higher the *k-star* statistics, the easier it is for communication to flow across network nodes. However, highly centralized structures may also be more vulnerable to external attacks, as central actors are more easily reached and, therefore, less protected (Malm et al., 2010).

- Alternating *k*-triangles. This higher-order parameter measures the presence of triangular relationships within a given network, also called *triangulation* or *transitivity* effects, exemplified by the expression "friends of my friends are my friends" (Boissevan, 1974). Triangles are network structures that include three actors. A triangular or transitive effect describes the tendency of node A, who is linked by some relational tie to node B, to become associated with node C, who is also linked to node B, as a result of the tie between A and B (Robins et al., 2007b). The alternating *k*-triangles parameter is useful to identify cohesive subsets, i.e. denser areas that are lumped together in the network (e.g. clusters or cliques). If this parameter is significant and positive, it indicates a tendency toward clustering and possibly a core-periphery structure as a result of overlapping cliques. Unlike for alternating *k*-star statistic, however, this is related to triangulation effects rather than degree distribution. This is an indication of strength but also closure, as information exchanges are more difficult.
- Alternating *k*-two paths. This configuration can be thought of as a triangle without the base and is an indicator of flexibility in the network (Snijders et al., 2006). This lower-order parameter is usually interpreted in conjunction with the *k*-triangles parameter, and it was in fact formulated to distinguish between typical triangulation processes that tend to transitive closure (i.e. formation of a clique between three nodes) from more flexible clustering processes that may precede them. Positive values of this parameter indicate a tendency toward 4-cycles in the network (i.e.

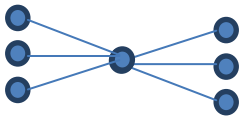
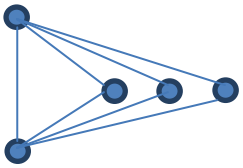
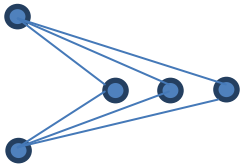
sets of four individuals maximally connected among each other, similar to the "chain" network described in Figure 4.3 above). This means that all actors are equal in terms of their structural position; hence, even if one were to be eliminated, this would not fatally affect the network (Malm et al., 2010).

In addition to measuring structural parameters, PNet allows to test the impact of actor attribute variables on network structures (Robins et al., 2001). This is a significant development, considering that in social selection processes "actors create or alter ties on the basis of the attributes of other actors; that is, actor attributes may contribute to the formation or change of network ties" (Robins & Pattison, 2005, p. 205). For example, theories based on the concept of *homophily* argue that individuals who share similar characteristics (e.g. same racial background) tend to become associated through some form of relational tie (e.g. friendship) more easily than individuals who are completely different (Robins et al., 2001; Wimmer & Lewis, 2010).

One of the advantages of ERG modeling is that it allows for simultaneously analyzing all configurations of interest, i.e. both structural and attribute parameters (Shumate & Palazzolo, 2010). To test Hypotheses 2 and 4, we added one binary actor to the four structural parameters discussed above, i.e. "suspect status" (0=non-extremist; 1=political extremist) to determine whether network structures were influenced by the presence or absence of relational ties between political extremists, i.e. far-right and Islamic extremists, and their non-extremist accomplices (homophily vs. heterophily effects). This dichotomous variable was obtained by recoding the strength of association variable, which measured the suspect's level of ideological involvement on a 4-point scale (i.e., 0=non-extremist; 1-4=extremist).

The table below summarizes structural and attribute parameters and configurations used in our ERGM analysis.

Table 4.4. Structural and attribute parameters for ERGM of financial extremist networks

	Configuration	Description
Structural Parameters		
Arc/Edge		Density, connectedness
Alternating *k*-stars (Alt-*k*-stars)		Centrality, core-periphery as a result of actor popularity
Alternating *k*-triangles (Alt-*k*-triangles)		Clustering, core-periphery as a result of transitivity, strength
Alternating *k*-two paths (Alt-*k*-2-paths)		Precondition for transitivity, flexibility
Attribute Parameters		
Homophily		Tendency to select associates with similar trait
Heterophily		Tendency to select associates with opposite trait

4.4 Methodological challenges and proposed solutions

There are a number of limitations related to the research design, data collection and analytical method used in this dissertation, which deserve to be further discussed and monitored. First of all, there is a possible selectivity bias related to the use of open sources for the identification of relevant cases and creation of the database. Because we rely on open sources to identify our study universe, our final data set might be biased, as publicly available cases retrieved through these sources may not accurately represent the general population of existing cases. For example, governmental agencies may have their own agenda in publishing cases that are especially extreme or have a higher public resonance. Similarly, watch-group publications might be especially keen on certain political issues and therefore publicize specific cases over others. In other words, we might be missing cases in a non-random way as a result of the partial data collected from the available sources.

As Chermak and colleagues point out, it is of utmost importance that social science researchers investigate the nature and quality of their data before undertaking sophisticated statistical analyses. In fact, "the application of any statistical method is only meaningful when researchers understand the strengths and weakness of their data source so that caveats can be explained and errors corrected" (Chermak, Freilich, Parkin, & Lynch, 2011, p. 1). To control for this problem, we put extra care in the identification process phase making sure that no case was left out. We drew our initial pool of cases from U.S. DOJ press releases, which publish criminal cases under federal investigation and prosecution on a monthly basis, and reviewed a variety of other sources that provide information on financial criminal cases, e.g. other official agencies websites (FBI, IRS, U.S. Treasury) and watch-group publications. We also reviewed extensively terrorism databases (i.e., ATS, GTD) and terrorism cases lists created by human rights organizations and watch-groups (e.g. NYU

Terrorism Trial Report Card, Human Rights First, NEFA Foundation, etc.). During the data collection process, we continued monitoring these websites and further updated our initial list with any new case we subsequently identified.

Another problem which may affect our data is related to the fact that multiple research assistants were involved in the open-source searching and coding process, introducing non-sampling errors related to inter-coder reliability. To prevent this problem and improve the quality of our data set, once the coding process was complete, we double-checked each single case by conducting follow-up searches using the Internet web engines mentioned above and editing the final dataset accordingly.

There are also specific methodological issues related to the use of social network analysis and the problem of missing data. This problem is common in network designs that involve non-survey research to construct the networks (Morselli, 2009; Malm, 2007). Archival network data are generally considered "safer" than survey and questionnaire data, which may suffer from self-report perception biases and respondents' flawed memory (Marsden, 2005). However, because of the variety of sources used for data collection and their different degrees of accuracy, information concerning network members and their relationships will necessarily constitute only a partial view of their true social networks.

These issues have been dealt with previously by network researchers, who treated them from the perspective of missing data *beyond* and *within* the parameters of the final network representation (Morselli, 2009). Missing data beyond the final network representation goes back to the boundary specification problem, which represents one of the biggest challenges for social network researchers (Laumann et al., 1992; Kossinets, 2008). Once the parameters of a setting are established, it is hard to assess the extent to which actors interacting within those parameters are missing. This is especially true for criminal networks, as they have "fuzzy" boundaries by definition and are also sensitive to

fluctuations related to the presence of unknown accomplices, individuals with false identities or "aliases" (Sparrow, 1991).

To limit the number of missing nodes, it is crucial to collect information as accurately as possible. Sageman (2004) created a scale of sources reliability to construct Islamic terrorist networks from open sources, favoring "transcripts of court proceedings subject to cross-examination, followed by reports of court proceedings, then corroborated information from people with direct access to the information provided, uncorroborated statements from people with that access, and finally statements from people who had heard the information secondhand" (2004, p. 65). Morselli (2009) argues that the accuracy of data compiled from criminal justice sources depends on the criminal justice stage from which they are extracted. Data obtained from general law enforcement monitoring activities are considered the least accurate, whereas data that are confirmed by a guilty verdict are arguably the most accurate. The degree of accuracy therefore increases when one moves from investigations to prosecutorial and adjudication activities. On the other hand, Kossinets (2008) maintains that researchers should look closely at the early stages in the investigation as key actors may be lost during the course of criminal proceedings because of strategic choices by public authorities.

This study uses criminal indictments as the primary sources for identifying network participants. Similarly to what Morselli did, we also examined documents from previous and subsequent stages of criminal proceedings to identify missing nodes and eventually eliminate those who fell out of the net. In addition, we consulted a variety of non-CJ open sources to supplement this information (including newspaper articles, government reports, watch-group publications, scholarly works, etc.) and detect additional individuals. This approach is consistent with previous research. Krebs (2002a), for instance, collected data on the 9/11 hijacking network using the Google search engine. Our research makes a step

forward in this sense, since we increased the number of web engines used from one to twenty-six. Importantly, in our research we did not focus solely on criminal suspects but also collected information on any individual who appeared to be connected to a primary suspect and contributed to the financial scheme. As recent research shows, boundary specification is improved by including multiple relational types, allowing for capturing the wholeness of a "dark" network beyond the narrow criminal justice focus (Laumann, et al., 1992; McGloin, 2005; Malm et al., 2010).

The problem of missing data within the final network representation refers to possible missing links in the network. Once a final set of participants is selected for inclusion in the network, the question becomes to assess how accurate these relational data are with respect to the actual connections among members. This problem is especially important for the study of covert networks, as even minor changes in graph configurations may affect network- and actor-level properties (Krebs, 2002b). Morselli suggests (2009) to measure the density of various networks and compare them with results from past research in this area, although such comparisons are in fact difficult, as there are not many studies focusing on criminal networks. On the other hand, Sparrow (1991) argues that network-level measures such as density, radius, and diameter, are unreliable because they are especially affected by missing data. As an alternative, he suggests referring to actors' betweenness centrality, which he considers the most useful measure for criminal networks. In this study, we will examine density and betweenness centrality measures comparing our findings with those of previous studies to ensure these results are consistent with this body of literature.

CHAPTER 5. COMPARING FINANCIAL SCHEMES AND SUSPECT CHARACTERISTICS

Following the multi-step procedure described above to identify our study population, we found 38 judicial cases involving at least one political extremist (far-rightist or Islamic extremist) indicted for a financial offense by U.S. federal courts in 2004. Using the judicial cases as our starting point, we generated a list of 109 suspects indicted in 2004 for their participation in one (or more) of 44 financial schemes. We subsequently identified 55 additional suspects, who were indicted either before or after 2004, and 10 related schemes that were included in the dataset to have a complete picture of the suspects' criminal networks. In total, our universe consists of 54 financial schemes and 164 unique suspects[7]. The figure below illustrates the various steps in the identification of our study universe.

[7] It is important to notice that some of the suspects were involved in multiple schemes. Therefore, we created multiple data files to analyze unique suspects' characteristics (e.g. demographics, network ties) as well as attributes related to their participation in multiple schemes (e.g. techniques used, trial outcomes, imprisonment terms, etc.).

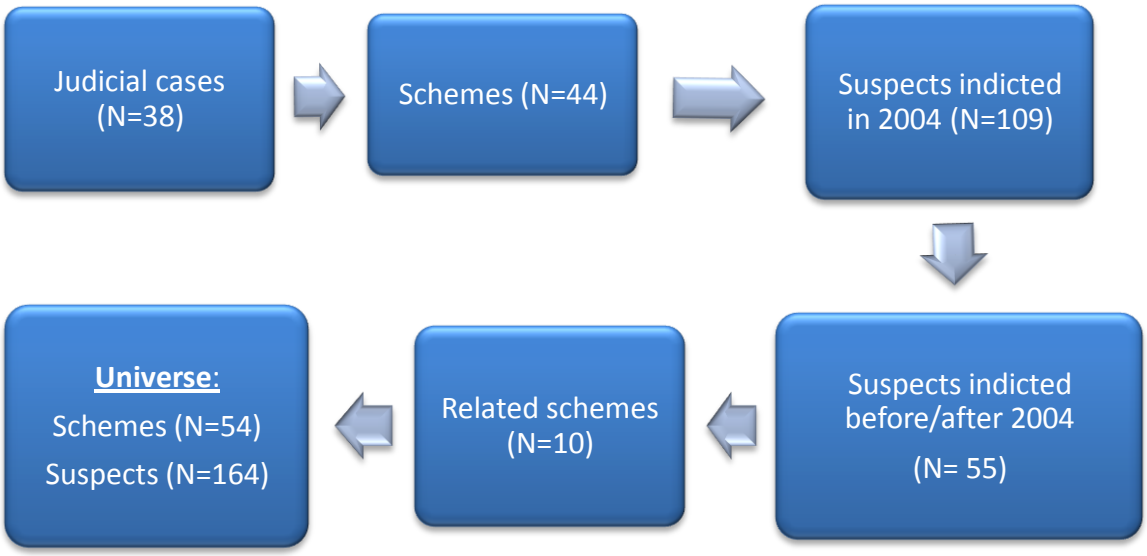


Figure 5.1 Study Universe – Judicial Cases, Suspects and Schemes

This chapter provides a descriptive analysis of financial schemes and suspects' characteristics using data collected in the ECDB. Specifically, we addressed the first three questions proposed in this research, i.e.:

1. What are the characteristics of financial schemes involving political extremists and profit-driven offenders in the US, and what criminal offenses are they associated with?
2. What are the characteristics of prosecuted individuals, and are there any differences or similarities between political extremists and non-extremist offenders?
3. What are the techniques used to carry out these schemes, and are there any differences or similarities in the *modus operandi* followed by political extremists and non-extremists?

First, we examined scheme-level attributes comparing across ideologies, i.e. between schemes perpetrated by far-rightists and those involving Islamic extremists. We also looked at the specific criminal offenses charged by federal prosecutors in the indictments. Next, we focused on the characteristics of prosecuting suspects comparing political extremists' attributes with profit-driven offenders'. In the following section, we compared techniques used by political extremists and non-extremist suspects in the context of specific scheme types. In conclusion, we discuss issues related to the quality of open-source information identifying possible biases which may affect our study findings. This final discussion is especially important as it provided direction for our subsequent network analysis.

5.1 Financial schemes and criminal offenses

5.1.1 Scheme-level attributes

Our study universe includes 54 financial schemes involving political extremists (either far-rightists or Islamists) and non-ideologically motivated suspects prosecuted in or around 2004. Each scheme was identified as either far-right or Islamic-related, since we did not find any scheme where both extremist types were present. Because our universe is not based on random sampling procedures, it is not possible to advance any generalizations at the scheme level. However, the descriptive findings still provide an interesting picture and offer useful insight for future research. In the table below, schemes' characteristics are presented and compared across ideologies.

Table 5.1 Scheme Attributes

	Total		By Ideology			
			Far Right		Islamic Extremist	
	N	Percent	N	Percent	N	Percent
Financial schemes	54	100.0	26	48.1	28	51.9
Scheme Type						
Tax avoidance	24	46.3	23	92.0	1	8.0
Money-dirtying	11	20.4	0	0.0	11	100.0
Money-laundering	7	11.1	1	16.7	6	83.3
General fraud	5	9.3	0	0.0	5	100.0
ID fraud	5	9.3	1	20.0	4	80.0
Pyramid	2	3.7	1	50.0	1	50.0
Length (months)						
Min-Max	2-233	---	8-195	---	2-233	---
Mean (SD)	65 (50)	---	69.5 (41.4)	---	61 (57.4)	---
Geographic scope						
Local	30	55.6	20	66.7	10	33.3
International	24	44.4	6	25.0	18	75.0
Single/multiple suspects						
Single	19	35.2	11	57.9	8	42.1
Multiple	35	64.8	15	42.9	20	57.1

As the table shows, a little over half of the financial schemes in our universe were committed by Islamic extremists (28, or 51.9 percent), while the other half involved at least one member of the domestic far right (26, or 48.1 percent).

Comparing scheme types immediately highlights striking differences across ideologies. In the study period under consideration, supporters of the domestic far right engaged in the majority of tax avoidance schemes (92 percent of cases compared to merely 8 percent Islamic-related). This finding is consistent with the extant literature on the American far right and its involvement in financial crime, which is often associated with the tax protest movement and so-called "paper terrorism" (ADL, 2005; de Armond, 1996;

Levitas, 2002; McNab, 2010; Pitcavage, 1996 & 1999; Sanchez, 2009). As the literature points out, these schemes include various kinds of activities, which range from simply cheating on taxes to elaborate operations to devise the illegality of the scheme (Belli & Freilich, 2009). Examples include the use of abusive tax shelters, exempt organizations, and strategies based on misinterpretations and distortions of federal tax obligations. We shall return to the various tax-avoidance strategies later in this chapter.

The remaining three far-right schemes involve one money-laundering operation, one pyramid scam, and one identity fraud case. As previously discussed, money laundering is the conversion of illicit incomes into assets that cannot be traced back to the underlying criminal activity that generated them (Reuter & Truman, 2004). Identity fraud (or ID fraud) occurs when someone assumes another person's identity to perform a fraud or other criminal act. Investment schemes, such as Ponzi or pyramid schemes, are based on the promise of high rewards to individuals or companies who invest their money in various high- or (allegedly) low-risk activities. The low incidence of non tax-related schemes does not allow for further discussion of these findings. Additionally, it is possible that they were committed because they were instrumental to tax avoidance schemes (e.g. money laundering is by definition a predicate crime committed to reinvest illicit revenues, in this case from tax evasion). Hence, we can argue that, with respect to the time period under consideration, tax avoidance was the prevalent scheme type among far-rightists.

Scheme types involving Islamic extremists appear to be more diversified. Consistently with the terrorism financing literature, we found a majority of money-dirtying and money-laundering schemes, followed by fraud-related ones (respectively 39.3 percent, 21.4 percent, and 17.8 percent of the total 28 schemes; see deKieffer, 2008; Masciandaro et al., 2007; Picarelli & Shelley, 2007). As noted, money-dirtying is similar to money laundering as they both require the use of diversion mechanisms to transform revenues

from illegal to legal, or *vice versa*. There are, however, two important differences: (1) the source of the money, i.e. criminal in the former, either legitimate or criminal in the latter; and (2) the goal of the financial operation, i.e. transforming "dirty" money into expendable income as opposed to channeling funds of any origin to individuals or groups to enable acts of terrorism.

Both money laundering and money dirtying presuppose the existence of precedent activities (either criminal or legitimate) which generated illicit capital to be "cleaned" or "soiled". Research on money laundering and terrorism financing shows that predicate acts may include theft and trade diversion (e.g. theft of over-the-counter pharmaceuticals, infant baby formula, computer hardware and other "hot" products which are then sold at higher prices), smuggling of contraband goods (e.g. cigarettes, counterfeit drugs, etc.), and drug trafficking (deKieffer, 2008; Shelley & Melzer, 2008).

Money dirtying, on the other hand, is often associated with fund-raising practices by militant activists collecting donations at religious centers (e.g. mosques) or through non-profit charitable organizations. Muslim charities in the U.S. and overseas have been accused of providing funds to terrorist groups, especially to Hamas and al Qaeda. The prosecution of such charities, which frequently does not end in actual convictions, has been the subject of heated controversies in the public and among researchers (Gunning, 2008; Hardister, 2003; McCulloch & Pickering, 2005; Passas, 2007; Warde, 2007). We provide more insight into these issues in the next sections examining criminal charges and techniques allegedly used in the context of such schemes.

To have a sufficient number of cases for comparison purposes, we created the "general fraud" category by including financial schemes committed by Islamic extremists through the use of deception that did not fall under any of the previous categories. Examples include: mortgage fraud, where the intent was to materially misrepresent or omit

information on a mortgage loan application to obtain a loan; insurance fraud, which involves acts committed to fraudulently obtain payment from an insurer; and food stamp fraud, which involves the intentional misrepresentation, concealment or withholding of information in order to get public assistance or food stamp benefits (Doig, 2006; Kim, 2007; IRS 2006 & 2008; Levi, 2003; Nelken, 2002).

Financial schemes coded in our database varied considerably both in time duration (from two months to almost twenty years) and geographic scope. In terms of scheme length, however, there were no significant differences between far right and Islamic cases. On average, a financial scheme took up to five years from start to end. The shortest Islamic scheme lasted only two months compared to eight months in the case of the far right. Some of the longest ones went on for several years – up to fifteen if involving Islamic extremists and twenty for the far right. As for their geographic scope, most schemes were committed within U.S. borders: 55.6 percent were domestic compared to 44.4 percent international. Not surprisingly, Islamic extremists, who oftentimes include Diaspora communities maintaining contacts with their origin country, were responsible for the majority of the latter type (75 percent).

Consistently with the criminology literature on co-offending patterns (Felson, 2003; Reiss, 1986; Warr, 2002), our data indicates that the majority of schemes involved two or more suspects (64.8 percent). It is interesting to notice that cases involving only one suspect were more common among far-rightists (57.9 percent) than Islamic extremists (42.1 percent). This finding provides support to the notion of "lone-wolf terrorism", which has gained substantial attention in recent years in the United States and overseas but has never been associated with non-violent ideological manifestations (Dishman, 2005; Johnston & Risen, 2003; Spaaij, 2010).

This argument should, however, be taken with caution, as suspects may in fact have benefited from interactions with individuals who provided some form of support but were not prosecuted, and therefore did not make it in our database as primary suspects. We further discuss this issue in the social network analysis section, where we examined all contacts the suspects had with individuals who contributed to the scheme. The presence of lone suspects involved in financial schemes further stresses the importance of studying informal networks to reveal underlying behavioral patterns which may refute existing theories about lone-wolf terrorism (Turk, 2004).

5.1.2 Scheme relevance and strength of ideological motive

As the literature points out, political extremists engage in financial crimes for a variety of reasons. American far-rightists refuse to pay taxes to express their ideological dissent against the U.S. government and its policies (Belli & Freilich, 2009; Pitcavage, 1996, 1999 & 2001; Sanchez, 2009). Others, like Al-Qaeda supporters, commit credit card fraud and money laundering to fund terrorist cells and prepare violent attacks (Kane & Wall, 2005; Hamm, 2007; Hamm & Van de Voorde, 2005; Horgan & Taylor, 2003; Picarelli & Shelley, 2005; Smith & Damphousse, 2003). Unfortunately, there is a lack of empirically sound research on these crime patterns. In this study, we make a first attempt at filling the gap by comparing goals and motives at the scheme- and suspect-level.

The ECDB captures scheme-level objectives through the "scheme relevance" variable, which refers to the function or purpose served by the scheme and distinguishes between: (a) schemes that were entirely driven by ideological or political grievances, either violent or non-violent; (b) schemes that were driven by non-ideological goals, i.e. profit or

greed; and (c) schemes that had a combination of greed and grievances, i.e. "hybrid" schemes. The table below provides univariate statistics on "scheme relevance".

Table 5.2 Scheme Relevance by Ideology

	Far Right		Islamic Extremist	
Relevance	**N**	**Percent**	**N**	**Percent**
Ideology/non-violent	20	77.0	0	0.0
Ideology/violent	0	0.0	12	42.9
Mixed profit/ideology	6	23.0	9	32.1
Pure profit/greed	0	0.0	7	25.0
Total	**26**	**100.0**	**28**	**100.0**

As expected, both far-right and Islamic-related financial schemes were, for the most part, ideologically motivated. However, they differed as regards the type of grievances expressed through such schemes, i.e. non-violent in the case of the far right (77 percent), violent for Islamists (42.9 percent). This is consistent with the literature. As noted, far-rightists who engage in financial crimes frequently do so as the ultimate form of anti-government protest, which usually (but not always) is limited to non-violent behaviors (Corcoran, 1990; Levitas, 2002; Sanchez, 2009). Their commitment to the cause is sometimes so strong that not even negative consequences such as criminal prosecution and conviction (and the financial hassle that comes with it) are able to stop them (Belli & Freilich, 2009; Pitcavage, 1999; Sanger-Katz, 2006).

Islamic extremists, on the contrary, commit financial crimes to raise funds for logistical or tactical purposes that are instrumental to violent crimes, e.g. as a form of self-sustainment for terrorist cells or to purchase equipment necessary to carry out a terrorist attack (so-called "preparatory acts"; see Smith et al., 2006). This should not be taken as an

indication that far-right extremists do not commit financial crimes in preparation of violent attacks. It simply suggests that, with respect to the study period here under examination, no such incidents were reported.

This point invites further speculation which should direct future research using a larger sample. It is possible that, at this particular moment in time, the American far right is not particularly active in planning and executing complex violent operations which require more substantial funding. In fact, as research shows (Freilich & Chermak, 2009; Freilich et al., 2009b), violent incidents involving far-right extremists frequently occur as "routine" acts, during internal fights or as random violence against occasional victims. Islamic terrorism, on the other hand, especially in its local manifestations (e.g. Hamas in Palestine, and Hezbollah in Lebanon) has been very active in recent years. This could justify the increased diversification of self-financing methods by militant activists residing in the United States.

Our descriptive analysis reveals another intriguing finding: profit was a key component in the commission of a number of financial schemes committed by both far-rightists and Islamic extremists. In 23 percent of far-right schemes and 32.1 percent of Islamic ones, the motivation was mixed. In other words, an ideological element was present (e.g. to sabotage the government or to support a terrorist group), but other motives were also at play. This finding is not surprising as it regards the domestic far right. Previous studies have indicated that people are sometimes drawn into the tax-protest movement because of the extra economic benefits for not paying taxes (Belli & Freilich, 2009; Sanger-Katz, 2006; SPLC 2001). Similarly, money laundering and other fund-raising activities by Islamic activists generate a stream of money which may be used to supplement their sources of income (Dishman, 2005; Shapiro, 2007; Shelley & Picarelli, 2005; Williams, 2008).

It is even possible that some far-rightists exploit the anti-tax rhetoric to justify their greed, as suggested by some experts (Pitcavage, 1999; Sanchez, 2009), although we find no support to this hypothesis in our data. We found, however, unexpected results concerning Islamic extremist schemes, as one out of four appeared to be non-ideologically motivated. This seems to provide support to the "convergence hypothesis" advanced by some researchers, who argue that not only methods but also motives driving political extremists and opportunistic offenders sometimes coincide (Makarenko, 2004; Shapiro, 2007; Williams, 2008). However, there may be different explanations which must be taken into consideration.

To better understand the role of ideology in the scheme commission process, we measured the "strength of ideological motive" for both far-right and Islamic-related schemes, using the scale described in the previous chapter, which assigns each scheme a value from 0 to 4 (with 0 being the lowest and 4 the highest) weighing evidence in favor and against the existence of ideological factors. The results are illustrated in the table below.

Table 5.3 Strength of Ideological Motive

	All Schemes		By Ideology			
			Far Right		Islamic Extremist	
	N	Percent	N	Percent	N	Percent
Strength of I.M.						
Min-Max	0-4	---	1-4	---	0-4	---
Mean (SD)	2.11 (1.2)	---	2.73 (1.0)	---	1.54 (1.2)	---
Value						
0	7	13.0	0	0.0	7	100.0
1	7	13.0	2	28.6	5	71.4
2	25	46.3	12	48.0	13	52.0
3	3	5.6	3	100.0	0	0.0
4	12	22.1	9	75.0	3	25.0
Total	**54**	**100.0**	**26**	**48.1**	**28**	**51.9**

First, we calculated the average strength for all financial schemes in our database and found that overall they had low ideological strength (M=2.11, SD=1.2). In only 22.1 percent of the schemes examined, ideology was paramount (i.e., had the highest score of 4). The majority fell in the medium-low range (46.3 percent had a score of 2). Next, we compared scheme strength by ideology and found some intriguing results. Ideological motives appeared to be stronger in far-right schemes (M=2.73, SD=1.0) compared to Islamic extremist cases (M=1.54, SD=1.2). In fact, the majority of far-right schemes scored between 2 and 4 (92.3 percent), whereas the opposite occurs with Islamic cases, which fell in the lower range (89.3 percent scored between 0 and 2).

As suggested before, these findings could be interpreted as positive evidence that the convergence hypothesis might hold true, especially as regards Islamic extremists who, despite their ideological status, seem to engage in financial crimes for reasons other than ideology. On the other hand, there may be something else going here that, unfortunately, we are not able to capture by simply looking at scheme-level variations. We shall return to this issue later in this chapter, when we compare suspects' ideological motives, and in the concluding section, when we address possible biases that may affect our findings.

5.1.3 Criminal offenses

In this study, we made a distinction between (a) financial schemes, (b) criminal offenses charged by prosecutors, and (c) techniques used by suspects to carry out the schemes. These three concepts are distinct but interrelated. Importantly, they allowed us to observe and compare different aspects of financial extremist criminality, and therefore improve our understanding of this complex criminal phenomenon.

As mentioned, financial schemes and criminal offenses do not always match. American prosecutors have extensive discretionary powers as regards their decision to initiate criminal proceedings as well as what charges to bring forth. Therefore, it is not unusual for prosecutors to use (and sometimes abuse) this power for strategic purposes, e.g. by overcharging initially and downgrading during the plea-bargaining stage (Heller, 1997; Gershman, 1999). In this section, we first look at criminal offenses in general, and subsequently focus on those charged in far-right and Islamic-related schemes. The figure below describes the federal offenses from the U.S. Criminal Code (U.S.C.) most frequently mentioned by public prosecutors in the initial indictments.

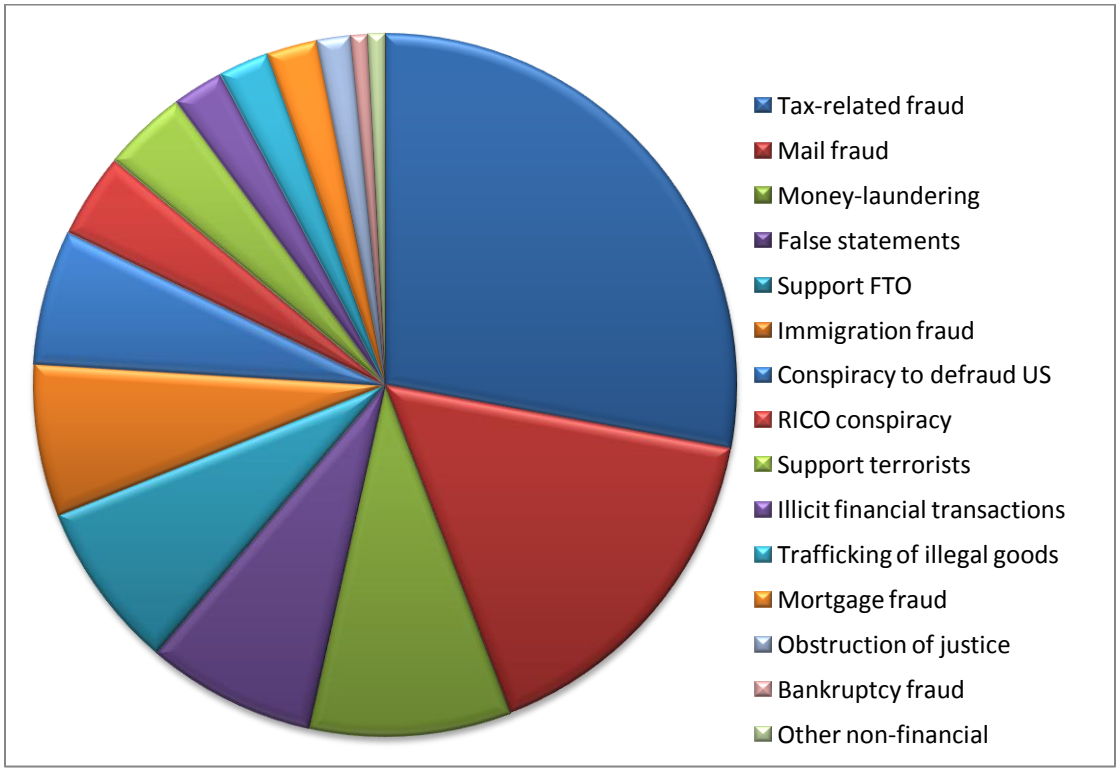


Figure 5.2 Criminal Offenses (N=129)[8]

[8] For this analysis, we used criminal offenses mentioned in scheme indictments as the unit of analysis. However, it must be noted that this does not represent the actual number of charges in the indictment, as it was not

The federal offense that was charged most is tax-related fraud (28 percent), which includes both proactive behaviors (e.g. tax evasion; see U.S.C. Title 26, Section 7201) as well as omission cases (e.g. failure to file an income report; see U.S.C. Title 26, Section 7203). The latter type corresponds to a typical far-right strategy that involves the use of "common-law" arguments and techniques to avoid tax liability, such as filing frivolous complaints to federal courts claiming to be "sovereign citizens" (Belli & Freilich, 2009). We talk about this and other anti-tax techniques in the next section.

In addition to tax fraud, federal prosecutors charged other typical financial offenses in different measures: mail fraud (16 percent), which refer to fraudulent activities perpetrated by using various financial transfer systems, including the postal service, bank wire transfers, and the Internet (see U.S.C. Title 18, Sections 1341-1346); money laundering (9 percent), which is defined as conducting a financial transaction with the intent to promote an unlawful activity "knowing that the transaction is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity" (see U.S.C. Title 18, Section 1956); and finally mortgage and bankruptcy fraud (2 percent and 1 percent).

Federal prosecutors made also use of terrorism financing statutes, specifically: providing material support to a specially designated foreign terrorist organization, or FTO (8 percent)(see U.S.C. Title 18, Section 2339B); providing material support to terrorists (4 percent) (see U.S.C. Title 18, Section 2339A); and dealing with the property of a specially designated terrorist, or SDGT (2 percent) (see Executive Order 13224, issued by President

---

possible to determine how many times a criminal offense was charged for each coded scheme because of missing values in our database. We remand this analysis to future studies.

George W. Bush on Sept. 24, 2001, which declared a national emergency after 9/11 and directed Treasury, in consultation with the Attorney General and Secretary of State, to take action to freeze designated SDGT assets subject to U.S. jurisdiction).

The "material support" formula has become one of the most powerful tools in the hands of public prosecutors involved in the post-9/11 war against terrorism, as it is sufficiently vague and broad to include a variety of activities, ranging from making donations to a charitable organizations, to participating in training camps overseas, and even providing translation services to alleged terrorists (Abrams, 2005; Chesney, 2005). Despite criticisms raised by civil rights activists and human rights organizations, this legislation was recently upheld by the U.S. Supreme Court (Barnes, 2010).

One case out of ten involved a conspiracy offense, i.e. conspiracy to defraud the U.S. government or its institutions (6 percent)(see U.S.C. Title 18, Section 371), and the famous RICO conspiracy (Racketeer Influenced and Corrupted Organizations Act), which has been used extensively to prosecute organized crime cases (i.e., Mafia) as well as a variety of other criminal acts carried out as part of an ongoing criminal enterprise (4 percent)(see Title 18, Section 1961).

Among the non-financial offenses charged by prosecutors we found: false statements (8 percent), which involves making or using materially false, fictitious, or fraudulent document entries in mortgage applications, health insurance claims, visa applications, etc. (see U.S.C. Title 18, Section 1001); immigration fraud (7 percent) (see Title 18, Section 1546); trafficking of illegal goods (2 percent), specifically contraband cigarettes, counterfeit pharmaceuticals, and stolen instant baby formula (Title 18, Sections 2342, 2315, 2320); obstruction of justice (2 percent); and one charge of attempted homicide.

In the figure below, we compare criminal offenses charged when prosecuting far-right and Islamic-related schemes. The differences are, once again, striking.

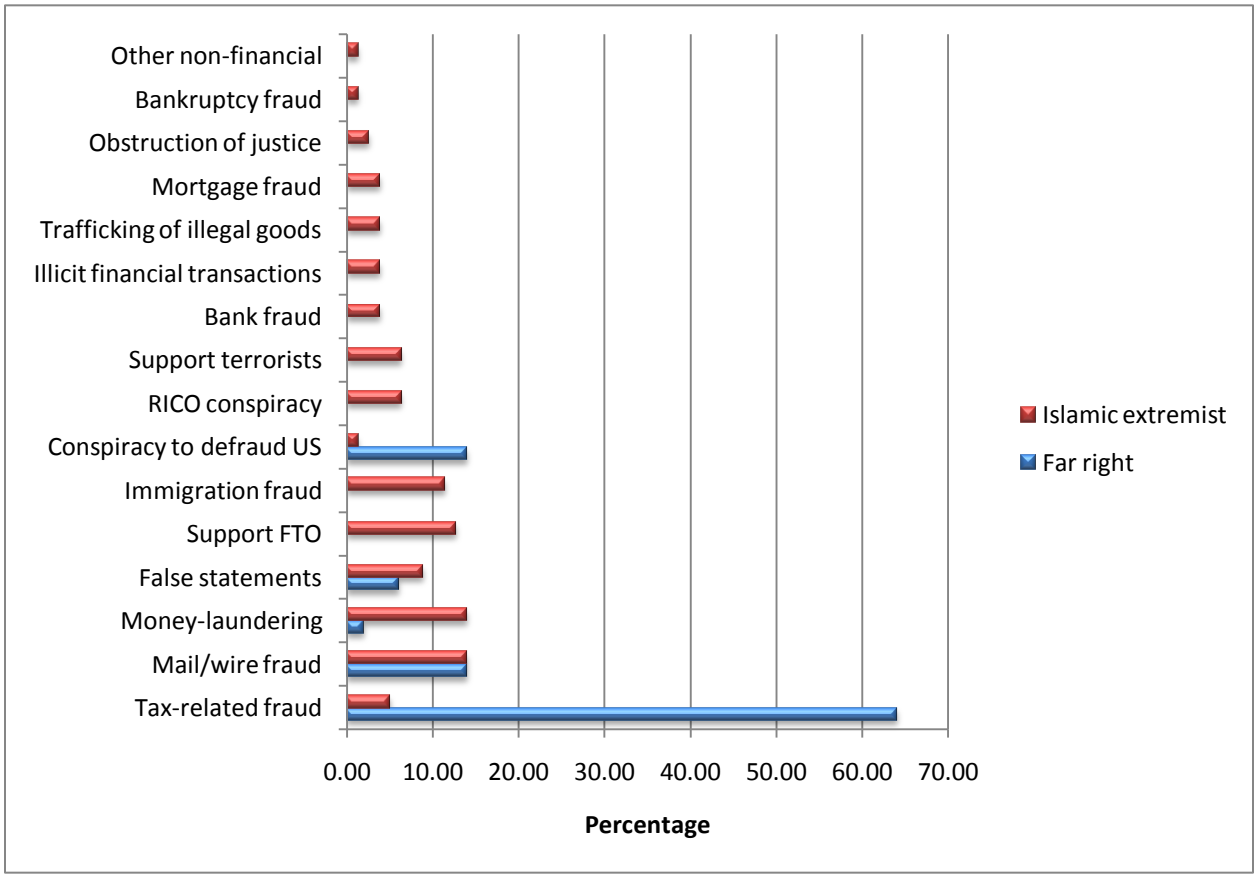


Figure 5.3 Criminal Charges by Scheme Ideology

Prosecutors in far-right cases charged typical financial offenses. The majority of schemes were prosecuted for tax fraud (64 percent), followed by mail and wire fraud (14 percent), conspiracy to defraud the US government (14 percent), false statements (6 percent), and money laundering in a small percentage (2 percent). Interestingly, the RICO statute was never used to prosecute far-right financial schemes. This finding is not consistent with Smith et al. (2002), who compared the prosecution of domestic and international terrorists and found that nearly one-third of charges against domestic terrorists involved racketeering conspiracy statutes. The reason may be related to the fact

that non-violent ideological crimes are usually not considered terrorism by U.S. courts (hence they end up prosecuted as regular white-collar crimes), unless the suspects are considered terrorist themselves (e.g., in the case of Islamic extremists). For future research purposes, it would be interesting to examine individual-level charges comparing far-rightists with Islamic extremists to test whether Smith et al.'s findings hold true in financial crime cases, as well as with non-extremist financial offenders to determine whether suspect ideological status plays any role in charging mechanisms.

The strategy used against Islamic extremists appears to be more diversified as federal indictments mentioned a variety of criminal offenses. Money-laundering and mail fraud were the offenses prosecutors charged most (each representing 14 percent of criminal offenses charged in Islamic extremist cases). Additionally, prosecutors made ample use of the USA Patriot Act legislation, which specifically targets terrorism financing, by applying the "material support" formula broadly (12.7 percent of criminal offenses involved "material support to a foreign terrorist organization", and 6.3 percent "material support to terrorists").

As previously noted, many have criticized the "material support" formula because it provide a "catch-all" solution that prosecutors use when they do not have sufficient evidence to charge more specific crimes. Interestingly, Islamic financial schemes were also prosecuted for violations of the RICO statute (6.3 percent of criminal offenses), which in many ways resembles the anti-terrorism legislation. Both infer "guilt by association", departing from the traditional legal notion of criminal intent and criminal act, and elude the principle of crime specificity by punishing a variety of unspecified illegal behaviors (Morselli & Kazemian, 2004; Naylor, 1997). The major difference between the two statutes is that the RICO conspiracy usually requires a criminal enterprise, whereas the material support formula can be used against single perpetrators. In future studies, it would be

interesting to further compare prosecutorial strategies looking at how these two legislations are applied to criminal cases involving political extremists.

Non-typical financial offenses were also utilized. In particular, immigration fraud (11.4 percent) and false statements in visa applications (8.9 percent) stand out. This is consistent with previous research on terrorism financing prosecutions, which found that prosecutors charge immigration-related offenses because they facilitate entry into the U.S. and access to jobs and social services (Kane & Wall, 2005). However, it has also been argued that alleged terrorism cases that were prosecuted because of immigration violations were simply not supported by credible evidence. In fact, some of these prosecutions were eventually challenged or dropped, "suggesting that at least some of the post-9/11 complaints may have been products of incorrect assumptions or hasty efforts to curtail terrorism" (Kane & Wall, 2005, p. 12).

In conclusion, we can say that prosecutorial strategies used in far-right cases appear to be very different from those applied in cases involving Islamic extremists. These differences may reflect the different scheme types far-rightists and Islamists were involved in, i.e. mostly tax-related the former as opposed to money-dirtying and money-laundering schemes the latter. However, there may also be other factors at play. For example, labeling suspects in terms of their ideological affiliation may have an impact on charging decisions. Far-rightists who engage in ideologically motivated tax fraud are not considered terrorists by the government, although experts define their actions as "paper terrorism" and some tax protesters have also committed violent attacks to further their cause (Beirich, 2004; Flynn & Gerhardt, 1995; Levitas, 2002; Pitcavage, 1998; Sanchez, 2009; SPLC, 2007). On the other hand, financial crime cases involving individuals who are allegedly linked to designated terrorists or terrorist organizations (even if the link is not proved beyond reasonable doubt) almost always end up being prosecuted for terrorism financing, although in practice

suspects may have simply cheated on their visa or mortgage applications. To shed light on these issues, it will be important to further examine and compare charges at the individual level using a larger sample. Additionally, comparisons should be made between cases prosecuted before and after 9/11, as the USA Patriot Act seems to have produced a new breed of terrorism cases that suffer from politicization of prosecutions. We shall come back to this issue later when we look at trial outcomes and sentencing decisions.

5.2 Extremist and non-extremist financial offenders

This section focuses on the suspects involved in the financial schemes examined above, comparing similarities and differences between far-rightists, Islamic extremists, and non-extremists. Because of our reliance on open sources, we can only provide summary statistics on some variables collected in the ECDB. Unfortunately, there were too many missing values in our data to describe important socio-economic and demographic characteristics (e.g. race/ethnicity, marital status, education, income, etc.) as well as variations in prosecutorial strategies at the individual level (e.g. criminal offenses charged and convicted with, etc.). The quality of open sources, in fact, varies greatly from case to case depending on a variety of factors, such as the complexity of the case (complex cases tend to be covered more and by multiple source types), media attention received (some cases raised national concern or popular protest, e.g. the prosecution of the biggest U.S.-based Islamic charity, "Holy Land Foundation", and were therefore more publicized than others), and the availability of court documents (e.g. criminal indictments, sentencing decisions, and trial transcripts), which tend to include more extensive information on

suspect demographics, criminal justice involvement, etc. We remand to this chapter's final section for a more in-depth discussion of these issues.

5.2.1 Suspect-level attributes

Our data set includes 164 suspects indicted by federal courts in or around 2004 for their involvement in a financial scheme. Among these, 56 (34.1 percent) appeared to be supporters of the domestic far right, 51 (31.1 percent) were identified as Islamic extremists, and the remaining 57 (34.8 percent) appeared to have no connection with any ideological movement. Therefore, our primary actors (or "nodes" in social network analysis terms) consist of two-third ideologically motivated individuals and one-third profit-driven offenders (or non-extremist suspects, as it should be better said in light of the findings reported below). The table below provides univariate statistics comparing characteristics of political extremists (far-rightist and Islamic) with non-extremist suspects.

Table 5.4 Suspects' Characteristics[1]

	Total		By Suspect Status					
			Far Right		Islamic Extremist		Non-extremist	
	N	Percent	N	Percent	N	Percent	N	Percent
Suspects	164	100.0	56	34.1	51	31.1	57	34.8
Gender	164	100.0	56	---	51	---	57	---
Female	27	16.5	17	63.0	0	0.0	10	27.0
Male	137	83.5	39	28.5	51	37.2	47	34.3
Age (at start)	123	75.0	39	---	43	---	41	---
Min-Max	17-69	---	27-67	---	22-54	---	17-69	---
Mean (SD)	38.80(12.4)	---	48.2(11.5)	---	33.8(7.9)	---	35.0(12.2)	---
Occupation	129	78.7	55	---	41	---	33	---
White-collar	17	13.2	13	76.4	2	11.8	2	11.8
Small owner	17	13.2	5	29.4	6	35.3	6	35.3
Top manager	14	10.9	6	42.9	6	42.9	2	14.2
Tax preparer	14	10.9	13	92.8	0	0.0	1	7.2
Promoters	12	9.3	4	33.3	0	0.0	8	66.7
Education	12	9.3	1	8.3	10	83.4	1	8.3
Blue-collar	8	6.2	1	12.5	6	75.0	1	12.5
Attorney	8	6.2	3	37.5	0	0.0	5	62.5
Accountant	7	5.4	1	14.3	1	14.3	5	71.4
Religious	5	3.9	0	0.0	5	100.0	0	0.0
Financial Advisor	3	2.3	0	0.0	1	33.3	2	66.7
Entrepreneur	3	2.3	3	100.0	0	0.0	0	0.0
Govt. employee	2	1.6	1	50.0	1	50.0	0	0.0
CJ-related	2	1.6	2	100.0	0	0.0	0	0.0
Other	5	3.9	2	40.0	3	60.0	0	0.0

[1] Excludes suspects with age and occupation unknown. Of the total 164 suspects, age was available for 123 suspects, respectively 39 far-rightists, 43 Islamic extremists, and 41 non-extremists; occupation was known for 129 suspects, i.e. 55 far-rightists, 41 Islamic extremists, and 33 non-extremists.

In total, there were 27 women (16.5 percent) who appeared to be either involved in the far right or non-extremist (respectively 63.0 percent and 27.0 percent). Based on these findings, no women associated with radical Islam participated in a financial scheme in the reference period. This is an interesting finding that will be discussed more in depth in the following chapter focusing on exploratory network analysis. It is well possible, in fact, that some of the non-extremist women were actually associated with Islamic extremist men by

marriage or kinship. Hence, women's participation in the execution of financial schemes by Islamic extremists should not be excluded *a priori* but further investigated taken into account their social network.

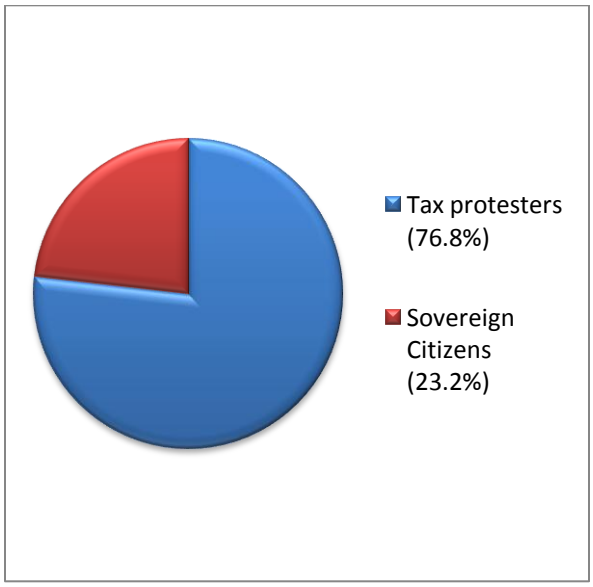
The average financial crime suspect was 39 years old when the scheme started or, alternatively, when she joined the scheme (M= 38.8, SD = 12.4). Islamic extremists appear to be comparatively younger (M= 33.8, SD=7.9) than non-extremists (M = 35.0, SD= 12.2) and far-rightists, who were the oldest (M= 48.2, SD=11.5). This is consistent with the American terrorism literature, which describes right-wing extremists as significantly older (usually over forty years old) than the average domestic left-wing and international terrorists (Smith, 1994).

Next, we compared employment types across suspect categories and discovered some interesting findings. As expected, white-collar jobs appear to be common among political extremists involved in financial schemes. Far-rightists held a variety of positions, ranging from low-level white-collar employee to top manager and business entrepreneur. In addition, many engaged in tax-related services, as expected considering their preference for tax avoidance schemes. This finding provides support to the "specialized access" argument theorized by routine activity scholars, which states that access to specialized professional knowledge may provide potential offenders with readily available opportunities for crime (Felson, 2002).

In addition to typical white-collar jobs, Islamic extremists were also employed in blue-collar jobs (e.g., cab drivers), small businesses (e.g., owners of tobacco shops and ice-cream parlors), and education or religious institutions (e.g. university professors, high-school teachers, computer tutors, and clerics, etc.). This diversity may be related to socio-economic and cultural factors (e.g., ethnic identity, immigration status, education level, religious involvement, etc.), which unfortunately we were not able to capture with our data.

Interestingly, among non-extremist suspects we found various types of professional experts, like promoters of business ventures, accountants, attorneys, and financial advisors. In accordance with this study's hypothesis, we could argue that their involvement in financial schemes is directly related to their professional expertise. This argument will be further developed when we examine the relational ties among all suspects involved.

Lastly, we focused our analysis on political extremists' group affiliation to better understand what ideological movements are involved in financial crime. As mentioned, our universe includes 107 political extremists, a little over a half identified as far-rightists (56, or 52.3 percent) and the other half as Islamic extremists (51, or 47.7 percent). The tables below illustrate group affiliation for far-right and Islamic extremists.



Figures 5.4 Far-right group affiliation

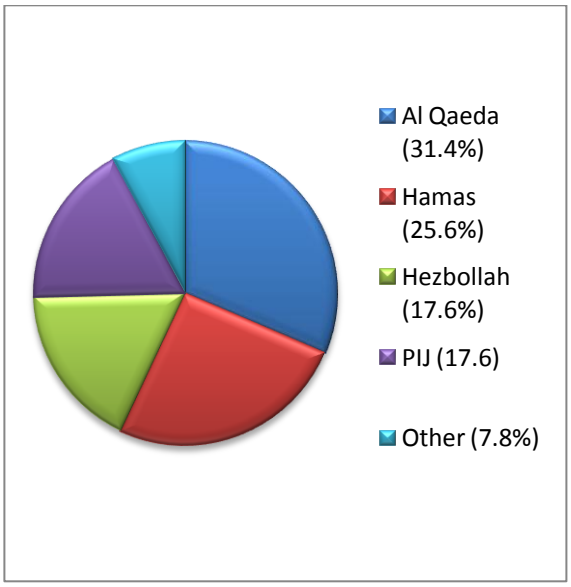


Figure 5.5 Islamic extremist group affiliation

All far-rightists in our data set were supporters of the tax protest movement, which is a fringe of the American far right that opposes the U.S. government in general and its tax regulations in particular. Some identified themselves as "sovereign citizens" (23.2 percent), i.e. they were members of loosely organized groups whose anti-government ideas originated in the 1970s in the context of the so-called Posse Comitatus. Sovereign citizens believe that everything the U.S. government is concerned with is illegal and unconstitutional, and therefore refuse to abide by any federal laws, including the duty to pay taxes, to use driving license plates, etc. (ADL, 2003 & 2005; McNab, 2010; Sanchez, 2009).

The majority of far-right extremists in our data set, however, did not identify with any specific sub-group, and appeared to be mostly concerned about the tax issue. This is an interesting finding that provides support to Chermak et al. (2009), who argue that "lone wolves or far rightists acting with others but not as part of an established group tend to commit […] non violent crimes (such as tax refusal and other financial crimes)".

As discussed in the literature review, the American far right is a complex socio-political movement which comprises a myriad of groups (e.g. Neo-Nazis, skinheads, tax protesters, Sovereign Citizens, Freemen, Patriots, anti-abortionists, etc.) holding different perspectives concerning religion (ranging from atheism to Christian Identity), racial (anti-Semitic, anti-black, anti-immigrant, etc.) and socio-economic issues (e.g. anti-gay, anti-homeless, anti-federal government, etc.). This diversity is also found in the criminal activities they engage in and the organizational structures in which they operate. To better understand the far-right movement, it is important to keep in mind these differences and further compare crime types across far-right sub-groups. According to Chermak, Freilich, and Shemtob (2009), this is the only way to improve counterstrategies, as different segments may represent different types of threats.

Islamic extremists appeared to be affiliated with various terrorist organizations. The ECDB Code Book makes a distinction between militant Islamic activists with a global or local focus: the first ones "are most concerned with combating the West in general and the United States in particular", whereas the second ones " are focused on a specific conflict such as Somalia; Russia/Chechnya; India/Kashmir; Israel/Palestine; China/Uighur; Philippines/Moro, etc.".

The majority of Islamic extremists in our data set were global jihadists inspired by Al-Qaeda (31.4 percent). According to Gunaratna (2002, p. 1), "Al Qaeda is the first multinational terrorist group of the twenty-first century" and [...] "a worldwide movement capable of mobilising a new and hitherto unimagined global conflict". As a terrorist organization, Al Qaeda has evolved considerably from its origins, and today comprises three segments: (1) the original Al Qaeda group, which has been severely weakened by the US invasion of Afghanistan; (2) the Al Qaeda network, composed of the original founders and a number of associates spread around Asia, Africa and the Middle East; and (3) Al-Qaeda inspired cells, present worldwide and constituting the modern global jihad movement which today "represents an even greater threat to the U.S. and its allies and friends than does the classic and more limited Al Qaeda behind the 11 September attacks" (Gunaratna, 2008, p. 49).

The remaining activists supported terrorist organizations with a local focus, i.e.: Hamas (25.5 percent), a religious and socio-political movement whose primary goal is to liberate Palestine from Israel through the "holy war" (or jihad); Hezbollah (17.6 percent), which literally means "Party of God", a Shiite terrorist organization with ties to Iran aiming at creating a fundamentalist Islamic state in Lebanon; and the Palestinian Islamic Jihad (17.6 percent), a terrorist group committed to the destruction of Israel and creation of an

Islamic state in Palestine, which is smaller and more militant than Hamas (Atran, 2003; Mishal & Sela, 2000; Norton, 2009) [9].

Although the ideological and religious foundation of these radical Islamic movements are similar (i.e. anti-Western ideals, Islamic fundamentalism, call for violent *jihad*, i.e. "holy war"), there are also important differences that need to be taken into account as they may impact their *modus operandi* and financing methods (Juergensmeyer, 2001). We remand these important group-level comparisons to future studies, as our small sample unfortunately does not allow for this type of analysis.

5.2.2 Suspects' motives and strength of ideological association

According to rational choice theory, crime is goal-oriented behavior aimed at maximizing benefits while minimizing costs (Clarke, 1980). To better assess similarities and differences between political extremists and non-extremist financial offenders, we examined suspect-level motives related to their involvement in financial crime.

Political extremists are traditionally distinguished from non-ideological offenders because of the different motivation driving their actions (or objectives they try to achieve): ideological for the former, profit-oriented for the latter. However, research shows that this distinction may be simplistic and even inaccurate (Belli & Freilich, 2009; Naylor, 2000; Shapiro, 2007; Shelley & Picarelli, 2005; Williams, 2008). For example, some far-right tax evaders appear to be driven by a combination of anti-government ideology and greed.

[9] It was not possible to determine group affiliation for four individuals identified as Islamic extremists (7.9 percent).

Similarly, Islamic militant activists have engaged in cigarette trafficking and money laundering to raise funds to support Hezbollah in Lebanon, but also to make money off of it.

Ultimately, knowing what specific objectives criminals or terrorists aim to may not have any bearing on what they actually do to reach them. This is in accordance with the SCP approach, which argues that to prevent crime we must intervene in the crime-commission process and change the opportunity structure rather than the criminal's mind (focus on objective rather than subjective elements; see Clarke & Newman, 2006). This analysis provided us with useful insight for our final discussion on SCP measures against financial extremist crimes.

Table 5.5 Suspect Motives[1]

	Total		By Suspect Status					
			Far Right		Islamic Extremist		Non-extremist	
Motive	**N**	**Percent**	**N**	**Percent**	**N**	**Percent**	**N**	**Percent**
Ideological	42	34.7	20	40.9	22	66.7	0	0.0
Profit	43	35.5	1	2.0	6	18.2	36	92.3
Mixed	33	27.3	28	57.1	5	15.1	0	0.0
Other	3	2.5	0	0.0	0	0.0	3	7.7
Total	**121**	**100.0**	**49**	**100.0**	**33**	**100.0**	**39**	**100.0**

[1] Excludes suspects with unknown motive. Of the total 164 suspects, individual motives were available for 121 suspects, specifically 49 far-rightists, 33 Islamic extremists, and 39 non-extremists.

The table above provides a comparison of motives across suspect categories, highlighting some interesting points. As expected, non-extremists had no ideological or political interest in the financial schemes they were involved in. Profit was the most important goal for most of them (92.3 percent), although other motives were also at play for

a small number of individuals (7.7 percent). Hence, to be precise, we should talk about non-extremist financial offenders rather than profit-driven criminals, as there may be other factors involved in their decision to engage in these criminal activities.

Political extremists presented a more diversified scenario. Islamic extremists were, for the most part, motivated by ideology (66.7 percent). However, a substantial number pursued other goals: in 18.2 percent of cases, the motivation was purely monetary, whereas in 15.1 percent it involved a mix of ideology and profit. This combination of motives is even more evident among far-rightists, whose motivation was mixed in the overwhelming majority of cases (57.1 percent) and purely profit-oriented in a small percentage (2.0 percent). These findings lend support the convergence hypothesis advanced by scholars who argue that differences between terrorism and profit-driven crime are more nuanced than what is commonly thought (Makarenko, 2004; Shapiro, 2007; Shelley & Picarelli, 2005; Williams, 2008). More research is needed to confirm this hypothesis, but the existence of such a diverse scenario in our study universe sheds light over a much-debated issue that has never before been addressed empirically.

Similarly to what we did for financial schemes, we also looked at the suspect's strength of ideological affiliation to compare variations in ideological intensity between far-rightists and Islamic extremists. This variable was especially important because it also served as a test for our "attitudinal criterion" to identify relevant cases to be included in our database (see above section on inclusion criteria). Accordingly, a case was included if at least one of the suspects was either a far-rightist or Islamic extremist by reporting any evidence found in the open-source materials in favor or against the suspect ideological

affiliation to, respectively, a far-right or Islamic extremist credo. The results of this analysis are presented in the table below[10].

Table 5.6 Suspect Strength of Ideological Association

	All Suspects		By Suspect Status			
			Far Right		Islamic Extremist	
	N	Percent	N	Percent	N	Percent
Strength of I.A.	107	100.0	56	34.1	51	31.1
Min-Max	1-4	---	1-4	---	1-4	---
Mean (SD)	2.8 (1.0)	---	3.1(1.0)	---	2.5(1.0)	---
Value						
1	10	9.3	5	50.0	5	50.0
2	42	39.3	11	26.2	31	73.8
3	15	14.0	14	93.3	1	6.7
4	40	37.4	26	65.0	14	35.0
Total	**107**	**100.0**	**56**	**52.3**	**51**	**47.7**

As previously noted with regard to scheme ideological strength, we found differences between far-rightists and Islamic extremists. On average, far-right suspects displayed a stronger ideological link to the movement (M=3.1, SD=1.0) compared to Islamic extremists (M=2.5, SD=1.0). In fact, most far-rightists scored higher than 3 in our four-point scale, whereas most Islamic extremists scored lower than 2. This may be an indication that far-rightists who engage in financial crimes are more extremist in their belief system compared to Islamists, who on the other hand may be involved in this crime type for

[10] We did not include non-ideologically motivated suspects (N=57) in this analysis, as by definition their ideological affiliation was nil.

reasons other than pure ideological commitment to the cause. However, these results may be interpreted in a different way.

These diverging trends may be explained as a function of the quality of open-source materials or the nature of the cases examined. For example, it is possible that stronger ideological evidence was found in far-right cases compared to Islamic ones. On the other hand, it could also be that the evidence in Islamic cases was more controversial and did not provide a clear link between suspects and extremist ideology. These issues need to be addressed further as variations in the quality of open sources as well as any other problems related to these cases may affect our analysis, and possibly lead us to inaccurate conclusions. We shall return to this discussion in this chapter's concluding section.

5.2.3 Trial outcomes

Lastly, we examined variables from criminal trial proceedings, and once again compared political extremists with non-extremist suspects (see Table 5 below).

Table 5.7 Case Outcome[1]

	Total		By Defendant Status					
			Far right		Islamic extremist		Non-extremist	
	N	Percent	N	Percent	N	Percent	N	Percent
Trial result	132	---	49	37.1	38	28.8	45	34.1
Pled guilty	64	48.5	17	26.6	13	20.3	34	53.1
Guilty by jury	46	34.8	29	63.0	10	21.7	7	15.3
Dismissed	16	12.1	1	6.2	11	68.8	4	25.0
Acquitted	4	3.0	0	0.0	4	100.0	0	0.0
Guilty by bench	2	1.6	2	100.0	0	0.0	0	0.0
Sentence (months)	80	46.2	34	42.5	20	25.0	26	32.5
Min-Max	3-900	---	3-648	---	10-900	---	8-120	---
Mean (SD)	90(140)	---	90(117)	---	161(218)	---	35(27)	---

Upon indictment, the majority of defendants in financial crime cases chose to go to trial and received various outcomes (51.5 percent). This is not consistent with previous research on terrorism-related prosecutions that found that most political extremists tend to plead guilty (Smith et al., 2002). This is an intriguing finding that suggests the existence of significant differences with regard to the prosecution of violent and non-violent ideological crimes.

Although they were not the majority, numerous cases across all three categories were resolved with plea-bargaining. Non-extremist defendants chose this option more frequently (53.1 percent) compared to far-rightists (26.6 percent) and Islamic extremists (20.3 percent). The decision not to settle may, therefore, have something to do with the status of political extremist. For far-rightists, this could be related to their strong, anti-government ideological commitment, which may justify their relentless attitude even when

[1] Excludes cases pending or cases with outcome unknown. Of the total 164 suspects, case outcomes were available for 132 defendants, and sentencing results for 80 defendants.

faced with serious consequences such as criminal prosecution (Belli & Freilich, 2009; Cords, 2005; Pitcavage, 2001; SPLC, 2001). In the case of Islamic extremists, there may be other issues at play. As Smith and colleagues point out, this may be the result of the "'hard line' stance [...] taken by the government in their [sic] response to international terrorism" (2002, p. 323). Hence, alleged terrorists may be offered fewer options to negotiate by federal prosecutors. There could also be other reasons, such as for example defense counsel strategies related to the nature of these criminal proceedings.

Of those who went to court and were found guilty by jury, which was the most common outcome for all three categories (34 percent), the overwhelming majority were far-rightists (63 percent compared to 21.7 percent of Islamic extremists, and only 15.3 percent of non-extremists). Two far-right members renounced their right to a jury and were convicted by bench trial. Interestingly, only four defendants were acquitted, and they were all Islamic extremists. Even more interesting are the percentages of cases that were dismissed because of mistrial or prosecutorial misconduct, which concerned nearly one-third of Islamic defendants (29 percent of the total 38 defendants). Among the 16 defendants whose cases were dismissed, 68.8 percent (11 defendants) were Islamic, whereas only one was a far rightist and 4 were non-extremists.

As previously noted, post-9/11 investigations involving alleged Islamic terrorists appear to be problematic for various reasons. Federal prosecutors have been accused of mounting cases based on ill-founded evidence, for example by using the "guilt by association" argument when accusing individuals or charities of terrorism financing because of their humanitarian work in war-torn zones (Gunning, 2008; Warde, 2007). One of the most publicized examples involves the "Holy Land Foundation" (HLF), the largest U.S.-based Muslim charity that was accused, together with its executive board members, of assisting Hamas and Hamas-affiliated local committees by collecting donations for the

families of martyrs in the Palestinian territories (Eaton, 2007). The prosecution ended with a hung jury, which prompted the judge to declare a mistrial because of lack of evidence concerning the link with Hamas. Some of the defendants were eventually retried and convicted of non-terrorism related charges, whereas others were acquitted.

To shed light over these issues, especially as regards possible misconducts related to the "politicization" of terrorism-financing cases, it would be important to examine prosecutorial strategies more closely, by comparing for example charges mentioned in the indictment and charges for which suspects were convicted. We previously noted that a variety of non-financial statutes have been used in terrorism cases, for example violations of immigration regulations. In addition, consistently with previous research (Smith et al. 2002), we found anecdotal evidence in our open-source materials pointing to the use of dubious practices by the government in similar cases, such as the use of intelligence information by paid informants, including an out-of-status immigrant fearing deportation who offered to collaborate in a sting operation.

The problem of politically biased prosecutions is of fundamental importance for this study as it may considerably affect our findings, given that judicial cases were the starting point for our analysis. Unfortunately, in this dissertation we were not able to provide the level of analysis necessary to look into these issues more in depth. However, we did take these problems into account to fine-tune our network analysis by eliminating problematic cases and focusing on the "stronger" ones following the criteria described in this chapter's concluding section. Comparing punishment treatments provide further interesting insight. Overall, political extremists tended to receive longer sentences; Islamic extremists in particular were sentenced most harshly. On average, Islamic extremists were sentenced to 13 years in prison (M=161 months, SD=218 months), whereas far-rightists received 7.5 years (M=90 months; SD = 117 months). Non-extremists were treated most leniently,

receiving less than 3-year sentences on average (M=35; SD=27). Hence, Islamic extremists received significantly harsher sentences compared to non-extremists, especially in consideration of the nature of the crime (i.e. white-collar), which is usually associated with lesser punishments. As Smith et al. (2002) have noted, the "explicit politicality" of Islamic extremists might be one of the reasons explaining these trends. These findings deserve further examination taking into account other factors, e.g. prosecutorial and defense strategies, sentencing guidelines, court jurisdictions, etc.

5.3 Techniques by scheme type

To better understand how financial schemes are carried out, we broke them down into smaller components and examined specific activities or techniques utilized for their execution. This procedure resembles the "script approach" developed by Cornish to identify crime patterns and opportunity structures by describing the crime-commission process as a sequence of steps (Cornish, 1994). This method has been applied to a variety of crime types to simplify crime analysis and develop targeted situational preventive measures (Cornish & Clarke, 2002; Freilich & Chermak, 2009; Lacoste & Tremblay, 2003; Morselli, 2009; Smith, 1998). Our analysis of financial techniques represents a first step in this direction, and will hopefully provide useful insight for future studies aiming to develop situational prevention strategies against financial extremist crimes.

In this section, we compare techniques used by extremists and non-extremists in the context of different scheme types. Our previous analysis identified tax avoidance as the prevalent scheme type committed by far-rightists during the study period. Money dirtying and money laundering appeared to be most common among Islamic extremists. As noted,

although there are some differences between money dirtying and money laundering, experts argue that the methods used are very similar (Compin, 2008; Masciandaro et al., 2007). Because of the limited number of cases, we decided to merge these two scheme types and examine their techniques jointly. In future works, however, it will be interesting to test whether this assumption is true by comparing money-laundering techniques against money-dirtying ones.

5.3.1 Tax avoidance techniques

The figure below displays techniques used by far-right suspects and their non-extremist accomplices involved in tax avoidance schemes.

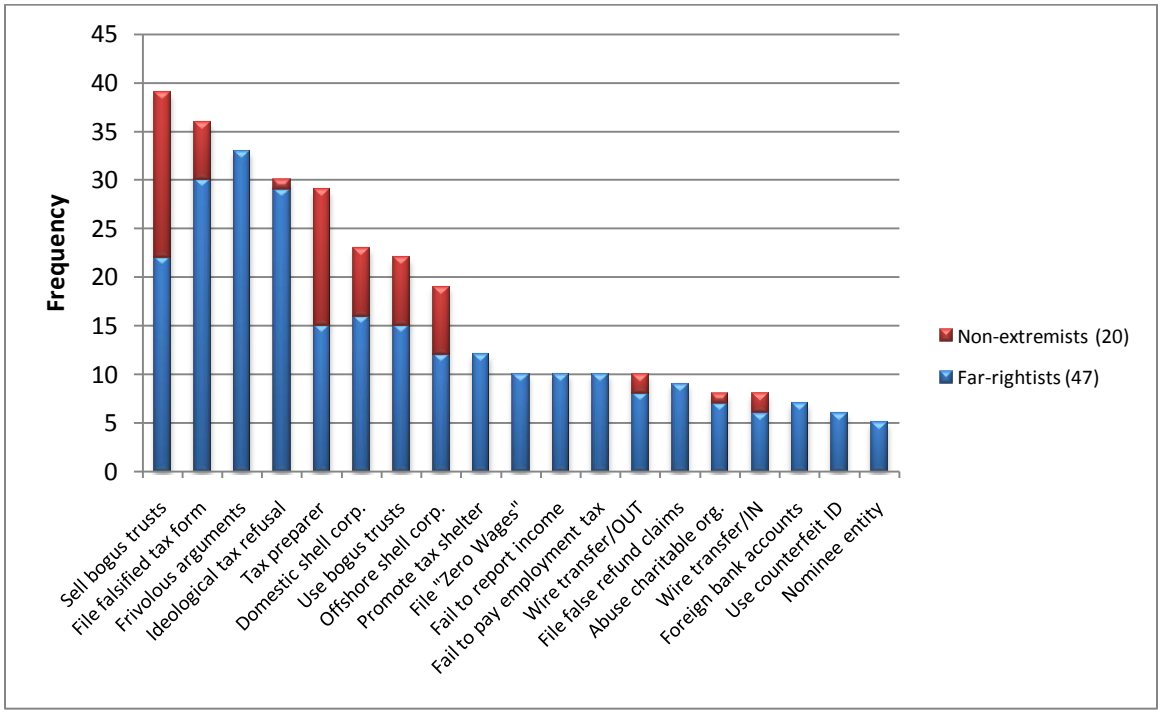


Figure 5.6 Techniques used in tax avoidance schemes

As the figure shows, tax avoidance schemes were carried out using a variety of different techniques. As expected, the majority of suspects involved in this scheme type were members of the far right (70.1 percent compared to 29.9 non-extremist associates). Among the techniques most frequently used by far-rightists we found typical anti-tax strategies, i.e. the use of "frivolous arguments" in court, ideologically motivated tax refusal, and filing of falsified tax forms. "Frivolous arguments", as defined by the IRS and federal courts, are questionable claims advanced by tax protesters to justify their refusal to comply with tax obligations. Such claims usually consist in misinterpretations of the Constitution and tax laws as regards tax liability. For example, tax protesters argue that paying income taxes is merely voluntary because of the language used on Form 1040 instruction booklet, and declare to be "sovereign citizens" instead of US citizens (Sanchez, 2006). As Belli and Freilich (2009) observed, tax protesters engage in both proactive as well as passive behaviors. Ideologically motivated tax refusal is an example of the second type, i.e. a popular crime of omission that involves the repeated failure to file an income return or the failure to pay employment taxes.

Proactive behaviors include a variety of methods, such as filing falsified documents, underreporting, and marketing anti-tax packages. We found evidence of the use of the so-called "Zero Wages Return" strategy, which was recently included in the "Dirty Dozen", a list of the most popular financial scams (IRS, 2008). Promoters of this scam instruct taxpayers either to enter all zeros on their federal income tax filings or to enter zero income, report their withholding and then write "*nunc pro tunc*"–– Latin for "now for then"––on the return. The sale and use of bogus trusts and "shell" corporations to hide income both domestically and abroad appear to be also common among far-right extremists. Interestingly, these techniques were frequently used by non-extremist associates, who appear to be also involved in tax preparation services. This may indicate that non-ideologically motivated

individuals involved in tax avoidance schemes possess certain specialized qualities, such as the ability to deal with trusts and incorporation, and may therefore hold a significant role as professional service providers. More insight into the relationship between political extremists and non-extremists, especially with respect to their service-providing function, will be given in the next chapter exploring network structures.

5.3.2 Money-laundering and money-dirtying techniques

The figure below illustrates techniques used by Islamic extremists and non-extremist suspects engaging in money-laundering and money-dirtying schemes.

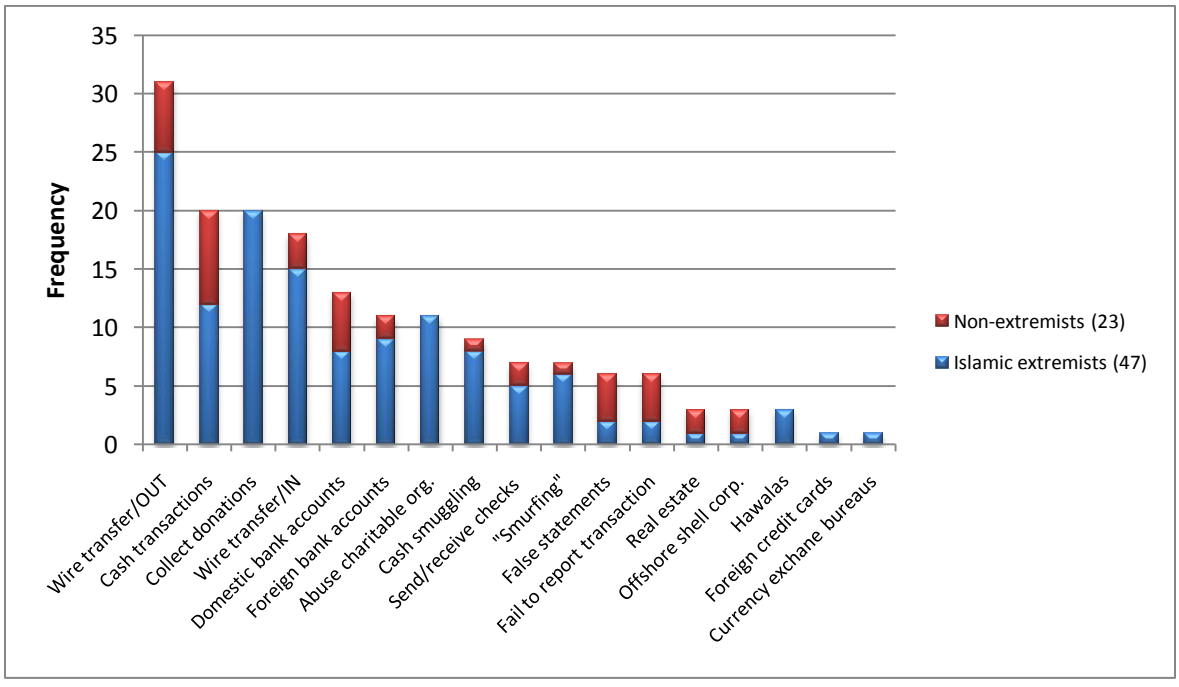


Figure 5.7 Techniques used in money-laundering and money-dirtying schemes

We immediately noticed how this scenario is completely different from the one presented before when examining tax avoidance strategies. Traditional financial transfer mechanisms appear to be among the most commonly used methods in a typical terrorism-financing scheme. Islamic extremists involved in money laundering and money dirtying made ample use of wire transfers from the United States to foreign destinations, as well as within national borders. They also owned and managed domestic and foreign bank accounts, sent and received checks, and structured financial transactions by breaking down large sums into smaller amounts to be deposited at different times and locations to avoid being detected (a technique also called "smurfing"; Reuter & Truman, 2004). These findings bear policy-relevant implications. Despite international and domestic efforts to protect the financial sector by adopting *ad-hoc* legislations and enforcing strict regulatory procedures and controls (such as the "Suspicious Activity Report" and "Know-your-customer" rules for financial institutions), financial systems appear to be vulnerable to malicious uses and infiltrations by criminals and terrorists alike.

Another interesting finding relates to the presence of techniques that are considered "informal value transfer systems", i.e. "mechanisms […] facilitating the transfer of funds or value without leaving a trail of entire transactions or taking place outside the traditionally regulated financial channels" (Passas, 2003, pp. 14-15). Consistently with previous research, we found that a large number of Islamic extremists preferred to conduct transactions in cash, and were also involved in cash smuggling operations by physically transporting money across borders. These methods seem to work because they are simple to execute, economically efficient, and effective in hiding financial trails (Passas, 2007). Some extremists appeared to have resorted to the use of *hawalas*. The number, however, is too small to advance any significant conclusions concerning their role as terrorism-financing mechanisms.

Some schemes were executed by channeling funds through charitable organizations as well as by collecting donations directly from mosques and other religious entities. Kane and Wall (2005) argue that this may be a preferred fund-raising method because money can be funneled to terrorist organizations abroad disguised as donations for humanitarian purposes. In addition, it is also attractive because of the economic advantages in terms of tax benefits. As previously noted, however, the prosecution of charitable organizations as instruments of terrorism financing has been the subject of intense controversies because of its politically sensitive nature (Warde, 2007). Therefore, we invite to take these arguments with caution, as judicial cases mentioning these techniques would need to be further scrutinized to determine whether these allegations held true or were just part of the prosecutorial strategy. For this to be possible, it will be important to follow up on open judicial cases until proceedings are concluded (i.e., all appeals are exhausted) and corroborate the findings with additional open-source materials.

Although non-extremists appear to have a smaller role in these scheme types, they made important contributions. Interestingly, they engaged in both formal and informal transfer systems, by wiring money abroad, hiding it in domestic and foreign bank accounts, transporting and paying in cash, and also lying to public authorities as regards financial transactions and other document applications.

5.4 Open-source quality assessment and selectivity bias

Until recently, research on terrorism and extremist crime has suffered from a lack of empirical studies based on valid and reliable data (Chermak, 2002; Gruenewald et al., 2008; Hamm, 2007; Merari, 1991; Silke, 2001). Researchers interested in these topics face many

challenges, including the lack of reliable and accessible information, the reluctance of law enforcement agencies to share their information, and the underground nature of terrorist and criminal organizations (LaFree & Dugan, 2004; Hamm, 2007). Despite these limitations, terrorism publications have flourished in the past decade, in part as a reaction to the 9/11 attacks and the international response that immediately followed (Silke, 2008). According to Sageman (2004, p. 67), the majority of these publications are journalistic accounts that tend to "fill in the gaps between facts in order to create a better narrative" rather than accurately investigate the extent of the problem. In return, these have contributed to the creation of a number of myths – like the idea that Al-Qaeda profited from speculations in the stock markets after the 9/11 attacks, subsequently debunked in the 9/11 Commission Report – that have led to the implementation of ineffective and even counterproductive policy choices (Biersteker & Eckert, 2008; Passas, 2007; Warde, 2007; Williams, 2008).

As LaFree and Dugan point out (2004), relying merely on official data to study a complex social phenomenon like terrorism presents two major difficulties, i.e. (a) political pressures may influence government's course of action, hence it is likely that collected data may be biased from the very beginning; and (b) oftentimes, alleged terrorists are prosecuted for offenses that may have nothing to do with actual terrorism. Self-report data obtained through interviews with former or current political extremists are also problematic for three reasons: (a) samples are small and consist of available participants; (b) results may be biased by the respondent's perception, flawed memory (i.e. retrospective reconstruction), or personal agenda; and (c) the absence of a comparison group does not allow for meaningful generalizations (Chermak et al., 2011; Horgan, 2008; Silke, 2001).

The advent of open-source databases, such as the ECDB, ATS, and GTD, therefore provides a new venue for quantitative research taking advantage of technological developments, such as the Internet and the existence of numerous web engines that provide

access to a variety of documents. Data collection methods are considerably improved by following rigorous protocols that allow for identifying relevant cases using predefined inclusion criteria, searching a variety of open-source materials, and developing more accurate and comprehensive incident- and suspect-based data sets for statistical analysis (for a more in-depth discussion of the characteristics, strengths and weaknesses of the mentioned databases, see: Chermak et al., 2011). The ECDB is especially innovative in this regard, as it includes information on all crime types committed by political extremists, i.e. violent and non-violent, ideological and routine crimes, as well as data on their non-extremist criminal associates. This is a remarkable feature, considering that most terrorism studies focus on ideologically motivated violence, neglecting the relationship existing between terrorism and other crime forms.

Creating a data set using open sources, however, is not a process which is immune from bias. Although relying on multiple source types improves the overall quality of the data compared to using a single one, such as law enforcement records or self-reported interviews, there are still some important issues that must be resolved. Chermak et al. (2011) describe at least two possible types of selectivity bias which may affect the validity and reliability of open-source databases, i.e. (a) publicity effects, and (b) source effects.

The first type refers to the popularity surrounding certain high-profile cases that draw a lot of attention in the public and tend, therefore, to be more publicized in the media. On one hand, this may be a positive aspect, as researchers are able to gather and compare a variety of different sources providing multiple perspectives on these cases. On the other hand, the perception of their importance may be biased by their ultra-popularity, which may overshadow other less prominent but still relevant incidents, resulting in a partial or distorted view of the phenomenon under study. Additionally, publicity bias may also produce an enhanced public interest, which may result in increased media coverage in the

period following a high-profile incident, a phenomenon so called "echo effect". For example, Chermak (2002) noted that the 1995 Oklahoma City bombing raised widespread concern over the rise of far-right terrorism, which continued to be portrayed in the media as an alarming trend many years after the incident.

The second type, i.e. source selection bias, relates to the fact that quantitative analyses of terrorism may vary depending on the specific source type used by researchers. Chermak et al. (2001) found variations in the number of incidents of right-wing homicides reported by GTD compared to SPLC and ECDB. However, comparing the distribution of suspect, victim, and incident characteristics, they found few statistically significant differences across data sets, suggesting that "using different sources of terrorism data may not lead to different findings and conclusions about terrorism "(Chermak et al., 2011). Variations in the percentages of homicides reported by different sources were, in fact, related to different inclusion criteria. Importantly, Chermak et al. (2011) also pointed out that combining various sources has several advantages in terms of improved validity and reliability of open-source databases, allowing researchers to get closer to including the entire universe of existing cases.

Given the novelty of this data collection method, the authors recommend that researchers create an "error profile" to improve the transparency of their research efforts and identify "possible sources within the data collection methodology which may bias the results through non-sampling errors, which can negatively affect the data even if a census or random sample is used" (Chermak et al., 2011). With respect to the ECDB, the authors further propose taking into account two possible non-random sampling errors which may affect the database, i.e. (a) identification of incidents, and (b) coder decisions. Since this dissertation uses secondary data from the ECDB, it is important to first address the question

of selectivity bias and non-random sampling errors related to our methodology before we can continue with social network analysis.

As mentioned, this study aimed at providing a snapshot of financial crime cases prosecuted by federal authorities in 2004 to describe the characteristics of financial schemes involving far-rightists, Islamic extremists, and their non-extremist associates, as well as their financial criminal networks. To identify our study population we followed a multi-step procedure described more extensively in the previous sections and here briefly summarized. First, we searched cases through a variety of open sources, including official government websites (e.g. US Department of Justice, US Tax Division, IRS, FBI, US Treasury, etc.), terrorism databases (ATS, GTD), watchdog publications (e.g., ADL, SPLC, Militia Watchdog, Jihad Watch, etc.), news and scholarly databases (e.g., Lexi-Nexis, Westlaw, FindLaw, etc.), and other Internet websites (e.g., Google, Yahoo, ProQuest, etc.). To guarantee a rigorous identification process and avoid source selection biases, all these sources were checked multiple times and follow-up searches were conducted periodically to identify any possible additional case. Next, we created a list of far-right and Islamic extremist suspects indicted in 2004 for participating in a financial scheme, and subsequently searched each single case using 26 web engines to gather all publicly available information. Finally, the open-source documents were coded in a relational database which consisted of four codebooks focusing on scheme, suspect, business entity, and open sources characteristics. To ensure that data were coded accurately and prevent issues related to inter-rater reliability, we personally double-checked each coded case, conducted follow-up searches and, when necessary, edited the database (see Section 4.1. for a more detailed description of these procedures).

The table below describes the number and type of sources retrieved and used to code the far-right and Islamic extremist financial schemes discussed above.

Table 5.8 Open Sources Assessment

	All Schemes		By Ideology			
			Far Right (26)		Islamic Extremist (28)	
	N	Percent	N	Percent	N	Percent
Sources by Scheme						
Min-Max	1-135	---	6-120	---	1-135	---
Mean (SD)	32.2(28.9)	---	22.7(25.8)	---	41.0(29.2)	---
Source type						
Court docs	311	18.1	170	54.7	141	45.3
Police/Government	191	11.1	106	55.5	85	45.5
Newspaper articles	983	57.1	240	24.4	743	75.6
Watchdog docs	28	1.6	7	25.0	21	75.0
Websites	115	6.7	48	41.7	67	58.3
Scholarly docs	6	0.3	0	0.0	6	100.0
Other	88	5.1	19	21.6	69	78.4
Total	**1722**	**100.0**	**590**	**34.3**	**1132**	**65.7**

As mentioned, our study universe consisted of 54 financial schemes, 26 involving at least one far-rightist, and 28 involving at least one Islamic extremist. Looking at the open-source assessment table, it is interesting to notice a considerable variation in the number and type of sources that were retrieved during the data collection process. Although roughly half of the schemes were far-right related whereas the other half was Islamic-based, a disproportionately larger number of sources were found concerning the second ones compared to the first ones (1132, or 65.7 percent, compared to 590 or 34.3 percent). On average, an Islamic extremist financial scheme was covered in 41 documents, whereas a far-right one was discussed in nearly 23.

Overall, newspaper articles represent the most frequent source type on financial schemes involving political extremists (57.1 percent of the total 1722 documents retrieved). This primacy holds true if we look at the distribution by ideology, although the overwhelming majority of newspaper stories focused on Islamic-related cases rather than

far-right ones (75.6 percent compared to 24.4). More extensive media coverage, therefore, seems to explain the substantial difference in the number of documents identified. In fact, if we exclude newspaper articles, far-right and Islamic financial schemes are presented in almost the same number of documents (350 and 389 respectively).

Court documents, i.e. criminal indictments, court sentences, appellate decisions, trial transcripts, etc., appear to be the second most frequent source type for both far-right and Islamic cases: in total, 311 court documents were identified, 54.7 percent of which concerned far-right defendants while the remaining 45.3 percent involved Islamic extremists. This is a reassuring point which confirms the good quality of our data, considering that court documents are considered to be the most reliable open-source type by network researchers (Morselli, 2009; Sageman, 2004).

Following court documents, the open-source searches identified, in descending order: police and government documents, such as investigative reports, official notices, etc. (191 in total, 55.5 percent by far-rightists, and 45.5 involving Islamic extremist suspects); Internet websites, such as blogs or private organizations websites (115 in total, 41.7 concerning far-right schemes, and 58.4 about Islamic cases); other sources, e.g. e-mails, discussion threads, etc. (88 in total, 21.6 for the far right and 78.4 for Islamic extremists); watch-dog publications from websites such as ADL, SPLC, Militia Watchdog, Jihad Watch, etc. (28 in total, 75 percent on Islamic extremism, and the remaining 25 percent on the far right); and finally six scholarly publications that focused on Islamic cases.

These results lend support to the abovementioned publicity bias affecting open-source research dealing with "hot" topics, like post-9/11 Islamic-based terrorism. More specifically, we argue that the disproportionate media coverage concerning Islamic cases may be the product of an "echo effect" following the 9/11 attacks. As mentioned, the "war on terror" became a powerful slogan used by the U.S. government to launch an anti-

terrorism campaign that involved a variety of domestic and international strategies to detect and deter future terrorist incidents (Biersteker & Eckert, 2008; Eckert, 2008; Warde, 2007). An important component of this strategy involved targeting terrorism financing to deprive terrorists of crucial resources needed for survival and logistical purposes. The USA Patriot Act was conceived in this climate, and its provisions, allowing for heightened investigative and prosecutorial measures, were swiftly applied. As a result, over one hundred suspects were prosecuted as alleged terrorists between 2001 and 2003 (Kane & Wall, 2005). Of those charged, however, only a small number was convicted for actual terrorism-related activities, while the others were either acquitted, convicted of unrelated charges (e.g. immigration fraud, mortgage fraud, etc.), or their case was dismissed due to prosecutorial misconduct.

This discussion leads us to the second type of non-random sampling error possibly affecting our data, i.e. coder decisions. The *ECDB Financial Crimes* requires that two criteria be met for a case to be included: (a) a *behavioral criterion*, i.e. a financial crime, as defined in the US Criminal Code, must be committed and criminally prosecuted by federal authorities; and (b) an *attitudinal criterion*, i.e. at least one of the suspects must be identified as a far-right or Islamic extremist as defined in the ECDB Codebook and the inclusion criteria section above. The first criterion was not a source of problems overall, as the open sources usually indicated what type of criminal offenses the suspects were charged with, especially when official documents, such as criminal indictments and court decisions, were retrieved. The second criterion, however, appeared to be more problematic. As mentioned, we used a 4-point scale to measure suspects' strength of ideological association. This variable allowed coders to verify the attitudinal criterion by reporting any evidence found in the open sources supporting the presence or absence of an extremist link.

If the open-source materials revealed only positive indicators and no contrary evidence, a suspect was assigned a score of 4 or 3 depending on whether there were multiple indicators or a single one. The positive indicators included, among others, prosecutorial evidence, witness testimonies, self-proclaiming statements, and so forth. If, on the other hand, evidence contrary to an extremist link was found, e.g. denial by family and friends, evidence presented by the defense, motions by human rights activists, etc., the suspect was assigned either a 2 or 1, depending on whether there were multiple or a single positive indicator. In other words, if a suspect scored 3 or 4 in our strength of ideological association scale, we could reasonably assume that he or she was likely to be an extremist at the time of the scheme, whereas a score of 2 or 1 raised doubts as to whether the suspect was actually linked to an extremist ideology. The table below summarizes this scoring system, which was discussed more in detail in the previous chapter.

Table 5.9 Suspect Strength of Ideological Association

Value	Criteria
4=Undisputed established present or past adherence to far-right or Islamic extremist ideology	1) Multiple (2 or more) far-right/Islamic extremist indicators found, and 2) No evidence found contrary to far-right/Islamic extremist association
3=Clear established present or past adherence to far-right or Islamic extremist ideology	1) Only single far-right/Islamic extremist indicator found, and 2) No evidence found contrary to far-right/Islamic extremist association
2=Disputed present or past adherence to far-right or Islamic extremist ideology	1) Multiple (2 or more) far-right/Islamic extremist indicators found, and 2) Evidence found contrary to far-right/Islamic extremist association
1=Disputed established present or past adherence to far-right or Islamic extremist ideology	1) Only single far-right/Islamic extremist indicator found, and 2) Evidence found contrary to far-right/Islamic extremist association

During the coding process, problems arose when coders had to review and make decisions regarding complicated and highly sensitive terrorism trials (e.g., the prosecution of the Holy Land Foundation, the largest US Islamic charity based in Texas that was accused of collecting donations to fund Hamas military wing in Palestine). Many of these high-profile prosecutions, which were initiated as part of the government anti-terrorism financing campaign, were put in the spotlight after allegations that they were strongly politicized and lacked evidentiary basis (Kane & Wall, 2005; Passas, 2007; Smith et al., 2002; Warde, 2007).

Although coders were instructed to record any type of indicator that would allow to determine whether or not the suspect was an extremist, concerns arose when the evidence of an extremist link was entirely based on controversial prosecutorial evidence (e.g. obtained through paid informants or sting operations) that was eventually dismissed by the judge. These concerns are reflected in the distribution of suspect's strength of ideological association scores. To illustrate this point, we estimated the maximum suspect strength of association per scheme reported by coders, comparing between Islamic and far-right cases (Table 5.10).

Table 5.10 Maximum suspect strength of ideological association by scheme ideology

	Max. Suspect SIA (%)				Total
	1	2	3	4	
Scheme Ideology					
Far right	1 (50.0)	4 (19.9)	6 (100.0)	15 (60.0)	26
Islamic extremist	1 (50.0)	17 (80.1)	0 (0.0)	10 (40.0)	28
Total	**2 (3.7)**	**21 (38.9)**	**6 (11.1)**	**25 (46.3)**	**54 (100.0)**

The differences between far-right and Islamic extremist cases, once again, are striking. Overall, the majority of financial schemes (46.3 percent) had at least one suspect with the strongest ideological association possible, i.e. multiple positive indicators were present and no contrary evidence was found in the open-source materials. However, a little over 40 percent of schemes involved individuals whose ideological affiliation was disputed, i.e. no suspect scored higher than 2 on the 4-point scale.

Comparing by ideology, we can see that the overwhelming majority of far-right financial schemes (over 80 percent) involved individuals who appeared to be strongly associated with their ideological movement, i.e. at least one of them per scheme scored higher than 3. Financial schemes involving Islamic extremists, on the other hand, concerned for the most part suspects whose adherence to the movement was disputed, i.e. no suspect involved in the scheme scored higher than 2 (18 out of 28 schemes, or 64.3 percent of the total). Interestingly, the remaining schemes (10 out of 28, or 35.7 percent) involved at least one suspect whose ideological affiliation was strongest, i.e. multiple positive indicators were found and no contrary evidence.

The large number of Islamic extremist cases for which conflicting evidence concerning the suspect extremist link was found is evidence of possible selectivity bias. Specifically, we hypothesize the existence of publicity and echo effects affecting our Islamic sample as a result of the post-9/11 counter-terrorism strategy pursued by the Department of Justice. In other words, some of these alleged terrorism prosecutions may have been a byproduct of the DOJ's official strategy to use "every tool and every tactic in the arsenal of the justice community […], from aggressive enforcement of the criminal code to the deployment of the new and critical tools of the USA Patriot Act, […] to deter, disrupt and destroy terrorist threats" (Ashcroft, 2004).

5.4.1 Study universe for social network analysis

The previous discussion on open sources quality and the existence of possible selectivity biases within our data set led us to the decision to drop cases that did not involve at least one suspect whose extremist link was undisputed, i.e. he or she scored higher than 3 on our 4-point scale. This dissertation employs social network analysis to investigate how political extremists (i.e. far-rightists and Islamic extremists) who engage in financial criminal activities associate with non-ideological profit-driven offenders. In other words, our population of interest consists of all individuals who participated in a financial scheme, provided that at least one of them was either a far-rightist or Islamic extremist at the time of the scheme. To make sure that our analysis portrayed actual financial extremist networks and not something else, we decided to focus on the "stronger" cases and get rid of the "weaker" ones. As a result, our study universe for social network analysis purposes included all suspects involved in 31 schemes, 21 concerning the far right and the remaining 10 involving at least one Islamic extremist. Summary descriptive statistics of the selected schemes are provided in the table below.

Table 5.11 SNA Schemes Attributes

	Total		By Ideology			
			Far Right		Islamic Extremist	
	N	Percent	N	Percent	N	Percent
Financial schemes	31	100.0	21	67.7	10	32.3
Scheme Type						
Tax avoidance	19	61.3	19	100.0	0	8.0
Money-dirtying	5	16.1	0	0.0	5	100.0
Money-laundering	2	6.5	0	0.0	2	100.0
General fraud	2	6.5	0	0.0	2	100.0
ID fraud	1	3.2	1	100.0	0	0.0
Pyramid	2	6.5	1	50.0	1	50.0
Relevance						
Ideology/non-violent	16	51.6	16	100.0	0	0.0
Ideology/violent	7	22.6	0	0.0	7	100.0
Mixed profit/ideology	7	22.6	4	57.1	3	42.9
Pure profit/greed	1	3.2	1	100.0	0	0.0
Length (months)						
Min-Max	2-233	---	8-195	---	2-233	---
Mean (SD)	72.9 (60.0)	---	74.3 (44.2)	---	70.2 (84.5)	---
Geographic scope						
Local	16	51.6	16	100.0	0	0.0
International	15	48.4	5	33.6	10	66.7
Single/multiple suspects						
Single	7	22.6	6	57.9	1	42.1
Multiple	24	77.4	14	42.9	10	57.1

Before we continue our analysis, it is important to clarify that the decision to exclude more controversial cases should not be taken as an indication that they are any less significant. On the contrary, future research should examine these schemes more in depth, as their analysis may improve our understanding of this complex phenomenon and, in particular, the impact of certain prosecutorial strategies on terrorism research. To the extent of our knowledge, this is the first empirical study focusing on criminal prosecutions that makes a distinction between actual and alleged terrorists or political extremists by

measuring their strength of ideological association using objective indicators from multiple sources. In this sense, we hope that this study will contribute to improve scientific rigor in terrorism and extremism crime research.

CHAPTER 6. COMPARING FINANCIAL EXTREMIST NETWORKS

After providing a general picture of the financial criminality of far-right and Islamic extremists, this chapter focuses on their social networks. As mentioned, social network analysis can be a very powerful investigative tool for exploring the organizational structure of covert networks, uncovering hidden relational dynamics and vulnerabilities, and ultimately facilitating the development of more effective counterstrategies (Bruinsma & Bernasco; 2004; Coles, 2001; Sparrow, 1991; Van der Hulst, 2009; Xu & Chen, 2008).

According to opportunity theories, crime is the result of an interaction between a motivated offender and a set of available opportunities, which include a suitable target, the absence of a capable guardian, and resources needed to successfully execute it (Clarke, 1997; Cornish & Clarke, 1986; Clarke & Felson, 1979). Some of these resources are found within the offender (e.g., cognitive and moral resources), whereas others are external and may require searching for a "suitable co-offender" providing access to specialized knowledge, professional services, transportation, etc. (Ekblom & Tilley, 2000; Felson, 2002; Gill, 2005; Tremblay, 1993). For these reasons, examining the whole network of contacts, both legal and illegal, that participated in the different stages of the crime commission process, i.e. before and after its execution, is of utmost importance if we want to fully comprehend the interplay between offender and crime opportunities (Malm et al. 2010; McGloin, 2005; Morselli, 2009; Tremblay, 1993).

This chapter addresses the second set of questions proposed in this research by conducting an exploratory analysis of relational data collected in the ECDB, i.e.:

1. How are the suspects related to each other, and how are they connected to other non-prosecuted individuals who took part in the scheme?

2. What are the properties of these financial criminal networks, and how do they vary taking into account schemes and suspects' characteristics?
3. What types of relational ties exist among network members, and how do these vary taking into account schemes and suspects' characteristics?

This dissertation also advanced four hypotheses that were tested using Exponential Random Graph (p*) Modeling (ERGM), which provides a rigorous and innovative method to analyze and compare structural and attribute characteristics of social networks.

In the next section, we first provide a general description of the overall financial criminal network, which consists of the relational ties between *egos* (i.e., primary suspects involved in the 31 schemes previously identified) and *alters* (i.e. any additional person who was connected to the primary suspect and participated in the scheme but was not prosecuted). Next, we examine the role of multiplexity comparing structural and attribute properties of networks formed by three types of relational ties (i.e., co-offending, family, and business ties), distinguishing between far-right and Islamic extremist settings (Hypotheses 1 and 2). The final section focuses on the two largest far-right and Islamic components within the overall *egos* and *alters* network, comparing network-, sub-group, and actor-level characteristics to determine structural and attribute variations between these two ideological sub-sets (Hypotheses 3 and 4).

6.1 Network description

Consistently with previous research, to explore and compare structural and attribute characteristics of the overall criminal network, we recoded the different types of

ties (i.e. criminal tie, business tie, and family tie) as a binary variable (0= tie is absent, 1=tie is present; Malm et al. 2010; Sageman, 2004). In other words, we aggregated the three separate relational ties into a single linkage, which can be operationalized as the exchange of goods (e.g., money, products, etc.) or services (e.g., labor, legal advice, etc.) in furtherance of an illegal financial scheme. As a result of the screening process described in the previous chapter, our final data set for social network analysis resulted in 125 suspects (*egos)* who participated in 31 financial schemes prosecuted in 2004. The identified *egos* appeared to be connected to an additional 161 individuals (*alters),* for a total of 286 actors, or "nodes". The table below provides descriptive statistics of the *egos* and overall networks from ECDB data.

Table 6.1 Network Descriptive Characteristics

	Egos		Egos + Alters	
	N	**Percent**	**N**	**Percent**
N. of nodes	125	---	286	---
N. of edges	640	---	901	---
Gender				
Male	108	86.4	243	85.0
Female	17	13.6	43	15.0
Status				
Far-rightist	51	40.8	71	24.8
Islamic extremist	35	28.0	74	25.9
Non-extremist	39	31.2	141	49.3
N. of isolates	7	5.6	3	1.0
N. of components	12	---	16	---
Largest	27	21.6	65	22.7
Density	0.082	---	0.022	---
Degree				
Average	10.240	---	6.301	---
Maximum	39	---	46	---

As the table shows, the percentage of men compared to women did not vary from *egos* to the overall network. The majority of financial criminal network members were male (86.4 percent compared to 13.6 female in the *egos* network, and 85.0 percent compared to 15.0 in the overall network). On the other hand, there are some variations as regards the number and type of associates within the two networks. In the *egos* one, the majority of actors were far-rightists (51, or 40.8 percent), followed by non-extremist suspects (39, or 31.2 percent), and a minority of Islamic extremists (35, or 28.0 percent). This could be due to the larger number of far-right schemes which make up our study universe, i.e. twenty-one compared to only ten Islamic-related schemes, after we dropped the more controversial Islamic extremist cases.

After adding all *alters*, however, these proportions changed substantially. The overall network comprised for the most part non-extremist associates, who represent almost half of all network members (141, or 49.3 percent), followed by an equal percentage of far-rightists and Islamic extremists (respectively 71, or 24.8 percent, and 74, or 25.9 percent). This is an interesting preliminary finding, as it points out the crucial role played by individuals who do not appear to be ideologically motivated, further highlighted by the fact that these individuals were not among the primary suspects, which suggests that their function could have been overlooked by criminal justice authorities.

It is also interesting to look at the change in number of isolates and components from the *egos* to the overall network. In social network terms, an isolate is a node that has no nodes adjacent to it, whereas a component is a maximal connected sub-graph (Wasserman & Faust, 1994). In lay terms, an isolate is a single offender, or from a terrorism perspective, a "lone-wolf", whereas components are co-offending subsets of various sizes involving at least two linked persons. Specifically, the number of isolates decreased from 7 to 3, while the number of components increased from 12 to 16, suggesting that the apparent

lone wolves were in fact part of a sub-group that was not immediately visible. This intriguing finding questions the validity of lone-wolf terrorism research, and highlights the importance of going beyond criminal justice representations and considering the role of informal networks in the crime commission process (Dishman, 2005; Johnston & Risen, 2003; Spaaij, 2010; Turks, 2004).

From a structural perspective, the *egos* network appeared to be denser than the overall network. As discussed, density is a measure of social cohesion, and it is calculated as a proportion between the number of observed ties and the number of all possible ties existing in the network (Wasserman & Faust, 1994). The total cumulative number of ties (or *edges* in this case because they are non-directional) increased from 640 in the *egos* network to 901 in the overall network[11]. Density is inversely related to network size, and in fact we notice a considerable decrease from 0.082 in the *egos* network, which means that 8.2 percent of the total possible ties were observed, to 0.022, or 2.2 percent of all possible links, in the overall network.

Structural cohesion is considered an important factor for understanding social relationships (Scott, 2000). In general, it is argued that a strongly connected network facilitates social exchanges and communication flows (Burt, 1984). However, high connectivity can be a problem in the context of covert networks. Criminal activities are usually conducted in secrecy. Too many interactions can be dangerous as members are more exposed to internal (e.g. non-participating business associates, criminal competitors, etc.) and external threats (e.g. corporate security, law enforcement, etc.; Baker & Faulkner, 1993; Erickson, 1981). As a result, covert networks tend to be lower in density compared to

[11] The number is cumulative because of the existence of multiple tie types, which were added together to provide the actual link number.

legitimate social networks (Malm et al., 2010; McGloin, 2004; Morselli, 2009; Natarajan, 2006). For example, Morselli (2009) compared six criminal networks of various sizes (ranging from 25 to 174 actors) and found density values varying from 3.4 percent to 11.7 percent. The low density values in our data are consistent with this research.

It is important to clarify that the abrupt drop from *egos* to complete network's density value is likely an artifact of our research design, which employed an ego-centric approach to identify relational ties between *egos* and *alters*, but not between *alters* and *alters*. Limited time and available resources were the primary reasons why we decided to construct network boundaries around the primary suspects' social networks. However, we believe we were able to capture the almost totality of relational ties between primary suspects and their accomplices involved in financial criminal activities. Additionally, by including non-prosecuted individuals and multiple relational tie types, we have already made considerable advances compared to previous research, which relied on determinations by criminal justice agencies or examined only one type of relationship (McGloin, 2004; Malm, 2007; Morselli, 2009; Natarajan, 2006). In future research, we plan to expand our network universe to include *alter*-to-*alter* ties.

6.1.1 Network components by ideology

One of the advantages of social network analysis is that, similarly to crime mapping, it provides a simple and direct way for researchers to inspect network structures through visual representations (Freeman, 2005). For optimal visualization, we used *multi-dimensional scaling (MDS),* a technique that utilizes spring-embedding algorithms to display network data taking into account meaningful distances between actors, and is especially

useful to explore complex network structures and detect cohesive sub-groups (Knoke & Yang, 2008). For this routine, we used the Kamada-Kawai algorithm provided in the software package *Pajek,* because it allows for a better visualization of separate components (deNooy et al., 2005).

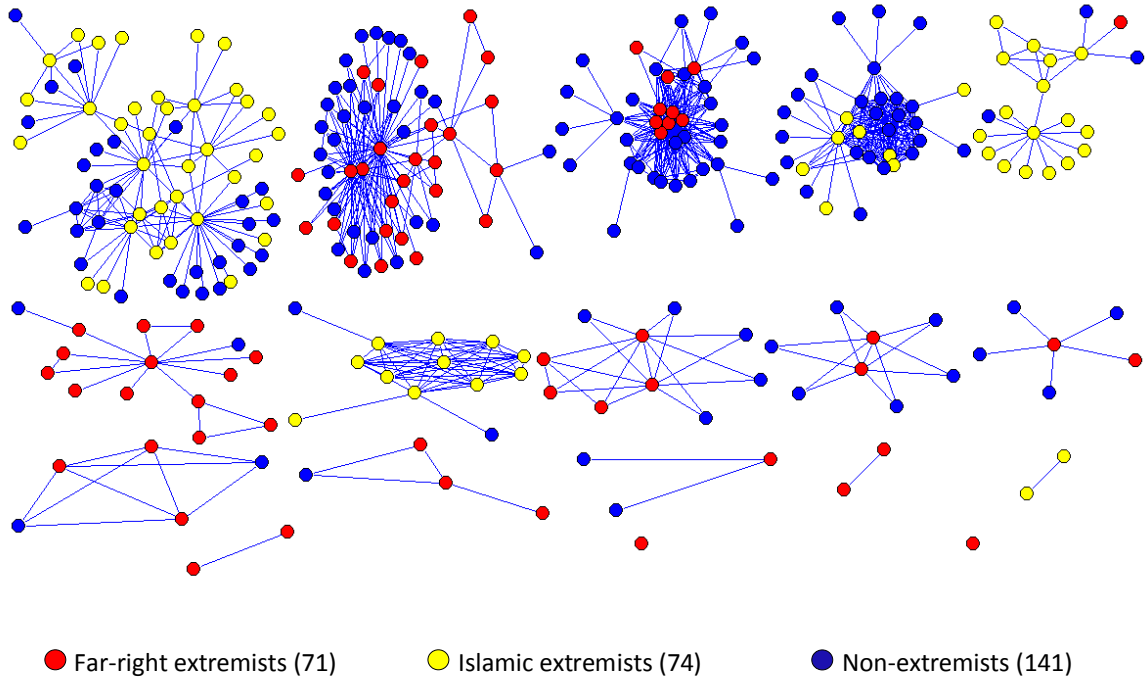


Figure 6.1 Overall network of *egos* and *alters*

Figure 6.1., which illustrates the overall network of financial offenders and their associates, presents a variety of structural patterns. First of all, it is interesting to notice that the only "true" financial lone-wolves were far-rightists, confirming previous research on far-right non-violent crime trends (Chermak et al., 2009). Additionally, there appears to be a clear separation between Islamic and far-right financial criminal networks, with the exception of one component, at the top right side, which is composed by a majority of Islamic extremists, three non-extremists, and one far-rightist. This intriguing finding

suggests that collaborations across ideologies may occur in the context of financial crimes. However, with respect to our data set, this is an exception, as far-rightists and Islamic extremists appeared to collaborate extensively with non-extremists, but not among each other. The table below provides additional descriptive characteristics that help interpret the overall network by looking at components by ideology.

Table 6.2 Network Characteristics by Ideology

	Total		By Ideology			
			Far-right		Islamic	
	N	Percent	N	Percent	N	Percent
N. of nodes	286	100.0	152	53.1	134	46.9
N. of edges	901	---	519	---	382	---
N. of components	16	---	11	68.7	5	31.3
Largest	65	22.7	56	19.6	65	22.7
Status						
Extremist	145	50.7	70	46.1	75	56.0
Non-extremist	141	49.3	82	53.9	59	44.0
Gender						
Male	243	85.0	115	47.3	128	52.7
Female	43	15.0	37	86.0	6	14.0
Density	0.022	---	0.045	---	0.043	---
Degree						
Average	6.301	---	6.829	---	5.701	---
Maximum	46	---	46	---	27	---

As the sociogram clearly shows, the majority of components, or maximally connected sub-groups within the overall network, are far-right related (i.e., eleven components, or 68.7 percent, compared to only five Islamic extremist ones, or 31.3 percent). However, the number of actors across ideologies is similar: the eleven far-right

components include 152 individuals (53.1 percent of the total 286), whereas the five Islamic ones involved 134 persons (46.9 percent). This suggests that Islamic extremists sub-groups in our study are indeed less numerous but overall more populated than far-right ones. On average, a far-right financial criminal network involved nearly 13 participants, whereas an Islamic one was composed of almost 27 individuals, i.e. more than twice the number of co-offenders.

As mentioned, the overall network was made of roughly half political extremists and half non-extremists (respectively, 145, or 50.7 percent, and 141, or 49.3 percent). However, there appear to be variations if we look at the distribution by ideology. Far-right sub-groups involved for the most part non-extremists (53.9 percent compared to 46.1 percent of extremists), whereas Islamic sub-sets included more extremists than non-extremists (56.0 percent compared to 44.0 percent). This descriptive finding lends preliminary support to our research hypotheses concerning the existence of different homophily and heterophily effects within Islamic extremist and far-right financial criminal networks. These arguments will be further developed in the following sections.

Density values for far-right and Islamic financial sub-networks are almost identical, i.e. 0.045 compared to 0.043, which means that, respectively, 4.5 percent and 4.3 percent of all possible ties were present in financial extremist networks involving far-rightists and Islamic extremists. These findings are consistent with the extant research on low connectivity within covert networks previously discussed.

6.2 Multiplexity in financial extremist networks

The previous section provided some basic information on the overall network of criminal suspects (*egos*) prosecuted for their participation in a financial scheme and their links with additional actors (*alters*) who contributed to its execution. We also initiated a discussion on similarities and differences between far-right and Islamic-based financial criminal networks. In this section, we expand this comparative analysis further by exploring structural and attribute characteristics of networks formed through three different types of relational ties, i.e. co-offending, family, and business ties.

Most studies on social networks focus on one type of link between actors for reasons of simplicity (Hanneman & Riddle, 2005). However, many researchers have stressed the importance of including multiplex relationships in social network analysis, because these better represent the reality of human interaction, which is rarely based on only one form of connection between two individuals (Cook et al., 2001; Koehly & Pattison, 2005; Krackhardt, 1987). This point is even more important in the context of covert networks, as research shows that co-offenders are oftentimes linked through an array of different relationships, including kinship, gang membership, or legitimate business association (Malm et al., 2010; McGloin, 2004; Sarnecki, 2001). Therefore, to truly understand the complex dynamics occurring within illegal networks, it is crucial to explore the nature and variety of links between actors. Including multiplexity in criminal network research has also the advantage of reducing the problem of boundary specification and missing data (Laumann et al., 1992). As noted, limiting the analysis to the suspects identified during criminal justice investigations may misrepresent the overall network structure, which could be functioning thanks to individuals who were not directly targeted by law enforcement interventions (Curtis & Wendel, 2000; Natarajan, 2006).

In the following sections, Research Hypotheses 1 and 2 were tested using Exponential Random Graph Modeling (ERGM), which allowed us to compare structural and attribute characteristics of co-offending, family, and business networks involving far-rightists, Islamic extremists, and non-extremists who participated in a financial scheme. This analysis provided us with useful information about strength and weaknesses of financial extremist networks as regard their ability to be flexible and allow the flow of information as well as resiliency against external threats (Malm et al., 2010).

The table below provides descriptive characteristics of each sub-network, which was partitioned out of the overall network of *egos* and *alters*, distinguishing between Islamic and far-right sub-sets. It is important to notice that there is an overlap between co-offending, family, and business networks, as some people were connected through more than one tie. This approach is consistent with previous research on multiplexity, and allowed us to draw interesting comparisons using ERGM standardized parameter estimates (Hanneman & Riddle, 2005; Malm et al., 2010).

Table 6.3. Co-offending, family, and business networks of far-right and Islamic extremists involved in financial schemes

	Co-offending Network			Family Network			Business Network		
	Total	Far Right	Islamic	Total	Far Right	Islamic	Total	Far Right	Islamic
N. of nodes (%)	178 (62.2)	82 (46.1)	96 (53.9)	79 (27.6)	44 (55.7)	35 (44.3)	244 (85.3)	142 (58.2)	102 (41.8)
N. of edges	613	285	328	95	40	55	391	231	360
Gender (%)									
Male	156 (87.6)	62 (41.7)	94 (58.3)	56 (70.9)	26 (46.4)	30 (53.6)	206 (84.4)	107 (51.9)	99 (48.1)
Female	22 (12.4)	20 (90.9)	2 (9.1)	23 (29.1)	18 (78.2)	5 (21.8)	38 (15.6)	35 (92.1)	3 (7.9)
Status (%)									
Far-rightist	56 (31.5)	56 (100.0)	0 (0.0)	33 (41.8)	33 (100.0)	0	66 (27.0)	65 (98.5)	1 (1.5)
Islamic extremist	64 (36.0)	0 (0.0)	64 (100.0)	21 (26.6)	0 (0.0)	21 (100.0)	49 (20.1)	0 (0.0)	49 (100.0)
Non-extremist	58 (32.5)	26 (44.8)	32 (55.2)_	25 (31.6)	11 (44.0)	14 (66.0)	129 (52.9)	77 (59.7)	52 (40.3)
N. of components	19	12	7	24	15	9	22	17	5
Largest (%)	31 (17.4)	28 (34.1)	31 (32.3)	10 (12.7)	6 (13.6)	10 (28.6)	57 (23.4)	53 (37.3)	57 (55.9)
Density	0.039	0.085	0.072	0.030	0.042	0.091	0.013	0.022	0.031
Degree									
Average	6.887	7.000	6.833	2.405	1.864	3.200	3.393	3.535	3.196
Maximum	27	27	26	10	5	10	43	43	25

The first network (co-offending network) was generated by ties between financial scheme participants that were prosecuted together, i.e. linked actors were co-defendants in the same judicial case or co-suspects in separate but related criminal investigations. It must be noted that, although relying on criminal justice records as a proxy for criminal tie has some limitations because official data may not necessarily reflect actual co-offending behaviors, this approach is commonly used in social network research, and is considered fairly reliable (Coles, 2001; Morselli, 2009; Sparrow, 1991; Xu & Chen, 2008).

The co-offending network comprised 178 suspects (62.2 percent of the total 286 actors). For the most part, these were individuals accused of participating in an Islamic-related financial scheme (53.9 percent compared to 46.1 percent accused of participating in a far-right scheme). The majority of criminal associates were men (87.6 percent); only twenty-two women were prosecuted for a financial crime (12.4 percent), the majority of whom were involved in a far-right scheme (90.9 percent compared to a mere 9.1 percent in Islamic criminal networks). Far-rightists, Islamic extremists, and non-extremist associates were equally represented within the overall co-offending network as well as within the two ideological subsets (i.e., both far-right and Islamic sub-networks included approximately two-third political extremists and one-third non-extremists).

From a structural perspective, there appeared to be no significant differences between far-right and Islamic criminal networks. Overall, Islamic extremist component were fewer compared to far-right ones, but included a larger number of people, consistently with what we previously observed for the overall network. The low density value within the co-offending network (0.039, or 3.9 percent) indicates that criminal connections were sparse. It is interesting to notice that density was higher in criminal networks than in family and business networks, suggesting that connections occurred more frequently within criminal rather than legitimate settings. As noted, because density is affected by network

size, it is not the most reliable measure of social cohesion (deNooy et al., 2005). The degree centrality, on the other hand, seems to confirm this trend. Suspects in far-right and Islamic criminal networks had an average degree of 7.0 and 6.8, which is higher than corresponding values in both family and business networks (respectively: 1.8 and 3.2 in family networks; 3.5 and 3.2 in business networks). This suggests that financial scheme participants within far-right and Islamic subsets had a larger number of associates through criminal rather than family or business ties. These findings, however, should be taken with caution, as they may be an artifact of the way we defined criminal association. We shall return to this point later in this chapter.

The second network (family network) was created by linking individuals who were related by marriage or kinship tie. For this relationship type, we adopted a broad approach referring to the concept of extended family to include all immediate and non-immediate relatives who participated in a financial scheme (i.e., partners, siblings, cousins, etc.). About 27 percent of all actors were related through family ties. The majority were involved in a far-right financial scheme (55.7 percent compared to 44.3 percent in Islamic-related schemes). Consistently with previous research (Malm et al., 2010), a greater percent of women were found in this network (23 in total, or 29.1 percent); once again, the majority of female participants were involved in far-right related schemes (78.2 percent compared to 21.8 percent involved in Islamic schemes). As previously noted with regard to the co-offending network, the proportion of far-rightists, Islamic extremists, and non-extremist associates linked by blood or in-law relationship was similar, although unexpectedly we found a considerable number of non-extremists in radical Muslim families. Connections were thicker within Islamic extremist families compared to far-right ones, indicated by density values of 0.091 (or 9.1 percent of all possible ties) and 0.042 (or 4.2 percent of all possible ties), although we have to keep in mind once again that density decreases with

increased network size. On average, actors within the far-right subset had a degree centrality of 1.86, whereas actors in Islamic sub-sets had an average degree centrality of 3.20. This suggests that overall family networks were decentralized and composed of smaller clusters.

The third network was formed by actors that shared a legitimate business relationship, including individuals working in the same company, co-owning a property, sharing professional services, and so forth. Interestingly, this was the largest network, consisting of a total of 244 individuals (85.3 percent of the total 286). Unlike the co-offending network, which was composed for the most part of actors involved in Islamic-related financial schemes, the business network included a majority of participants in schemes perpetrated by the far right (58.2 percent compared to 41.8 percent). Female involvement in business relationships was also noted, although in smaller percent compared to the family network (only 15.6 percent). Once again, the majority of women were part of a far-right scheme (92.1 percent).

Probably the most interesting finding from this descriptive analysis concerns the number of political extremists compared to non-extremists present in the business network. Unlike what we observed with respect to the co-offending and family networks, here we notice a disproportionate involvement of non-extremist associates (52.9 percent), followed by far-rightists (27.0 percent), and lastly Islamic extremists (20.1 percent). About 60 percent of non-extremists were involved in far-right financial schemes, while the remaining 40 percent took part in an Islamic-related financial scheme. Notice that the only incident indicating a collaborative venture between far-rightists and Islamic extremists, previously observed by inspecting the overall network graph, concerned a legitimate business relationship.

Business networks appeared to be the least cohesive of all three, indicated by density values that were below 3 percent (0.031). In other words, links between business associates were sparse, particularly within the far right. However, there were individuals who had very high degree centrality (i.e., 43 in the far-right subset and 24 in the Islamic one), suggesting that, although connections were rare, few actors attracted a large number of ties, which could be evidence of a core-periphery structure. In the following sections we further investigate these issues comparing structural and attribute characteristics of far-right and Islamic extremist co-offending, family, and business networks using Exponential Random Graph (p*) Modeling (ERGM).

6.2.1 Comparing social structures using Exponential Random Graph (p) Modeling (ERGM)*

In this dissertation, we advanced two hypotheses regarding multiplex relationships within financial extremist networks. Specifically, we argued that political extremists who engage in financial crimes will be associated with each other and non-extremist accomplices through three types of relationships (i.e. co-offending, family, and business ties), and that these relationships will form networks that are structurally different (Hypothesis 1). Additionally, we hypothesized the existence of homophily effects within family and co-offending networks, and heterophily effects shaping business networks (Hypothesis 2).

To determine whether our data support these hypotheses, we performed a series of statistical analyses using Exponential Random Graph Modeling (ERGM, or p* star models) with the software program *PNet* (Wang et al., 2004 & 2009). As previously discussed, this method involves simulating a probability distribution of random graphs from a starting set

of selected parameters to estimate whether certain structural characteristics observed in a given network are more prevalent than would occur by chance (Robins et al., 2007a; Wasserman & Pattison, 1996). The first step in this process involved choosing the structural parameters (or network configurations) for modeling our network data set. The four selected parameters were: (1) edge, indicating density; (2) alternating *k*-star, a higher-order parameter which is a measure of degree distribution, or centrality; (3) alternating *k*-triangles, a higher-order parameter measuring triangulation or transitivity, i.e. the tendency to form smaller cohesive clusters; and (4) alternating *k*-two paths, which is a precondition for transitivity and indicates flexibility (for a more in-depth description of these parameters, see Section 4.3.3). Additionally, we also included one binary actor attribute parameter (suspect status: 0=non-extremist, 1=political extremist) to test for social selection effects within the observed networks (i.e., homophily and heterophily effects).

Subsequently, we drew graphs at random with *PNet* simulating a distribution with the same number of nodes observed in the far-right and Islamic co-offending, family, and business networks, and finally examined whether or not these configurations were significant. When the network is complex and includes a substantial number of nodes and links, random graph simulations must be repeated several times until the model is stabilized (Harrigan, 2009). In this analysis, we ran 500 estimations for each of the six models, including three iterations per estimation, for a total of 1500 estimations per model. Once we reached model convergence, i.e. all parameters had a convergence *t*-statistic below 0.10, which is required to be able to interpret the results, we completed three more estimation runs with the obtained parameter estimates to make sure our results were stable (Wasserman et al., 2009).

ERG models provide parameter estimates (θ), standard errors for each parameter estimate (SE), and convergence *t*-statistics (*t*). Parameter estimates are standardized

measures that indicate the maximum likelihood for selected network configurations. They can have a positive or negative sign, depending on whether the specific structural configuration they represent is observed to a lesser or greater extent than it would have been expected by chance. The convergence *t*-statistic compares the observed number of the chosen configuration in the network with the mean number of configurations found in a sample of 500 graphs generated using the same parameter estimate (Harrigan, 2009). Significance, indicated by the value of the convergence *t*-statistic, is obtained when the absolute value of the parameter estimate is twice the magnitude of the standard error calculated for that parameter. Smaller values of the *t*-statistic, i.e. closer to 0, indicate the parameter has converged well (Robins et al., 2007b; Snijders et al., 2006). Finally, *PNet* provides goodness-of-fit statistics, which indicate how well the model fits the observed data as well as how well it would fit using other possible configurations not included in the model. This involves simulating the resulting parameter distributions including non-parameterized features of the graph, which is in fact considered a rather stringent test that "goes a considerable way beyond what is usual in more standard statistical approaches" (Snijders et al., 2006, p. 206).

Theoretical considerations and research objectives should drive researchers in the determination of what parameters should be used to compare goodness-of-fit estimations (Goodreau, 2007). Because of our primary interest in centrality and transitive effects within financial extremist networks, we chose two parameters explaining degree distribution, i.e. standard deviation and skew of the degree distribution, and two parameters explaining clustering patterns, i.e. local and global clustering. Parameterized configurations are considered a good fit to the model if the absolute value of their *t*-statistic is below 0.10. For parameters not included in the model, a *t*-statistic below 1 is considered a good fit, although absolute values that are less than 2 are considered not extreme (Harrigan, 2009).

The figures below provide a graphic representation of the six sub-networks here examined, optimized for visualization through Kamada-Kawai and Fruchterman Reingold spring-embedded algorithms, which are available in the SNA package *Pajek*. The following tables present the ERG models, including standardized parameter estimates, standard errors, and *t*-convergence statistics. The goodness-of-fit estimation is discussed last in conclusion of this section.

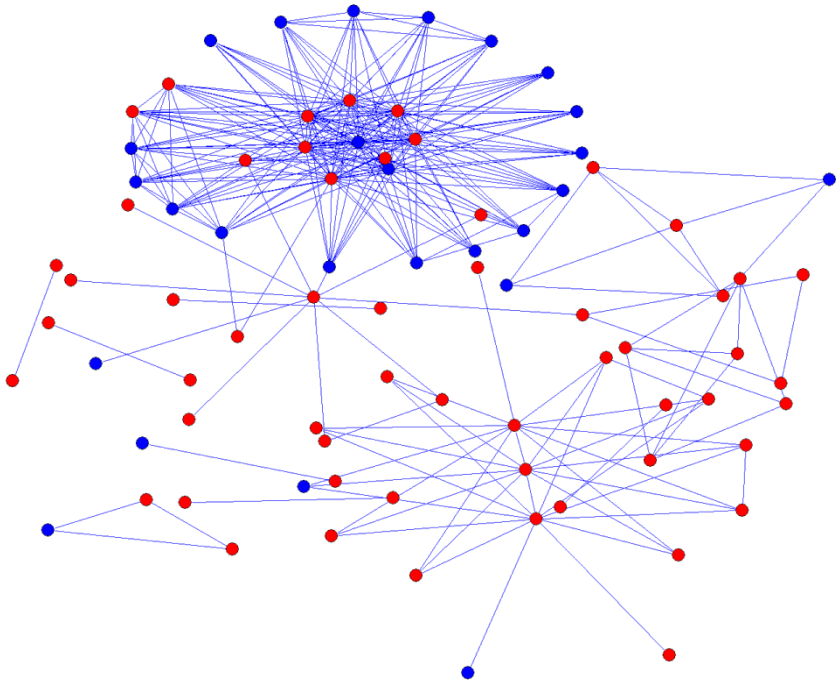


Figure 6.2 Far-right co-offending network (N=82)

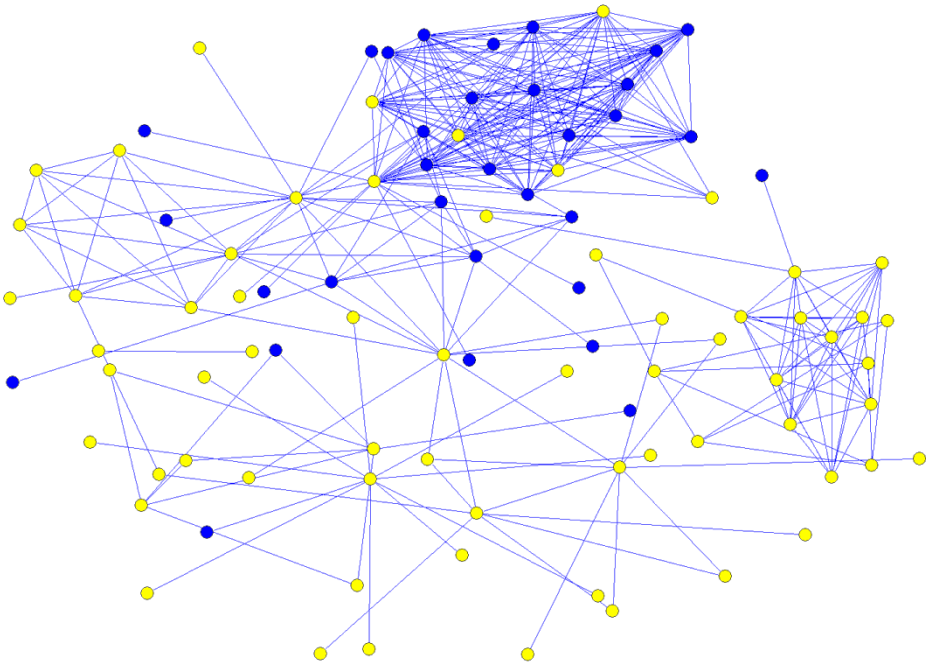


Figure 6.3 Islamic extremist co-offending network (N=96)

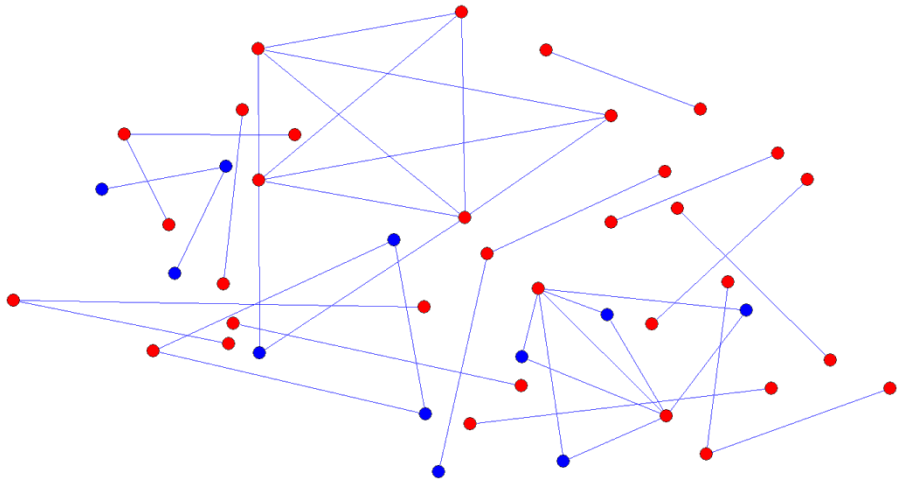


Figure 6.4 Far-right family network (N=44)

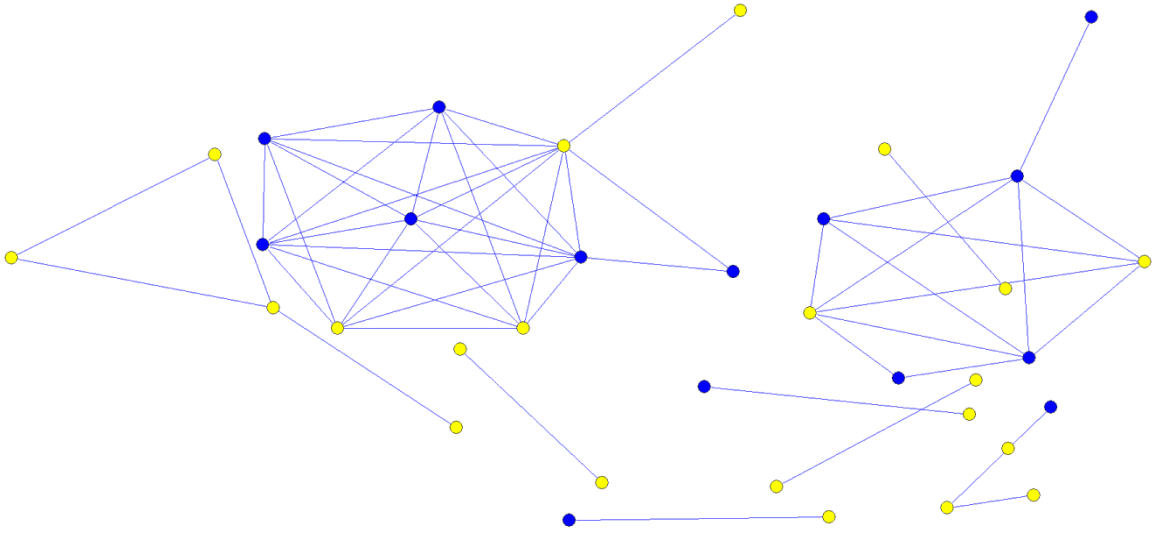


Figure 6.5 Islamic extremist family network (N=35)

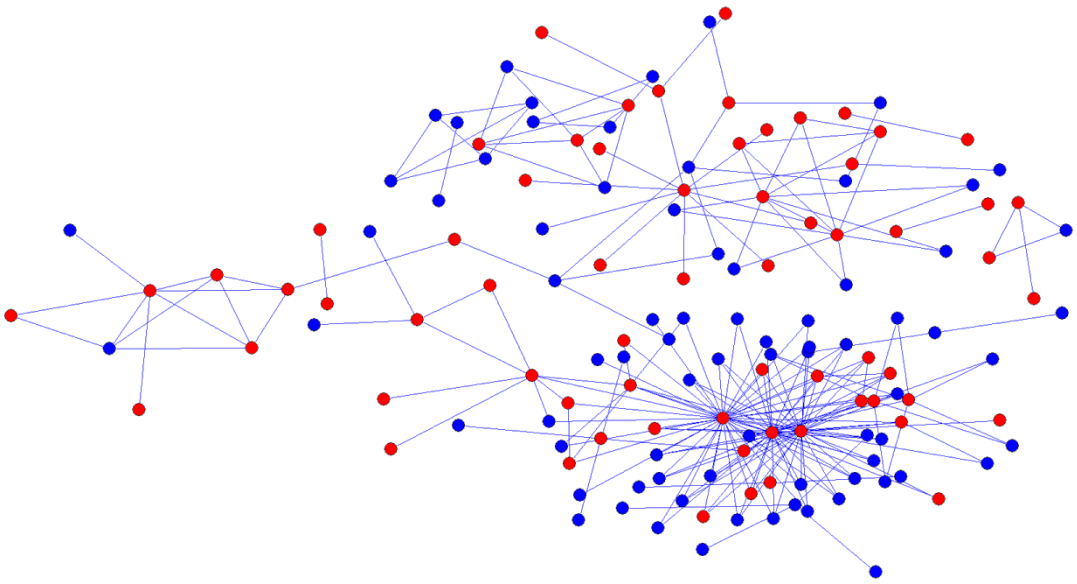


Figure 6.6 Far-right business network (N=142)

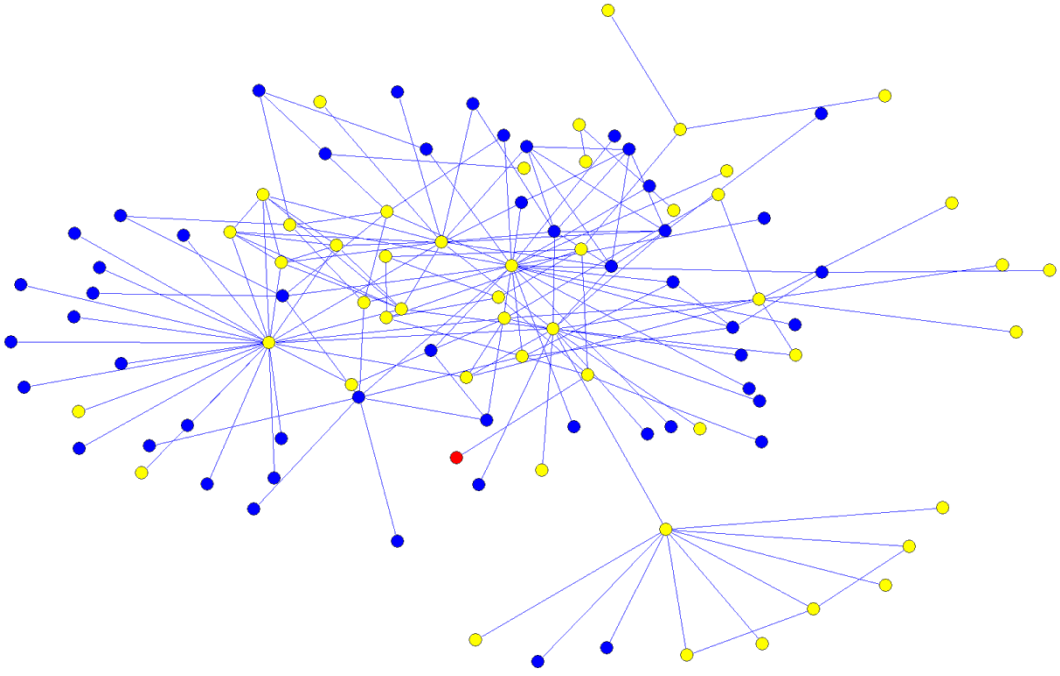


Figure 6.7 Islamic extremist business network (N=102)

Table 6.4 Parameter estimates, standard errors, and convergence *t*-statistics of ERGM comparing co-offending, family, and business networks by extremist ideology[1]

		Model 1 – Co-offending Network			Model 2 – Family Network			Model 3 – Business Network		
		Est.	**SE**	***t*-stat.**	**Est.**	**SE**	***t*-stat.**	**Est.**	**SE**	***t*-stat.**
Far-right Network	**Structural P.**									
	Edge	**-3.583**	**0.445**	**-0.03**	-2.101	1.290	0.01	**-3.604**	**0.406**	**-0.05**
	AK-star	**-1.165**	**0.127**	**-0.03**	-1.411	0.822	-0.01	**-1.105**	**0.139**	**-0.04**
	AK-triangle	**3.121**	**0.191**	**-0.03**	**1.994**	**0.350**	**-0.02**	**1.914**	**0.105**	**0.04**
	AK-2-path	DE	DE	DE	-0.383	0.509	-0.03	DE	DE	DE
	Attribute P.									
	Homophily	**0.606**	**0.191**	**-0.05**	-0.872	1.222	0.04	**-1.301**	**0.367**	**0.01**
	Heterophily	**-0.469**	**0.109**	**-0.04**	1.447	1.174	0.02	**1.542**	**0.309**	**0.03**
		Model 4 – Co-offending Network			**Model 5 – Family Network**			**Model 6 – Business Network**		
		Est.	**SE**	***t*-stat.**	**Est.**	**SE**	***t*-stat.**	**Est.**	**SE**	***t*-stat.**
Islamic Extremist Network	**Structural P.**									
	Edge	**-3.541**	**0.332**	**-0.05**	**-2.025**	**0.733**	**-0.04**	**-3.770**	**0.314**	**0.02**
	AK-star	**-1.039**	**0.098**	**-0.05**	-0.008	0.219	-0.04	**-0.312**	**0.130**	**0.02**
	AK-triangle	**2.858**	**0.163**	**-0.05**	**1.452**	**0.236**	**-0.04**	**1.366**	**0.133**	**0.01**
	AK-2-path	DE	DE	DE	**-0.652**	**0.154**	**-0.01**	DE	DE	DE
	Attribute P.									
	Homophily	**0.933**	**0.012**	**-0.05**	-0.263	0.680	0.01	**0.716**	**0.287**	**-0.03**
	Heterophily	**-0.628**	**0.064**	**-0.05**	0.235	0.459	-0.02	-0.252	0.179	-0.01

[1]Bold: significant; DE: degenerate or near-degenerate model.

6.2.2 Hypothesis 1

To review, this statistical analysis was meant to determine how co-offending, family, and business ties among financial scheme participants could be explained on the basis of four structural statistics and one covariate, i.e. suspect status. Hypothesis 1 argued that there would be structural variations between co-offending, family, and business networks involving far-right and Islamic extremists. From a visual perspective, the six sociograms

lend support to this hypothesis. More specifically, in both far-right and Islamic co-offending networks a distinct core-periphery structure is apparent made of several overlapping cliques. Core members are highly connected among each other forming dense cohesive subsets, whereas peripheral members appear to be more distant but still organized in cliques. Similar structural characteristics can be noted in both business networks, although the far-right one has a more visible core compared to the Islamic one. The two family networks, on the other hand, appear to have a different structural patterning: in the far-right family network members form smaller cohesive clusters than in the Islamic one, which appears to be more densely connected.

To test for structural variations in a more systematic way, we ran a series of Exponential Random Graph Models, which allow for statistically determining whether certain configurations are more prevalent in the network than would occur by chance alone (Robins et al., 2007a). Before we start interpreting the findings, it is important to notice that all six models successfully converged for this data set, although we had to modify our initial specification for the co-offending and business networks by dropping the fourth parameter (alternating *k*-two paths) because the models did not converge, i.e. they were degenerate. As previously mentioned, model *degeneracy* or *near degeneracy* occurs when the model estimation can only find nearly complete (e.g., very high density) or nearly empty (e.g., very low density) networks (Handcock, 2003; Harrigan, 2008). This is not uncommon, especially when complex network settings are examined, and may indicate the need to better refine the model using parameters that are more theoretically sound. Additionally, Snijders et al. (2006) maintain that more research should be conducted on the effects of including the alternating *k*-two-paths parameter in stochastic models, as it is not always clear how it interacts in association with other parameters.

This comparative analysis revealed interesting similarities and differences across far-right and Islamic networks formed through different relational ties. The simplest configuration (*edge),* which indicates the level of group cohesion or density, appears to be negative and significant in five out of six models, suggesting that fewer connections are observed than would have been expected by chance, while holding the other parameters constant. This is in accordance with previous discussions concerning the typical low level of social cohesion found within covert networks (McGloin, 2004; Morselli, 2009; Natarajan, 2006).

Consistently with the findings from our exploratory analysis, business networks involving far-rightists and Islamic extremists appeared to be the least cohesive (i.e., Model 3: θ=-3.604, SE=0.406; Model 6: θ= -3.770, SE=0.314). This suggests that business connections are loose and it is more difficult for information or commodities to circulate once business associates are removed. Similarly, co-offending networks also exhibited fewer connections than expected by chance (i.e., Model 1: θ= -3.583, SE=0.445; Model 4: θ=-3.541, SE=0.332). Far-right and Islamic family networks, on the other hand, were the most cohesive, suggesting that family bonds are a better "glue" than business and criminal associations (Malm et al., 2010). It must be noted, however, that the estimate for the far-right model became non-significant when we included the alternating-*k*-triangles parameter (Model 2: θ = -2.101, SE = 0.290; Model 4: θ = -2.025, SE = 0.733). These results have important policy implications which will be discussed in the next chapter.

The higher-order parameters should be interpreted conjointly as they describe different structural patterning depending on whether they are significant and positive or negative (Robins et al., 2007b). Once again, we found unexpected similarities between co-offending and business networks across ideologies. All four models exhibited positive and significant values of the alternating-*k*-triangles parameter (i.e., Model 1: θ = 3.121, SE =

0.191; Model 3: θ = 1.914, SE = 0.105; Model 4: θ = 2.858, SE = 0.163; Model 6: θ = 1.366, SE = 0.133), which indicate the presence of transitivity and clustering effects. Additionally, the alternating-*k*-stars parameter was negative and significant in all four models ((i.e., Model 1: θ = -1.165, SE = 0.127; Model 3: θ = -1.105, SE = 0.139; Model 4: θ = -1.039, SE = 0.098; Model 6: θ = -0.312, SE = 0.130), suggesting a tendency against degree centralization.

The combination of positive *k*-triangles and negative *k*-stars parameters presents a unique patterning structure which can be interpreted as evidence that two countervailing tendencies are present: "one towards a triangulated core-periphery structure and one against a degree-based core-periphery structure" (Snijders et al., 2006, p. 205). A core-periphery structure implies the existence of two distinct regions in the network, i.e. one that includes a dense and cohesive subset of actors, and another one where connections are looser and sparse (Borgatti & Everett, 1999). This pattern was, in fact, already noted by visually inspecting the four sociograms.

Network researchers maintain that this particular structure may form in two ways, i.e. (a) as a result of a strong centralization process, indicated by the presence of "hubs", i.e. prominent actors that attract most of the other ones, or (b) due to high triangulation, suggesting the presence of a large number of overlapping cliques (i.e., groups of three maximally connected actors). When the *k*-triangles parameter is positive and the *k*-stars parameter is negative, as exhibited in our data, there is a tendency from centralization to segmentation, suggesting that the core-periphery structure is a result of transitivity and clustering effects rather than actor's popularity (see Snijders et al., 2006). This trend is particularly evident within far-right and co-offending networks, as indicated by the large and opposite values of *k*-triangles and *k*-stars parameters. The smaller *k*-triangles and *k*-stars parameter estimates within far-right and Islamic business networks, on the other

hand, confirm a core-periphery tendency due to triangulation rather than popularity effects, but not for a segmented network (Robins et al., 2007b).

In short, far-right and Islamic co-offending networks exhibit a similar decentralized and segmented structure. Both networks present a distinct core of highly connected actors and a periphery of loosely connected ones; however, this is not because of prominent actors in the core who attract everybody else, but due to a chain of overlapping cliques (i.e. triangles) forming smaller regions of densely internally connected actors. In other words, criminal association occurs within separate, small, and leaderless groups. High triangulation can also be interpreted as an indication of strength provided by the overlapping ties between smaller actor subsets, suggesting that these networks are more resilient to external attacks (Malm et al., 2010). It is important to notice, however, that this may be partially an artifact of our operational definition of criminal tie, which referred to criminal justice records.

A similar pattern can be observed within business networks involving both far-rightists and Islamic extremists, which appear to be decentralized and displaying a distinct core-periphery structure as a result of high triangulation. The only difference from the co-offending networks is that the clustering tendency through overlapping cliques is more uniform across the network, as indicated by the lower values of the alternating-*k*-triangles parameter. Hence, business exchanges can spread out more easily from core to peripheral members, although the absence of central actors may delay such exchanges.

Structural variations can be found within far-right and Islamic familial networks, too. While holding the other parameters constant, both networks show a tendency toward transitivity, evidenced by the positive and significant values of the alternating-*k*-triangles parameters (i.e., Model 2: θ = 1.994, SE = 0.350; Model 5: θ = 1.452, SE = 0.236). As discussed, high transitivity effects can be interpreted as an indication of clustering and

strength. This is quite typical within family networks, which by definition tend be more cohesive and close-knit than other social network types. Additionally, the alternating-*k*-two paths parameter in the Islamic model, which represents a prerequisite for transitivity, is also significant but negative (Model 5: θ = -0.652, SE = 0.154). A negative alternating-*k*-two paths parameter in conjunction with a positive alternating-*k*-triangles parameter can be interpreted as a tendency against 4-cycles, or triadic closure (Malm et al., 2010). This means that there are few individuals in the network who could be easily replaced without affecting information flows within the network. In other words, although this network structure is strong and difficult to penetrate because of a predominance of small and tight subgroups, if one member was to be eliminated, information flows would be interrupted.

As mentioned, the edge parameter in the far-right model became non-significant once we factored in triangular effects. This suggests that connections occurred more significantly within higher order parameters, i.e. in groups involving at least three individuals rather than within dyadic relationships. These findings are supported by a visual inspection of the sociograms and additional information from the open-source materials, which further revealed that participants in far-right financial schemes involved mostly nuclear families (mother, father, and children), whereas Islamic networks involved extended families including non-immediate relatives, as well (e.g., cousins, in-laws, etc.).

6.2.3 Hypothesis 2

In recent years, the criminological debate concerning interactions between ideologically motivated and profit-driven offenders has intensified (Dishman, 2005; Hutchinson & O'Malley, 2007; Makarenko, 2004; Picarelly & Shelley, 2007; Shelley &

Picarelli, 2005; Williams, 2008). However, very few studies have explored this issue in a systematic way providing empirical evidence of the seemingly growing crime-terror nexus. This dissertation focuses on a specific setting, i.e. the financial crime sector, which according to some experts provides fertile ground for new criminal ventures thanks to lax security mechanisms, the existence of numerous offshore tax havens, and the relative easiness to commit these crimes (Bequai, 2002). Our previous descriptive analysis lends support to this assertion, which is further corroborated by a visual inspection of the six sociograms illustrated in Figures 6.2 to 6.7. However, the complexity of these social settings requires further examination.

For these purposes, we fitted two social selection models using ERGM to test whether similarities and differences in suspect status were more or less likely to lead to a tie, provided that a tie was observed (Robins et al., 2001). As mentioned, one of the benefits of using ERG modeling to study network structures is that it allows for testing the ability of attribute characteristics to explain properties of the network independently of the structural parameters (Shumate & Palazzolo, 2010). Hence, the structural configurations discussed above must be considered in the light of the results of the present analysis.

Social selection assumes that connections form more easily between individuals who display certain characteristics. When two social partners share the same trait (e.g. race, gender, education, etc.), homophily effects are said to be shaping their relationship (Cook et al., 2001; Goodreau et al. 2009; Wimmer & Lewis, 2010). On the opposite, two persons who become associated on the basis of their individual differences (e.g., different political opinions, different social background, etc.) are believed to be a product of heterophily (Burt, 2001; Everett, 1962; Lin, 2005). Homophily brings strength and security, but also isolation, whereas heterophily brings innovation and progress, but also increased risk exposure.

In this study, we first tested social selection within financial extremist networks under Hypothesis 2, which posited that co-offending, family, and business network structures would be influenced by suspect status (0 = non-extremist, 1 = political extremist). More specifically, we maintained that business relationships would be affected more by heterophily rather than homophily effects. In this sense, business associations between extremists and non-extremists should occur more frequently than expected by chance. On the contrary, we expected family and co-offending ties between financial scheme participants to arise among similarly motivated individuals. In other words, we hypothesized that political extremists would associate more significantly with family members and co-offenders who shared similar ideological goals.

Parameter estimates for homophily and heterophily effects are reported in Table 6.3, together with standard errors, and convergence *t*-statistics. The results of this analysis provide partial support to Hypothesis 2, although parameter estimates differ strongly across networks. In the previous ERGM structural analysis, we noticed how co-offending networks involving far-rightists and Islamic extremists exhibited a similar segmented core-periphery structure as a result of the tendency for actors to form smaller cohesive clusters. Controlling for these structural effects, we found positive and significant homophily effects within both graphs (Model 1: θ = 0.606, SE = 0.191; Model 4: θ= 0.933, SE = 0.012) as well as negative and significant heterophily effects (Model 1: θ = -0.469, SE = 0.109; Model 4: θ = -0.628, SE = 0.064), consistently to what hypothesized.

This suggests that collaborative structures based on co-offending ties do not arise merely because of a triadic tendency, but also because of homophilous selection among political extremists, reinforced by an opposite tendency of political extremists to not associate with non-extremists. In other words, in perpetrating a financial scheme, far-rightists tend associate with other far-rightists, and Islamic extremists tend to associate

with other Islamic extremists. Importantly, we must keep in mind that criminal association was defined as being prosecuted in the same judicial case or in separate but related criminal investigations. Hence, these results may simply indicate that political extremists were prosecuted together with other political extremists rather than with non-extremists.

Contrary to what he hypothesized, social selection did not have a significant impact on family structures, as both homophilous and heterophilous parameters in Model 2 and 5 were non-significant. This means that the structural properties previously observed, i.e. triangulation and clustering, were not affected by suspect status, and that there are organizing principles that go beyond homophilous or heterophilous selection in the creation of cliques (Snijders et al., 2006). In other words, participation in financial criminal activities by family members is not dependent on political extremists choosing to ally with similarly motivated individuals, but on the exclusive, close-knit structures that are typical of these social network types.

With respect to business relationships, we previously noticed a distinct self-organizing formation in both far-right and Islamic networks produced by a chain of close-knit triads. Controlling for these structural effects, we found that the heterophily parameter in the far-right model was positive and significant (Model 3: θ= 1.542, SE = 0.309), whereas the homophily one was negative and significant (Model 3: θ = -1.301, SE = 0.367). This lends partial support to our hypothesis that extremist/non-extremist collaborations would be prevalent within business settings. However, this trend exists only within the far-right setting, while the opposite is observed for business relationships among Islamic extremists. Homophilous selection significantly contributes to tie creation, when controlling for other structural effects, whereas heterophily effects were not significant (Model 6: θ= 0.716, SE = 0.287). Hence, we can infer that, although non-extremist associates are present in business networks of both far-rightists and Islamic extremists, collaborations tend to occur primarily

with far-rightists, whereas Islamic extremists tend to rely on each other when conducting businesses.

6.2.4 Goodness-of-fit estimation

In conclusion of this first ERGM analysis, it is important to take a look at the goodness-of-fit (GOF) estimation for the six models, which is reported in the table below.

Table 6.5 Goodness-of-fit statistics for far-right and Islamic extremist ERGM

	Far-right ERGM			Islamic Extremist ERGM		
	Model 1	**Model 2**	**Model 3**	**Model 4**	**Model 5**	**Model 6**
Graph counts						
Edge	-0.07	-0.03	-0.04	0.05	-0.05	0.06
AK-stars	-0.07	-0.04	-0.04	0.05	-0.05	0.05
AK-triangles	-0.07	-0.03	-0.04	0.05	-0.04	0.06
AK-2-path	-0.79	-0.08	1.33	-0.61	-0.06	0.70
Homophily	-0.02	-0.01	-0.03	0.03	-0.07	0.04
Heterophily	-0.04	-0.03	-0.04	0.03	-0.06	0.05
Degree distribution						
Standard deviation	0.88	1.61	2.84	0.63	0.63	1.46
Skew	0.48	3.92	6.90	-0.51	1.91	5.53
Clustering						
Global	1.48	-0.05	-4.10	3.37	0.84	-0.89
Local	1.33	-0.92	2.00	1.06	-0.70	0.68

As mentioned, goodness-of-fit statistics indicate how well the model fits the observed data as well as how well it would fit using other possible configurations not included in the model. Parameterized configurations are considered a good fit to the model

if the absolute value of their *t*-statistic is below 0.10. For parameters not included in the model, a *t*-statistic below 1 is considered a good fit, although absolute values that are less than 2 are considered not extreme (Harrigan, 2009).

The GOF estimation reveals that all six models fit our data well, i.e. all *t*-statistics for the selected parameters, both structural and attribute, are below 0.10. Additionally, the *t*-statistic value for the alternating-*k*-two paths parameter, which was dropped because of model degeneracy problems in Model 1, 3, 4, and 6, was also reasonable (three values below 1, and one value below 2). However, there are variations as regards GOF statistics for non-parameterized structures across models, i.e. degree distribution and clustering effects, suggesting that there may be configurations that would better explain these features of the observed network. Specifically, only Model 1 (far-right co-offending network) and Model 5 (Islamic family network) explained degree distribution and clustering well, indicated by a goodness-of-fit index between 1 and 2 for parameters not included in the model. Models 2, 3, and 6, on the other hand, do not do a particular good job in explaining the degree distribution. In particular, the observed far-right business network has a more dispersed and skewed degree distribution than Model 3 would suggest (respectively: t = 2.84; t=6.90). Both far-right family and Islamic business networks appear to be more skewed than suggested by Model 2 and 6 (respectively: t=3.92; t=5.53). Finally, global clustering indexes are higher in the observed far-right business and Islamic co-offending networks than those predicted by Models 3 and 4 (respectively: t=-4.10; t=3.37), suggesting that transitivity effects could be better explained using different structures.

To conclude, although overall our six models provide a good fit to our data as regards the selected parameters, we must notice that there are additional features that are not captured as well with these configurations (Snijders et al., 2006). In future research, we

intend to experiment with a different combination of lower and higher-order parameters to identify models that better explain these network structures.

6.3 Efficiency-security trade-offs and the role of non-extremist associates

Previous research shows that covert networks' structures vary greatly depending on a variety of factors, including the type of criminal activities, long-term and short-term objectives, actors' characteristics, and so forth (Antonopoulos, 2008; Bruinsma & Bernasco, 2004; Krebs, 2002a & 2002b; Levi, 2008b; Morselli, 2009; van der Hulst, 2009). In particular, different security-efficiency trade-offs appear to be important organizing factors for covert networks (Baker & Faulkner, 1993; Morselli et al., 2007).

Trust and secrecy are fundamental components of illegal conspiracies, as members must protect themselves and their illicit activities from internal (e.g., competitors, customers, etc.) and external threats (law enforcement, watchdogs, etc.; see: Baker & Faulkner, 1993; Erickson, 1981). However, even covert networks must function, and therefore a balance must be found between security and efficiency. According to Morselli (2009), criminal and terrorist networks are self-organizing structures that follow a "flexible order", adapting the number and type of interactions to specific situational circumstances which may require different efficiency-security trade-offs and "time-to-tasks". Morselli further argues that covert networks pursuing ideological goals (e.g., terrorist cells) have longer time-to-tasks than those aiming at profit-oriented objectives (e.g., drug trafficking organizations), because they are "less often in action" and put therefore more emphasis on security rather than efficiency (pp. 65).

From a social network perspective, different goals and security-efficiency trade-offs are reflected in different structural characteristics. A covert network that favors security over efficiency is likely to be dispersed and decentralized, with members separated by longer distances to guarantee insulation. On the contrary, when efficiency is more important than security, the network will present a more centralized structure that facilitate information flows, but puts its members more at risk of being detected. For example, the action segment of the 9/11 network reconstructed by Krebs (2002a) comprised a small subset of individuals (the 19 hijackers) who were positioned further apart. Upon closer look, however, this segment appeared to be surrounded by another subset of "dormant" facilitators who provided "shortcuts" and increased efficiency by means of financial and logistical resources right before the attacks were executed. Morselli and Roy's (2008) analysis of a drug trafficking network found evidence of a completely different structural patterning, characterized by a central core of ringleaders who directed operations and a number of peripheral members who carried out street-level activities. Hence, this criminal network was structured as to sacrifice some degree of security in favor of a more efficient configuration with shorter paths between core and periphery members.

In this dissertation, we argued that structural variations due to different efficiency-security trade-offs occur not only between criminal and terrorist networks, but also *within* different types of ideologically driven covert networks (Hypothesis 3). Specifically, we hypothesized that financial criminal networks involving far-right tax protesters would exhibit a more centralized structure that favors efficiency over security as a result of lesser risk associated with non-violent ideological goals, further strengthened by their firm ideological convictions. On the contrary, we argued that Islamic extremists participating in a financial scheme to finance terrorism activities would be embedded in more dispersed and decentralized structures that enhance security and insulation of key members.

Additionally, in Hypothesis 4, we argued that these structural properties would also be affected by different social selection processes: far-rightists involved in tax avoidance schemes should be more prone to establish contacts with non-extremist criminal associates (heterophilous effects), whereas Islamic extremists involved in terrorism financing operations should be more reluctant to involve individuals who are not ideologically motivated (homophilous effects). The following sections describe how we examined and tested these hypotheses using exploratory network analysis and Exponential Random Graph (p*) Modeling (ERGM).

6.3.1 Exploring cohesive subsets

For social network researchers, structure is the key to understand how social entities of any type function (Scott, 2000). Our society is based on interpersonal ties between people that share information, interests, attitudes, goods, and so forth. Within this overall structure of interpersonal relationships, smaller configurations are formed that can either enhance or restrict these exchanges. Social network analysis provides a set of measures and methods that allow for examining cohesive subsets within larger network formations and explaining how they affect specific social settings. Similarly, covert networks can also be partitioned into smaller subgroups involving co-offenders who collaborate closely with each other toward a specific objective (Xu & Chen, 2008).

To determine whether structural variations existed between far-right and Islamic financial networks aiming at different ideological goals, we extracted the two largest cohesive subsets (i.e., one component per ideology) from the overall network of *egos* and *alters* and examined their structural and attribute characteristics. For this analysis, we

aggregated the three separate relational ties (i.e. co-offending, business, and family tie) into a single binary linkage, which was operationalized as the exchange of goods (e.g., money, products, etc.) or services (e.g., labor, legal advice, etc.) in furtherance of an illegal financial scheme. This approach is consistent with previous research exploring the topology of covert networks (Albert & Barabasi, 2002; Xu & Chen, 2008). Because of the problem of "fuzzy" boundaries and possible missing data, small-scale groups are considered better settings, especially when using network modeling techniques, which are based on the assumption that networks are complete (Krebs, 2002; Malm et al., 2010; Sparrow, 1991). Additionally, some network- and actor-level measures, e.g. closeness centrality and centralization, can only be estimated for maximally connected sub-graphs. In other words, the network cannot contain isolates or other disconnected sub-sets (Knoke & Yang, 2008).

Summary statistics of the two largest components are provided in the table below.

Table 6.6 Description of far-right and Islamic largest components

	Far-right		Islamic	
	N	Percent	N	Percent
N. of nodes	56	19.6	65	22.7
Egos vs. alters				
Egos	15	26.8	19	29.1
Alters	41	73.2	46	70.8
Status				
Extremist	26	46.4	36	55.4
Non-extremist	30	53.6	29	44.6
Gender				
Male	38	67.9	64	98.5
Female	18	32.1	1	1.5

The two components appeared to be similar in size and composition of *egos* and *alters*. The far-right one included 56 actors and was generated by 15 individuals (26.8 percent of the total 56) who were formally charged for their involvement in a financial scheme (i.e. *egos).* The Islamic one was composed of 65 individuals, of whom 19 had been formally indicted (29.1 percent). There are differences, however, as regards the proportion of men and women as well as extremist and non-extremist members. The far-right subset involved for the most part men, although a noticeable number of women participated as well (38, or 67.9 percent, compared to 18 women, or 32.1 percent). The Islamic subset instead included only one female. Consistently with our previous findings, non-extremists were more numerous in the far-right subset (30, or 53.6 percent, compared to 26, or 46.4 percent in the Islamic one), while political extremists were more numerous in the Islamic component (36, or 55.4 percent, compared to 29, or 44.6 percent in the far-right one).

Additional information from the open-source materials retrieved during data collection revealed that the far-right subset represented a tri-tiered multi-level marketing organization that actively promoted and sold bogus trusts and anti-tax packages, including books, tapes, and tickets to offshore seminars, over a period of five years. The IRS-led investigation focused on five individuals, considered to be the founders, and a number of associates, including managers, directors, promoters, and local sellers. Therefore, it provided an ideal case study to represent a financial network aiming at non-violent, ideological goals. The sociogram of this anti-tax marketing network (illustrated in Figure 6.8) reveals a relatively centralized structure with a core of individuals in the center (*egos*, represented by circles) connected to a large number of *alters* (visualized as triangles), both extremists and non-extremists, and another subset of *egos* and *alters* extending in the periphery. Interestingly, although this was allegedly a three-tiered marketing structure, here we can only see two tiers. This is possibly an artifact of our data set, which employed

an ego-centric design. It is also likely that the open-source materials used to create the network did not include information on the "smaller fish", who were last in the marketing chain. In fact, their inclusion in the network could be problematic, as the same people who were drawn in the scheme to promote bogus anti-tax products were probably victims themselves.

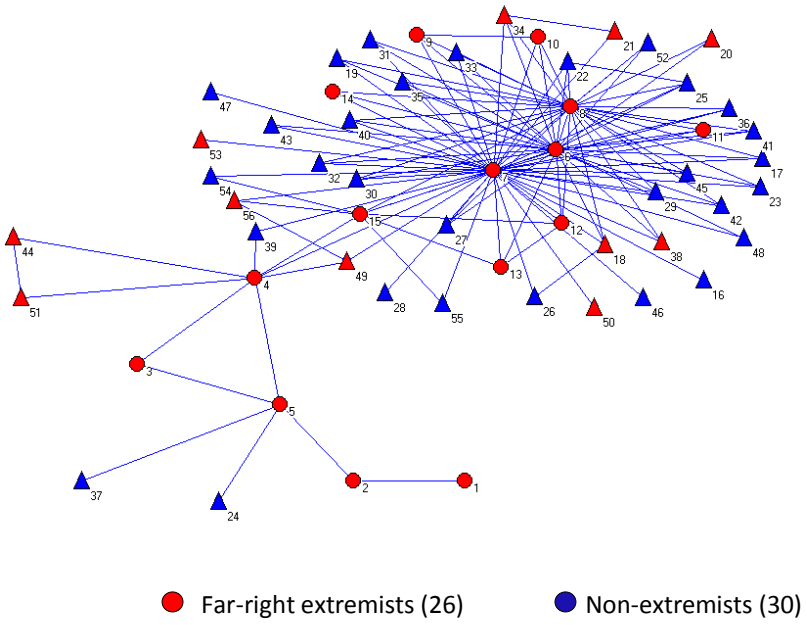


Figure 6.8 Far-right anti-tax marketing network

According to the open-source documents, the Islamic component comprised a variety of individuals, including the founders and directors of US-based Islamic charitable organizations, prominent businessmen, specially designated terrorists, political leaders, and other foreign nationals, who allegedly participated in a series of related money-dirtying and money-laundering schemes aimed at raising funds to support terrorist activities in Palestine and Saudi Arabia. Hence, it fits the type of financial criminal network aiming at violent, ideological objectives needed for our comparative analysis. The corresponding

sociogram (visualized in Figure 6.9) displays an interesting patterning, which appears to be more diversified compared to the far-right one. Consistently with previous research, this terrorism financing network appears to be dispersed and highly clustered (Krebs, 2002a & 2002b; Morselli, 2009). It is also possible to notice a tendency toward a separation between extremist and non-extremist clusters.

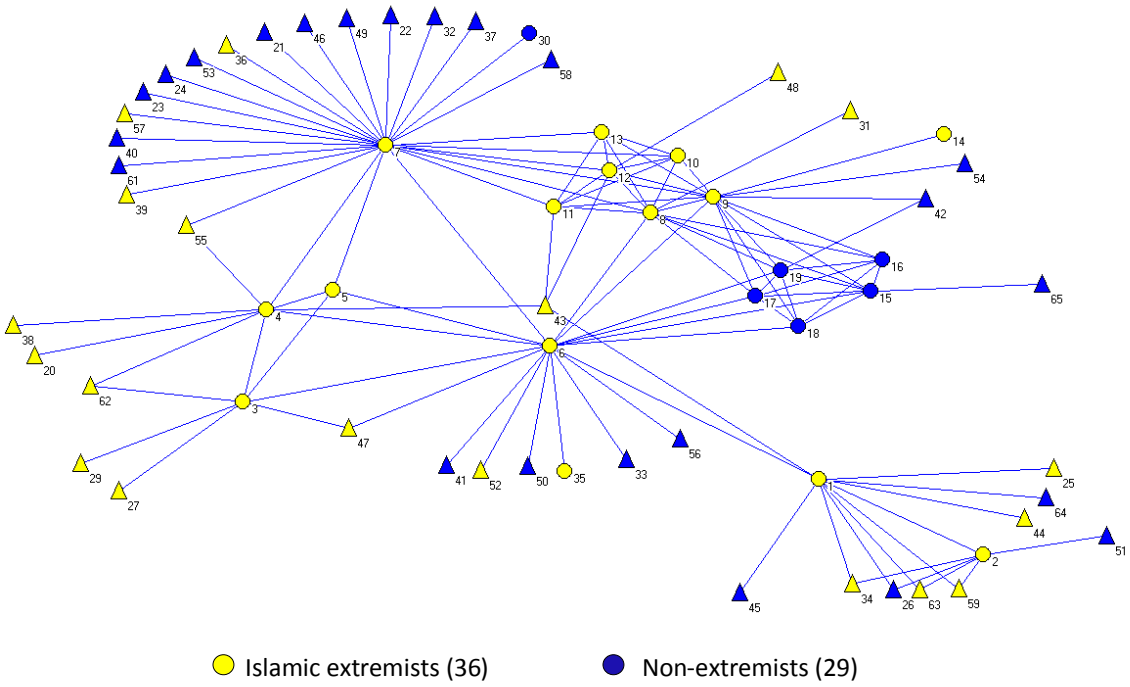


Figure 6.9 Islamic terrorism financing network

An exploratory analysis of cohesive subsets usually starts with an assessment of connectedness and centrality (Krebs, 2002a & 2002b; Morselli, 2009; Natarajan, 2006; Sageman, 2004). As discussed, centrality can be examined from a macro- and micro-level perspective, depending on whether the unit of analysis is the network at large or the actors that are part of it. Centralization indexes are macro-level measures that allow for determining whether or not a certain network is centralized around key individuals. The

table below provides cohesion and centralization measures comparing the anti-tax marketing network with the terrorism-financing one.

Table 6.7 Cohesion and Centralization in far-right and Islamic components

	Far-right	Islamic
	N	N
N. of nodes	56	65
N. of edges	130	119
Density	0.084	0.057
Degree		
Average	4.618	3.661
Maximum	46	26
Centralization		
Degree	0.779	0.361
Closeness	0.716	0.434
Betweenness	0.657	0.488

As noted, the two networks were similar in size but different in many aspects. As hypothesized and confirmed by eyeballing the sociograms illustrated in Figures 6.8 and 6.9, the far-right network was considerably more cohesive and centralized than the Islamic one, which appeared to be more dispersed and decentralized. Density in the anti-tax marketing network was 0.084, indicating that 8.4 percent of possible ties linked the network members, while the Islamic one had a density value of 0.057, indicating that only 5.7 percent of ties were present. Low density values are consistent with previous research on covert networks, which tend to be more dispersed than legitimate social networks because of security concerns and, possibly, missing data. Because density is inversely related to network size, we also examined average degree, which is the average number of direct contacts each

network member has. Here again we notice slightly higher values in the far-right network, suggesting that overall its members had more direct contacts than those in the Islamic one (nearly 5 compared to 4).

Comparing centralization indexes provide additional insight into the two network structures. As mentioned, degree centralization measures the network tendency to be more or less centralized taking into account variations within all actor degree centralities. The larger value in the anti-tax network (0.779 or 77.9 percent) compared to the terrorism financing one (0.361, or 36.1 percent) suggests that there was more variation in actors' degree centralities in the first compared to the second one. High degree centrality in social networks can be interpreted as an indication of power and leadership. In covert networks, however, it can also indicate higher visibility and vulnerability. Translated to our setting, this means that the anti-tax network was more centralized around a few prominent individuals with many direct ties which made them central but also more vulnerable to external attacks. The terrorism financing was instead decentralized; there was no prominent actor attracting more attention than others. These issues are discussed more in depth in the following section.

Interestingly, the anti-tax network was very high in closeness centralization (0.716, or 71.6 percent), suggesting the existence of central actors who were not only powerful because of many direct connections, but also because they were able to reach more people through shorter paths. These could be individuals who act as "reference points" for other actors and provide "a center of attention whose views are heard by larger numbers of actors" (Hanneman & Riddle, 2005). Closeness centralization was also high in the terrorism financing network (0.437, or 43.7 percent), suggesting that variations existed in the distribution of distances between actors. Finally, both networks had high betweenness centralization values (respectively 0.657, or 65.7 percent, and 0.488, or 48.8 percent). In

fact, this is where the terrorism financing network appeared to be most centralized, although to a lesser extent compared to the far-right one. High betweenness centralization values indicate larger variations in actors' betweenness centrality measures. In other words, consistently with previous studies on covert networks, there appear to be individuals who function as bridges in the financial extremist networks here studied, controlling information flows and providing strategic alliances (Morselli & Roy, 2008).

Unfortunately, centralization measures provide only limited information concerning network structural patterning. Additionally, centrality measures are sensitive to changes in network size, hence if new actors were to be found, the results would considerably be altered (Krebs, 2002a). To overcome these issues and further investigate structural and attribute differences between the two subsets, testing Hypotheses 3 and 4, we performed a new ERGM analysis following the same procedure described in Section 6.2. Table 6.7 presents the results of this analysis, including standardized parameter estimates, standard errors, and *t*-convergence statistics for each one of the two models. Goodness-of-fit statistics are discussed in this chapter's final section.

Table 6.8 Structural and attribute parameter estimates, standard errors, and convergence *t*-statistics of ERGM in financial criminal networks[1]

	Model 1 – Far-right component			**Model 2 – Islamic extremist component**		
	Estimate	**SE**	***t*-stat.**	**Estimate**	**SE**	***t*-stat.**
Structural P.						
Edge	**-4.009**	**1.250**	**0.01**	**-4.240**	**0.481**	**-0.02**
AK-star	**-1.354**	**0.294**	**0.02**	-0.003	0.180	-0.01
AK-triangle	**1.692**	**0.188**	**0.02**	**0.754**	**0.169**	**-0.01**
AK-2-path	DE	DE	DE	**0.067**	**0.009**	**-0.03**
Attribute P.						
Homophily	**-3.967**	**1.061**	**0.03**	**0.280**	**0.111**	**-0.01**
Heterophily	**4.126**	**1.019**	**0.02**	-0.167	0.156	-0.01

[1]Bold: significant; DE: degenerate or near-degenerate model.

6.3.2 Hypothesis 3

In this dissertation, we argued that criminal networks involving individuals who aim at ideological goals are not all structured in the same way. More specifically, we hypothesized the existence of structural variations between far-right and Islamic financial criminal networks as a result of the different ideological goals pursued (i.e. non-violent ideological protest for the former, financing violent political action for the latter) which require distinct security-efficiency trade-offs (Hypothesis 3). In this sense, the anti-tax marketing network involving far-rightists should display a more cohesive and centralized structure that favors efficiency over security, whereas the Islamic terrorism financing one should look more dispersed and decentralized including smaller cohesive subsets for enhanced security and insulation from outside threats.

This hypothesis was tested by running a series of ERGM simulations on the far-right and Islamic subsets described above using the same structural parameters previously discussed, i.e. : (1) edge, indicating density; (2) alternating *k*-star, a higher-order parameter which is a measure of degree distribution, or centrality; (3) alternating *k*-triangles, a higher-order parameter measuring triangulation or transitivity, i.e. the tendency to form smaller cohesive clusters; and (4) alternating *k*-two paths, which is a precondition for transitivity and indicates flexibility.

The results of this structural analysis lend partial support to Hypothesis 3, i.e. there appeared to be meaningful variations in the way the far-right anti-tax network was structured compared to the Islamic terrorism financing one, although the picture described through this analysis appears to be more complex than expected. Before interpreting the findings, we must point out that both models successfully converged, although once again we had to drop the fourth parameter (alternating *k*-two paths) in Model 1 because of

degeneracy problems (Handcock, 2003; Harrigan, 2009). As previously noted, although this higher-order configuration was developed to capture important transitivity effects within complex network settings, scholars maintain that more research is needed to better understand how it should be interpreted in interaction with other ERGM parameters (Snijders et al., 2006).

Model 1, representing the far-right anti-tax marketing network, included three parameters (edge, alternating *k*-stars, and alternating *k*-triangles), which were all significant, i.e. the parameter estimates were more than twice the value of their standard errors. As expected, while holding the other parameters constant, edges occurred relatively rarely, indicating a low level of connectivity among network members (θ = - 4.009, SE = 1.250). Interestingly, the far-right network presented a structural patterning that was similar to the co-offending and business networks described in the previous section. Model 1 found a large and positive value of the alternating-*k*-triangles parameter (θ = 1.692, SE = 0.188) in combination with a smaller and negative value of the alternating-*k*-stars parameter (θ = -1.354, SE = 0.294). As noted, a positive *k*-triangles parameter combined with a negative *k*-stars parameter suggests the existence of two competing tendencies within the network, i.e. "one towards a triangulated core-periphery structure and one against a degree-based core-periphery structure" (Snijders et al., 2006, p. 205). This pattern is evidence of a distinct core-periphery structure due transitivity and clustering effects rather than actor's popularity, suggesting the existence of several smaller regions (possibly connected) of triangulation and a tendency against central actors, or "hubs" (Snijders et al., 2007). Those that are in the core are not there because of many direct connections but because of their indirect connections to many smaller cohesive clusters. In simple terms, exchanges of goods and services within the anti-tax network occurred through a segmented process facilitated by many close-knit interactions rather than through a centralized

structure. This patterning indicates a strong self-organizing structure that will be difficult to disrupt given the overlap of ties (Malm et al., 2010).

Model 2, representing the Islamic terrorism financing network, included all four parameters, although only three were significant, i.e. edge, alternating *k*-triangles, and alternating *k*-two paths. The negative density ("edge") parameter indicates that, holding the other parameters constant, fewer connections than expected are observed in this network in general as well as compared to the far-right one (θ = -4.240, SE = 0.481). This provides support to our hypothesis that Islamic extremist networks in our data set would be less cohesive than far-right networks as a result of their need to emphasize security over efficiency. The alternating *k*-stars effect was not significant, and must therefore not be interpreted. The positive and significant alternating *k*-triangles (θ = 0.754, SE = 0.169) and *k*-two-paths (θ = 0.067, SE = 0.009) parameters indicate a tendency toward transitivity and flexibility, net of the density effect (Snijders et al., 2006).

As previously mentioned, a positive *k*-triangles parameter, although small, suggests regions of high triangulation indicating a core-periphery structure that is formed through a chain of overlapping cliques. The smaller but positive value of the alternating *k*-two-paths parameter in conjunction with the larger and positive value of the alternating *k*-triangles parameter provides evidence for pressures to transitive closure (Snijders et al., 2006). A positive *k*-two-path parameter indicates a tendency toward 4-cycles in the network, which resemble the decentralized "chain" network structure previously described. This means that, although there is a tendency toward clustering in close-knit structures within the network, the preconditions exist for forming new triadic relationships. In other words, in the terrorism financing network, members tend to interact within smaller and safer clique-like structures that are independent of central actors. However, some of these sub-sets are not fully closed, i.e. not all actors are connected, but display some degree of flexibility

leaving open the possibility to form new collaborations. This decentralized patterning is not optimal for communication flows, but it enhances security and elasticity; even if one of the actors were to be eliminated, this would probably not cause the network's disruption.

In conclusion, when considering all of the abovementioned results, Hypothesis 3 garners moderate support from our ERGM analysis. As hypothesized, the far-right network, which involved tax protesters and profit-driven individuals participating in an anti-tax marketing scheme, displayed a more cohesive structure compared to the Islamic terrorism financing one. However, both networks displayed a tendency toward a decentralized core-periphery structure as a result of triangulation effects, i.e. the tendency to form smaller cohesive clusters, rather than centralization around key actors. In particular, the far-right network was more segmented, which could be a result of the multi-tiered structure typical of the type of marketing fraud perpetrated. Moreover, the Islamic network was not only decentralized, including strongly connected cliques, but also more flexible. We can therefore argue that, with respect to the two financial criminal networks here examined, none of the actors in the core are essential for the network functioning. In practical terms this means that, given the overlap of ties, strategies aimed at the network disruption will be difficult for both. We shall remand to the next chapter for a more in-depth discussion of these findings.

6.3.3 Hypothesis 4

As previously noted, including covariates that represent actor attributes in stochastic estimations of network structures is an important development of ERG modeling, as network formation is a complex process that requires evaluating whether certain structural configurations are sustained while accounting for exogenous processes (Snijders

et al., 2006). In our final hypothesis, we argued that financial extremist networks aiming at violent and non-violent ideological goals would also be influenced by social selection processes based on suspect status. Specifically, we hypothesized a predominance of heterophily effects within anti-tax, far-right networks, and the opposite trend, i.e. a prevalence of homophily effects, within Islamic terrorism financing networks. Parameter estimates for homophily and heterophily effects are reported in Table 6.7, together with standard errors, and convergence *t*-statistics.

An examination of the findings lends support to Hypothesis 4. Controlling for structural effects in the far-right subset, the homophily parameter was negative and significant (θ = -3.967, SE = 1.061), whereas the heterophily parameter was significant and positive (θ = 4.126, SE = 1.019). We can infer that collaborative structures in this network, which tend to occur within smaller cohesive subsets, arise because of significant interactions between far-rightists and non-extremist associates. In the Islamic subset, on the contrary, only the homophily parameter was positive and significant, although its value was small (θ = 0.280, SE = 0.111), whereas the heterophily parameter was not significant. Hence, collaborations in the terrorism financing network occurred more significantly among political extremists than would have been expected by chance.

In conclusion, we can argue that non-extremist associates appear to be more important for the creation of ties within an ideological but non-violent financial crime setting, rather than an ideological and ultimately pro-violence fund-raising network. It is important to point out that certainly we cannot generalize this conclusion to all possible far-fight and Islamic extremist financial networks. However, this is a first step toward developing a more sophisticated analytical framework to examine the different facets of what is still an obscure phenomenon, i.e. the convergence of political extremism and profit-driven crime.

To gain further insight on these issues and investigate the role of non-extremists within financial extremist networks, we conducted an actor-level analysis focusing on their relational properties. Understanding how various actors are positioned in the network and in relation with one another can reveal many important aspects of the network functioning and vulnerabilities. From a social network perspective, actors' importance is equated with power and centrality, as "power is inherently relational" (Hanneman & Riddle, 2005). The most popular approach focuses on three types of centrality measures (Freeman, 1979), i.e.: (a) degree centrality, which refers to the number of direct ties each actor has; (b) closeness centrality, which includes indirect ties and measures the *geodesic distance* between nodes, i.e. the length of the shortest path connecting a dyad, or pair of actors (Knoke & Yang, 2008); and (c) betweenness centrality, which reveals "cut-points" or "brokers", i.e. actors who bridge otherwise unconnected part the network (McGloin, 2005).

Actor centrality analysis has been used frequently by researchers interested in covert networks. For example, Baker and Faulkner (1993) found that individuals who had high degree centrality in three price-fixing conspiracies received more guilty verdicts than individuals who were peripheral. Hence, they concluded that degree centrality in covert networks may result in higher visibility and risk of being targeted. Closeness centrality instead reveals the ability to access others in the network and monitor activities. Krebs (2002), for instance, found that distances between the 9/11 hijackers decreased once facilitators joined in, creating shortcuts and allowing for faster and more efficient coordination right before the attacks were executed. Betweenness centrality, on the other hand, is considered the strongest indicator of sophistication and organization within a covert network (Morselli, 2009). Brokers (i.e. individuals with high betweenness centrality) control information asymmetries, and are therefore manipulators that can create or destroy connections within the network (McGloin, 2005).

We have already examined macro-level aspects of network centralization, noticing how the far-right anti-tax network and the Islamic terrorism financing network appeared to be organized differently: the former exhibited a more cohesive and highly centralized structure, whereas the former appeared to be sparse and decentralized. This distinction was only partially confirmed by our ERGM analysis, which instead revealed some similarities between the two subsets, and more specifically a tendency toward high clustering and triangulation resulting in a unique type of core-periphery structure that does not depend on popular actors but rather the presence of many overlapping cliques. Finally, we noticed that non-extremists positively contributed to tie formation only within the far-right setting, whereas Islamic extremists preferred to associate with individuals who were similarly motivated.

Next, we looked at actor centrality measures to identify key players in financial extremist networks. If non-extremists were truly important for financial schemes, their structural position within the network should provide positive evidence in the form of higher centrality scores. The table below provides normalized degree, closeness, and betweenness centrality scores in the far-right and Islamic subsets. Centrality scores were calculated for all participants, i.e. 56 nodes in the anti-tax network and 65 in the Islamic terrorism financing one. However, only the most central participants are displayed. The following figures compare their distribution within far-right and Islamic subsets. While interpreting the findings, we also refer to information obtained from the open-source documents, which provide valuable insight.

Table 6.9 Normalized degree, closeness, and betweenness centrality scores in the far-right and Islamic subsets[1]

	Node	Degree	Node	Closeness	Node	Betweenness
Rank						
1	7	0.836	7	0.797	7	0.670
2	6	0.600	6	0.611	4	0.262
3	8	0.545	8	0.591	5	0.141
4	15	0.164	4	0.529	6	0.125
5	4	0.145	15	0.519	8	0.095
6	5	0.091	*49*	*0.487*	2	0.036
7	12	0.091	***39***	***0.482***	15	0.029
8	9	0.073	12	0.466	*49*	*0.002*
9	10	0.073	10	0.462	*34*	*0.001*
10	***25***	***0.073***	***22***	***0.462***	*18*	*0.001*
	Node	**Degree**	**Node**	**Closeness**	**Node**	**Betweenness**
Rank						
1	7	0.406	6	0.577	6	0.509
2	6	0.297	7	0.552	7	0.485
3	9	0.234	9	0.492	1	0.287
4	8	0.187	8	0.481	4	0.131
5	1	0.172	4	0.471	9	0.127
6	4	0.156	5	0.451	3	0.079
7	3	0.141	1	0.430	8	0.068
8	12	0.125	12	0.430	12	0.039
9	**17**	**0.109**	11	0.427	*43*	*0.039*
10	**19**	**0.093**	**19**	**0.410**	**15**	**0.034**

Bold: non-extremist; Italic: *alter*

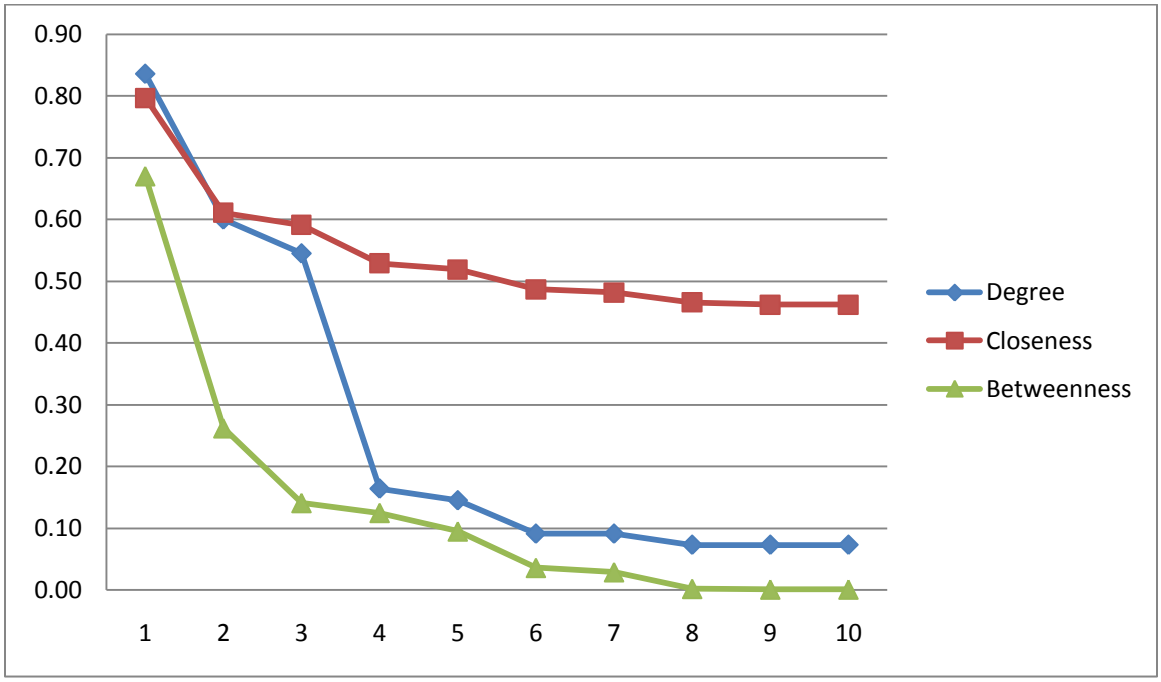


Figure 6.10 Degree, closeness, and betweenness centralities in the anti-tax marketing network

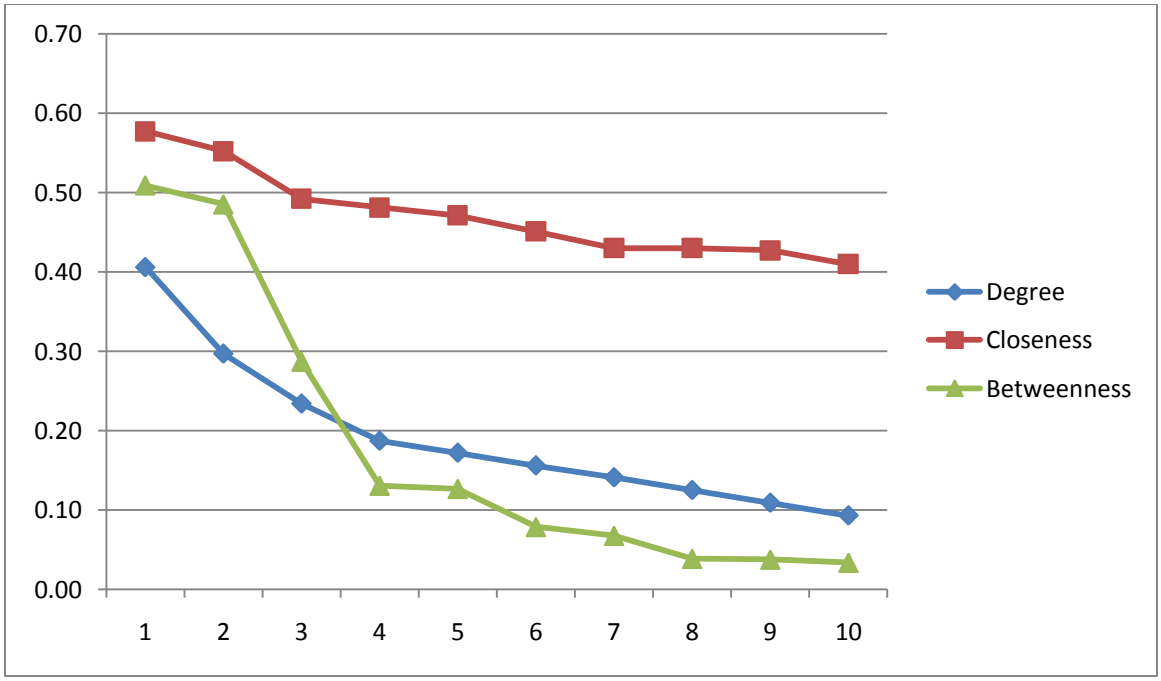


Figure 6.11 Degree, closeness, and betweenness centralities in the terrorism financing network

The anti-tax network appeared to be centered on three key participants, all political extremists and co-defendants in the anti-tax marketing scheme, who scored highest on all measures of centrality (N7, N6, and N8). Interestingly, Morselli (2009) described a very similar patterning in the drug trafficking network he studied, which he accurately redefined as "an overlap between the networks of these three key participants" (p. 77).

According to the open-source documents, these three actors were the founders of the anti-tax marketing scheme, and were all convicted as primary suspects. It is interesting to notice, however, that the criminal indictment that sparked the investigation mentioned two additional suspects, who were also convicted as scheme leaders (N9 and N10). This assessment does not find support in our analysis, which puts these two individuals in a rather marginal position, as can be noticed by inspecting the sociogram in Figure 6.8. The three key actors were not only the ringleaders, sharing direct connections with several other members; they were also able to reach out to a larger number of people, which means they were able to communicate their decisions and ideas easily throughout the network.

This finding is particularly interesting considering the pivotal role of far-right ideological propaganda for spreading anti-government strategies by means of economic sabotage. Only the primary ringleader (N7), however, was also the most important broker in the network, facilitating connections among more distant subsets. Right after him, we found two far-rightists (N4 and N5) who were strategically positioned in between the majority of actors and a smaller subset. According to the open-source documents, N4 and N5 were not involved in the primary anti-tax marketing scheme, but were associated with some of the promoters and subsequently started their own spin-off scam. This helps understand the unique conformation of the graph, which displays a peripheral extension expanding "westwards". We will return to this point in the concluding chapter, when

discussing the limitations inherent in analyzing network structures from a cross-sectional rather than longitudinal perspective.

As anticipated, among the most central actors we also found a few non-extremist associates, although none of them in a brokerage position. In fact, most played the role of "intermediaries" and "reference points" (see closeness centrality scores for N39 and N22). Finally, we also identified central individuals who had not been targeted by law enforcement (i.e. they were *alters).* Interestingly, three *alters* were network brokers (see betweenness centrality scores of N49, N34, and N18). This suggests that criminal justice authorities may have focused on the obvious ringleaders, underestimating the importance of political extremists who were less immediately visible but perhaps more dangerous "crossovers" (McGloin, 2005; Williams, 2001).

When compared to the anti-tax network, the terrorism financing network provided a very different image of network centralization and actor centrality. Degree centrality scores were lower than closeness and betweenness centrality scores, suggesting the absence of clearly identifiable ringleaders. On the contrary, reachability was highest and relatively consistent across all participants. However, it is actor betweenness centrality that stands out, suggesting the existence of many brokerage positions. This network was also centered on two key participants, coincidentally having the same node number as those in the far-right network (N7 and N6). Their most important characteristic was not having many direct ties, but rather being reference figures (high closeness centrality) and connectors (high betweenness centrality). In real life, too, these two key players were charismatic personalities: N7 was the president of a large US-based Islamic charity and N6 was a senior member of Hamas. Similarly to the far-right network, two non-extremist associates were also important players with many direct ties (see degree centrality scores of N17 and N19), although they were not in top positions. Finally, we must notice that these

findings are in accordance with the assessment by criminal justice authorities. In investigating this terrorism financing network, the prosecutorial strategy was especially comprehensive, leaving "no criminal behind", as suggested by the fact that the top central actors were all *egos,* except for one individual (N43) who was a broker but was never indicted.

In conclusion, the actor-centered analysis did not provide much insight into the role of non-extremists in financial criminal networks, although their significance was highlighted by our ERGM analysis, at least with respect to the far right subset. We remand to this study's final chapter for a more in-depth discussion of this point including recommendations for future research efforts.

6.3.4 Goodness-of-fit estimation

To conclude, we present the results of the goodness-of-fit (GOF) estimation for the two models comparing structural and attribute properties of a far-right anti-tax network and an Islamic terrorism financing one, reported in the table below.

Table 6.10 Goodness-of-fit statistics (*t*-ratio) for far-right and Islamic extremist ERGM

	Model 1 – Far-right component	Model 2 – Islamic Extremist component
Graph counts		
Edge	0.01	0.05
AK-star	0.01	0.05
AK-triangle	0.01	0.06
AK-2-path	3.99	0.06
Homophily	-0.01	0.04
Heterophily	0.01	0.05
Degree distribution		
Standard deviation	5.41	0.51
Skew	6.20	0.05
Clustering		
Global	-6.79	1.48
Local	4.61	0.55

As mentioned, goodness-of-fit statistics indicate how well the model fits the observed data as well as how well it would fit using other possible configurations not included in the model. Parameterized configurations are considered a good fit to the model if the absolute value of their *t*-statistic is below 0.10. For parameters not included in the model, a *t*-statistic below 1 is considered a good fit, although absolute values that are less than 2 are considered not extreme (Harrigan, 2009).

Similarly to our previous estimation modeling multiplex networks, the GOF shows that both models explained well the selected structural and attribute parameters, i.e. all *t*-statistics were below 0.10. Additionally, the non-parameterized configurations in Model 2 were also a good fit to the data: standard deviation and skew of the degree distribution as well as global and local clustering coefficients were all below 2 (Snijders et al., 2006). In other words, we can infer that this model accurately describes the structural and attribute characteristics of the observed Islamic terrorism financing network.

However, Model 2 fails to provide a plausible explanation for non-parameterized structures, i.e. alternating-*k*-two-path parameter, standard deviation and skew of the degree distribution, global and local clustering coefficients had larger than 2 values. This means that, although the parameterized configurations were able to partially describe the examined anti-tax far-right network, there are other important structural processes that are not captured with this model. Future work should introduce additional or alternative explanations to account for these network dimensions (Shumate & Palazzolo, 2010).

CHAPTER 7. DISCUSSION AND CONCLUSIONS

The relationship between political extremism and profit-driven crime has recently become a topic of interest for academics and a growing concern for policy-makers. Although the empirical literature is sparse, proposing a variety of sometimes conflicting perspectives, scholars seem to agree as regards two current trends: (a) political extremism and profit-driven crime converge in a variety of ways which are dependent upon situational factors, such as specific needs and objectives, available resources, and opportunities for interaction (Hamm, 2007; Horgan & Taylor, 2003; Hutchinson & O'Malley, 2007; Makarenko, 2004; Picarelli & Shelley, 2007; Shelley & Picarelli, 2005; Williams, 2008); and (b) political extremists and profit-driven individuals are seldom organized within rigid, hierarchical structures, but tend instead to form loose networks, whose size and structural patterning vary substantially (Antonopoulos, 2008; Dishman, 2005; Krebs, 2002a; Levi, 2008b; McGloin, 2004; Morselli, 2009; Natarajan, 2006; Sageman, 2004; Xu & Chen, 2008).

This dissertation addressed both of these issues collectively by focusing on the financial crime sector in the United States, which provided an ideal venue for examining whether and to what extent political extremism and profit-driven crime converge. The following sections outline these study's findings and discuss them more in depth in light of their implications for criminological theories, policy strategies, and methodological advances. In conclusion, we address some of the limitations inherent in this research and propose our future research agenda.

7.1 Discussion of study findings

7.1.1 Financial schemes, crimes, and techniques

Given the absence of empirical research in this study area, this dissertation's first goal was to produce knowledge on the different types of financial schemes, crimes, and techniques used by American far-rightists and Islamic extremists prosecuted in the United States. Although merely descriptive, this analysis was extremely informative, highlighting similarities and differences between the two ideological movements with respect to their *modus operandi* and providing insight into the strategies used to prosecute them. It is important to notice, however, that these findings cannot be generalized to the overall population of financial crime cases involving political extremists, given that our study universe was not obtained through random sampling procedures but provides instead a snapshot of judicial cases prosecuted in 2004.

This discussion is especially important in light of the innovative methodology used to collect and analyze financial crime data, which will be reviewed and further discussed for intellectual merit in the following sections. This dissertation is the first empirically based study that examines both legal and behavioral aspects of complex financial crime scenarios by breaking them down into three major components, i.e. (a) financial scheme, i.e. the ECDB main unit of analysis, which is defined as the overall illicit financial operation; (b) financial crimes, which refer to the specific criminal offenses charged by federal prosecutors (i.e. *legal component*); and (c) techniques, or methods used by the suspects to further the scheme (i.e. *behavioral component*).

From a scheme-level perspective, we noticed considerable differences between far-right and Islamic extremist cases. Consistently with previous research, the most typical far-

right financial scheme involved tax avoidance as a form of anti-government protest (Belli & Freilich, 2009; Pitcavage, 1996; Sanchez, 2009). This scheme type was carried out using techniques that involved proactive and passive behaviors. Proactive behaviors included filing false tax documents, underreporting income, using bogus trusts, marketing anti-tax packages, and setting up offshore "shell" corporations. Passive behaviors included ideologically motivated tax refusal, i.e. a popular crime of omission that involves the failure to file an income return or to pay employment taxes on the basis of misinterpretations of tax laws and the Constitution, usually rejected as "frivolous arguments" by the IRS and US Courts.

Islamic extremists appeared to be mostly involved in financial schemes to raise funds for terrorism-related activities through money dirtying and money laundering. Money dirtying (also called the "reverse" of money laundering) refers to the process of using money raised legitimately (e.g., through donations or legitimate investments) for illicit purposes (i.e., funding of terrorist operations). These findings are consistent with recent research, which argues that terrorism finances do not always come from illegal capital, subsequently transformed into expendable income through money-laundering acts, but are often obtained by legitimate means, including donations and legitimate business revenues, which are channeled to individuals or groups associated with foreign terrorist organizations (Compin, 2008; deKieffer, 2008; Masciandaro et al., 2007). This is also in line with a growing body of research which maintains that terrorists increasingly resort to financial crime for logistical as well as survival purposes (Kane & Wall, 2005; Hamm, 2007; Picarelli & Shelley, 2007; Shapiro, 2007; Smith & Damphousse, 1998).

Among the various methods employed, Islamic extremists made ample use of traditional money transfer mechanisms (e.g., wire transfers, bank accounts, cash deposits, checks, etc.) both domestically and internationally, and structured financial transactions to

avoid being detected (also called "smurfing"; Reuter & Truman, 2004). Funds were also channeled through US-based charitable organizations, although doubts remain as regards the validity of this finding due to the highly politicized nature of criminal prosecutions involving these entities (Gunning, 2008; Hardister, 2003). Comparatively, Islamic extremists used informal value transfer systems (IVTS) less frequently. As noted, counterterrorism initiatives have targeted these methods, which facilitate the movement of funds by avoiding paper trails (e.g. through cash transactions, cross-border cash smuggling, etc.) or through traditional money-transmitting practices (e.g., *hawalas*). Recent studies argue that government strategies put too much emphasis on regulating or suppressing ethnic-based practices that provide a reliable and cost-effective alternative to formal banking systems for many local communities (Grabbe, 2002; Passas, 2007).

Our analysis further revealed variations as regards the role of ideology within both far-right and Islamic related schemes. Although ideological motives, whether violent or non-violent, were important factors in the majority of far-right and Islamic related schemes, profit was also a defining element. This was not surprising as regards the far-right movement, which attracts a diverse crowd of more committed tax protesters as well as mundane offenders who mix political grievances with monetary benefits. It was, however, an unexpected result for Islamic related cases, although this lends partial support to the literature on the growing crime-terror nexus (Bovenkerk & Chakra, 2007; Dishman, 2005; Hutchinson & O'Malley, 2007; Makarenko, 2004; Shelley & Picarelli, 2005; Williams, 2008). Certainly, this is an indication that the traditional, rigid distinction between political extremism and profit-driven crime based on allegedly different motivational factors does not adequately describe these phenomena. This point bears significant theoretical and policy implications, which will be discussed next.

Finally, there appeared to be considerable differences in the way far-right and Islamic extremist financial crime cases were handled by federal prosecutors. Comparing criminal charges mentioned in the federal indictment, we noticed that far-right cases were usually prosecuted for typical financial crime offenses (e.g., tax evasion, mail fraud, money laundering, etc.). Indictments concerning alleged Islamic extremists instead included a variety of criminal charges, ranging from provisions especially created to combat terrorism financing methods (e.g. material support provisions introduced by the USA Patriot Act) to immigration fraud and false statements. As noted, these differences may be a by-product of the specific scheme types perpetrated within the two movements. Alternatively, it is possible that this has something to do with the unique historical circumstances when these prosecutions were initiated, and particularly the political agenda pursued during the post-9/11 "war on terrorism".

Taken collectively, these findings seem to suggest that the methods and motives followed by American far-rightists and Islamic extremists engaging in financial schemes give rise to two very distinct crime phenomena. The small sample, however, requires that we take this conclusion with caution, as similarities could emerge if the study universe were to be expanded. We leave this point for further exploration in future studies.

7.1.2 Extremist and non-extremist financial offenders

Comparing suspect-level characteristics offered additional insight concerning similarities and differences between far-right and Islamic-related financial criminality. First and foremost, this descriptive analysis certainly supports the hypothesis of a nexus between political extremism and profit-driven crime in the financial crime sector, as evidenced by

the large proportion of non-extremist associates involved in financial schemes. This point is emphasized by our network analysis' results, as discussed in the following sections.

Second, our data evidenced socio-demographic variations between American far-rightists, Islamic extremists, and profit-driven offenders. Consistently with previous research, we found that far-right extremists were older, on average, than both Islamic extremist and non-extremist suspects (Smith, 1994). Female participation was prevalent among far-rightists and non-extremists, although our network analysis revealed that this data should be taken with caution, as women may be involved in financial schemes through informal networks of familial ties which are not always captured by simply relying on law enforcement determinations. As a result, the role of women in Islamic related financial schemes may have been underestimated.

Far-rightists held qualified positions in typical white-collar jobs, such as tax preparation, financial and business consultancy, legal advice, etc. This lends preliminary support to Felson's claim (2002) that individuals who commit white-collar offenses take advantage of opportunities provided through their privileged access to professional knowledge. Islamic extremists were employed in a wider range of job sectors, from business management to college education, from public transportation to religious services, and so forth. As noted, this diversity may be related to various social, economic, cultural and situational factors (e.g. ethnic identity, immigration status, education level, religious participation, etc.), suggesting that financial crimes involving Islamic extremists may constitute a more complex scenario than far-right ones. More research is needed using statistical modeling to understand the relationship between employment and financial extremist crime, as suggested in conclusion of this chapter.

A large proportion of non-extremist suspects were professionals with expertise on legal, financial, and business matters, indicating that non-extremists may have been service

providers for financial extremist schemes. Recent studies on organized crime point to the pivotal role played by these secondary actors (e.g., lawyers, accountants, bankers, and real estate agents) who provide crucial resources to the primary actors involved in various criminal activities (Di Nicola & Zoffi, 2005; Kenney, 2007; Levi et al., 2005; Middleton & Levi, 2005; Morselli & Giguere, 2006). This dissertation supports this contention by providing empirical evidence that these facilitators played a major role in the execution of financial extremist schemes, too, as further discussed in the following network analysis section.

Although our definition of the American far-right movement was broad and encompassed a myriad of different groups and ideological belief systems, our data identified a specific segment, i.e. that of the so-called "Sovereign Citizens", which appeared to be disproportionately involved in financial criminal activities. Clearly, our small sample does not capture the entire universe of far-right financial offenders, but we can assert that far-right tax protesters are involved in promoting large-scale illegal behaviors that have already caused substantial economic harm to the U.S. government and its citizens. So far, this has not been a primary concern for policy-makers, and in fact recent budget cuts have further weakened the powers of the IRS, which is responsible for implementing tax compliance. We will return to this issue when we discuss this study's policy implications.

Financial schemes perpetrated by Islamic extremists primarily benefitted four terrorist organizations, i.e. Al Qaeda, Hamas, Hezbollah, and the Palestinian Islamic Jihad. While the first one is considered the "first multinational terrorist group of the twenty-first century" because of its global focus, the other three are concerned with local conflict situations in Palestine and Lebanon (Gunaratna, 2002, p. 1). This finding suggests that financial crimes committed within U.S. borders have the potential to not only harm the United States, but further ignite political turmoil abroad. Strategies aimed at preventing or

combating the problem, therefore, should have international resonance and not be merely concerned with domestic security matters.

Our descriptive analysis also focused on ideological commitment from a micro-level perspective. Similarly to what was observed at the scheme-level, we noted variations in the suspects' strength of ideological affiliation at the individual level, too. Ideological reasons frequently mixed with monetary concerns for both far-right and Islamic extremists involved in financial schemes, offering preliminary evidence that the convergence hypothesis might hold true (Belli & Freilich, 2009; Shapiro, 2007). At the same time, profit-driven offenders appeared to be driven by reasons other than profit, such as prestige and power. This finding suggests that the traditional and simplistic distinction between political extremists as ideologically motivated individuals and non-extremists as profit-driven offenders should be revisited because it does not accurately portray these complex social phenomena. This does not mean that ideology and profit should be excluded from the analysis, as they are important factors that help understand the nuances inherent in different suspects' decision-making processes and facilitate the development of targeted interventions. On the contrary, we argue that better categorizations are needed, which take into account variations in suspects' motives measuring them on a continuum line from pure ideology to pure profit instead of labeling suspects as either extremists (0) or non-extremists (1). We shall return to this discussion later in this chapter.

Finally, our analysis compared criminal justice outcomes for a number of far-rightists, Islamic extremists, and non-extremist suspects for which data were available. Once again, we noticed considerable differences in judicial outcomes concerning the three suspect types. In particular, we noted a tendency toward harsher treatment of Islamic extremists compared to far-rightists and especially non-extremists, who were treated most leniently. As some have argued, this may be an indication that the "explicit politicality" of

terrorist suspects may have influenced prosecutorial strategies, which became "tougher" to reflect post-9/11 guidelines to fight terrorism using all available means (Ascroft, 2004; Smith et al., 2002). Future research should look into these issues more in depth conducting multivariate statistical analysis on a larger sample of cases.

7.1.3 Financial extremist networks as self-organizing structures

Although our descriptive findings provided useful information to understand similarities and differences between far-rightists, Islamic extremists, and non-extremist suspects involved in financial schemes, the core of this dissertation consisted in an in-depth investigation of their relational ties, using various exploratory and statistical network modeling techniques to uncover hidden behavioral patterns and vulnerabilities that could ultimately direct and ameliorate policy interventions.

Criminologists have become increasingly interested in studying complex social phenomena, such as terrorism and profit-driven crime, through the lens of social network analysis (Krebs, 2002a & 2002b; Malm, 2007; Malm et al., 2010; McGloin, 2004 & 2005; Morselli, 2009; Natarajan, 2006; Sageman, 2004). As noted, social network analysis can be a very powerful investigative tool that allows for "systematically accumulating knowledge about the structural 'blue print' of criminal activity", thus improving "our understanding of their functioning and flaws" and ultimately leading to "effective ways to counteract and disrupt those networks" (Van der Hulst, 2009, p. 102).

One of the biggest advantages of this method is that it allows for exploring structural properties of social networks using different units of analysis. This dissertation focused on network-, subgroup-, and individual-level properties comparing far-right and Islamic

extremist structures. Furthermore, through a ground-breaking modeling technique (ERGM), which as of today has been employed in only two published criminological pieces (Malm et al., 2010; Young, 2010), we were able to determine how local structural configurations (e.g., edge, triangles, stars, etc.) impacted the global patterning of an observed network and test two social selection hypotheses using a binary actor-level attribute (i.e. suspect status as extremist or non-extremist) as covariate.

Summary network statistics revealed interesting preliminary findings. First of all, we immediately noticed the significant participation of non-extremist associates in financial extremist networks. Most of these actors were, in fact, identified as *alters*, i.e. individuals who had not been officially charged by criminal justice authorities. This finding suggests that law enforcement strategies may be too narrowly focused on prosecuting political extremists, underestimating the role of non-extremist associates. Moreover, it may also indicate a tendency to separate terrorism investigations from criminal investigations, a strategy that has been criticized as myopic by some experts (Dishman, 2005). In a similar fashion, we also noted that seeming "lone-wolf" offenders were in fact part of small cliques, frequently composed of the primary suspect's relatives, which had not been directly targeted by law enforcement. These findings emphasize the importance of expanding network exploration to informal contacts in order to provide a more comprehensive picture of financial extremist networks and be able to accurately identify hidden behavioral patterns and crime opportunity structures.

Looking at the results of our exploratory analysis, a variety of complex structural configurations emerged, consistently with previous research which argues that criminal networks, like other social networks, do not form at random, but follow instead identifiable patterns (Albert & Barabasi; Xu & Chen, 2008). By inspecting the sociograms and comparing network statistics, we observed the existence of several subsets of various sizes producing a

clear separation between far-right and Islamic extremist settings. In line with previous research, density coefficients were low across all examined networks, suggesting that overall financial scheme participants were not connected with many other actors in the network. This result may be due partially to missing data, a problem that unfortunately affects this type of research. Nonetheless, previous studies show that this is also a fundamental quality of illegal networks, whose members try to minimize the frequency of contacts to avoid being detected (Erickson, 1981; Hutchinson & O'Malley, 2007; Morselli, 2009).

Our ERGM analysis certainly confirmed that meaningful structural configurations existed within the observed far-right and Islamic extremist financial networks. Consistently with previous research, our data suggest that financial scheme participants were linked through at least three types of relational ties (i.e. co-offending, family, and business ties), forming networks that displayed various structural characteristics (Malm et al., 2010; McGloin, 2005; Sornecki, 2001). Interestingly, we discovered some unexpected similarities between far-right and Islamic co-offending, family, and business networks, as discussed below. First of all, networks formed through legitimate business relationships appeared to be the largest and least cohesive of all three types for both far-rightists and Islamic extremists, as indicated by the low density coefficients and confirmed by the *edge* parameter values. This means that, although a large of number of people engaged in exchanges of financial goods and services, connections were loose. This could be considered a structural weakness, because the limited connectivity prevents information from flowing easily across members, hence the elimination of key individuals may seriously compromise connections between the other members (Malm et al., 2010). Co-offending networks were similarly sparse, suggesting that financial scheme participants engaged in illegal activities with only a handful of associates. However, this may also be an artifact of our research

design, which used criminal justice determinations as a proxy for criminal ties. In other words, low connectivity among co-offenders may simply indicate that prosecutors charged suspects in small subsets. Finally, as expected, family networks were smaller compared to the other two types but more cohesive, suggesting that kinship was an important bond but only for a small number of far-rightists and Islamic extremists.

Second, and more interestingly, a common structural pattern emerged in all three network types across ideologies, i.e. the tendency toward a core-periphery structure due to high transitivity effects. As mentioned, in a core-periphery structure, individuals who are in the core are highly connected among each other and further linked to peripheral members, whose connections are looser and sparse (Borgatti & Everett, 1999). Because this patterning was caused by transitivity (i.e., the tendency for actors to form many overlapping cliques) rather than degree centralization, we inferred that the various networks were decentralized and highly clustered. This finding was not surprising with respect to familial networks, which are considered, by definition, strong and close-knit social settings. Hence, this particular configuration indicated the presence of "clans" of Islamic extremists and a small set of nuclear families of far-rightists involved in financial schemes.

What caught our attention, however, is that both far-right and Islamic extremist co-offending networks displayed a similar decentralized and segmented structure, suggesting that criminal associations occurred within small and separate "leaderless" settings. As previously noted, we must be cautious interpreting this finding as it may reflect prosecutorial strategies which targeted selected co-offending subsets together rather than actual behavioral patterns. Nevertheless, we noticed a similar patterning within both far-right and Islamic business networks, which were decentralized and highly clustered, suggesting that business associates interacted within small and close-knit structures. Therefore, even though it is possible that the triadic clustering within co-offending

networks may be partly influenced by law enforcement determinations, the fact that similar decentralized formations were found within business networks suggests that this is not only a byproduct of criminal justice strategies.

These unique structural features imply the absence of "hubs", or leaders, and the presence of a strong, self-organizing structure that is "essentially driven by the emergent behavior of its parts" (Morselli, 2009, p. 11). In other words, financial schemes by political extremists in our data set did not require leadership figures to be successfully executed, whether these be criminal, business, or family "bosses". Collaborations occurred in the context of small and cohesive cliques, which may not be ideal for efficiency purposes in the short run, but guarantee strong and safe settings in the long run. Trustful relationships better develop when all members know each other, because betrayal is more difficult (Tremblay, 1993; Weerman, 2003). At the same time, the continuity and success of this structure is insured by the overlapping cliques, which allow for small-scale exchanges to be replicated over and over again across the overall network. These complex relational patterns may be more resilient to law enforcement attacks, which traditionally aim at identifying and eliminating the most central actors (Krebs, 2002a; Klerks, 2001; Malm et al., 2010; McGloin, 2004; Morselli, 2009; Van der Hulst, 2008). More sophisticated analysis are required to understand their functioning and flaws, and it is possible that alternative disruption strategies, involving for example situational crime prevention measures, may be better suited than traditional investigation and prosecution approaches, as will be discussed later in this chapter.

The subsequent ERGM analysis comparing two large components aiming at different ideological goals, i.e. a far-right anti-tax network and an Islamic terrorism financing network, partially confirmed this interesting trend. Based on previous research, we hypothesized the existence of structural variations between far-right and Islamic financial

criminal networks as a result of different efficiency-security trade-offs. Specifically, we expected the far-right network to exhibit a more cohesive and centralized structure favoring efficiency over security, including distinct "hubs" functioning as reference points for other tax protesters, while the Islamic terrorism financing network should have displayed a more dispersed and decentralized structure, including smaller cohesive subsets for enhanced security and insulation from outside threats. Although we found support for this distinction through the exploratory network analysis, the statistical models provided a different picture.

Our data supported the hypothesis that the anti-tax network would be more cohesive than the Islamic one. Connections between participants in the tax avoidance scheme occurred more frequently than expected by chance compared to the terrorism financing network. However, contrary to our expectations, the far-right network was not centralized, and in fact its structural patterning resembled the self-organizing structure previously discussed. Once again, we observed a tendency toward clustering in closed triads, suggesting that exchanges occurred primarily within close-knit interactions between known individuals rather than through a centralized structure. The Islamic terrorism financing network displayed a similar decentralized structure with an additional feature, i.e. a tendency toward flexibility, indicated by the presence of 4-cycles in the network. These characteristics accentuate the self-sufficient and resilient nature of the terrorism financing network, which will be not only more difficult to disrupt because of the multiple overlapping linkages, but also because there are few people whose elimination would compromise the flow of information and exchanges within the network. In fact, if one actor was to be eliminated at random, it is likely that she would be easily replaced by another actor in a similar position.

To conclude, in spite of the differences previously discussed with respect to far-right and Islamic extremist *modus operandi*, our structural analysis highlighted significant similarities in the way their co-offending, family, and business networks were structured. This intriguing finding could be interpreted as evidence that financial schemes by political extremists occur within similar operational settings, characterized by decentralized, self-organizing structures that facilitated exchanges between individuals acting within close-knit groups regardless of their ideological affiliation. The fact that the same trend was found within networks formed through different relational tie types as well as within smaller cohesive clusters extracted from the overall network rules out the hypothesis that this is a byproduct of our ego-centered research design. Theoretical and policy implications of these results are discussed below.

7.1.4 The crime-extremism nexus as a function of social selection

Criminologists agree that one of the possible ways in which the crime-terror nexus manifests itself is in the form of collaborations between political extremists and profit-driven offenders. Some define them as "business relationships", usually involving short-term transactions (Shelley & Picarelli, 2005). Others refer to "alliances", which occur when either criminal or terrorist groups need to fill an operational or expertise gap (Makarenko, 2004). In general, it is argued that these joint ventures are opportunistic and temporary, and only in very rare instances they turn into something deeper, in which case there is usually a transformation of the group from profit-oriented to political, or vice versa (Hutchinson & O'Malley, 2007; Williams, 2008).

This body of research, which indeed advances interesting theoretical conceptualizations, utilizes a simple methodology to illustrate the various types of convergence or divergence, usually involving the analysis and comparison of selected case studies; hence, unfortunately it lacks the scientific rigor needed to develop plausible theoretical explanations. More importantly, these studies implicitly define the crime-terror nexus as a group-level phenomenon, neglecting the existence of lower-level interactions occurring outside static and predetermined organizational settings. In other words, the crime-terror nexus is described in a simplistic way based on a very limited number of instances whereby collaborations between terrorist and criminal organizations have occurred as reported in the media (e.g. alleged incidents involving drug smuggling ventures between Russian criminal groups and Colombian guerrillas; Makarenko, 2004). These studies' limitations are due, in part, to the absence of valid and reliable large-scale data. Additionally, until recently, there were no adequate statistical methods to model complex network structures using attribute and structural predictors to test hypotheses on tie formation.

This dissertation provides the first attempt to explore these issues more in depth by examining the nexus between political extremism and profit-driven crime in the U.S. financial crime sector using Exponential Random Graph Modeling (ERGM), a superior statistical method which allows for capturing "both the regularities in the processes giving rise to network ties while at the same time recognizing that there is variability that we are unlikely to be able to model in detail" (Robins et al. 2007a, p. 174). As our exploratory network analysis revealed, financial extremist networks included a substantial number of non-extremist individuals, providing preliminary support to the crime-extremism nexus hypothesis. The ERGM analysis further strengthened this point demonstrating that links between political extremists and non-extremists were affected by different social selection

processes. As noted, homophily refers to social selection based on a similarity of traits (e.g. race, gender, education, etc.; see Cook et al., 2001; Goodreau et al. 2009; Wimmer & Lewis, 2010; Young, 2010). Heterophily describes the opposite phenomenon, whereby two persons become associated on the basis of their individual differences (e.g., different political opinions, different social background, etc.; see Burt, 2001 & 2005; Everett, 1962; Lin, 2005). Translating these concepts to our study, we considered the presence of significant and positive homophily effects as an indication that tie formation was not affected by meaningful interactions between extremists and non-extremists, whereas significant and positive heterophily effects were interpreted as evidence that connections between extremists and non-extremists were meaningful, hence supporting the crime-extremism hypothesis.

Our statistical analysis confirmed that significant homophily and heterophily effects existed within financial extremist networks formed through different relational tie types. In particular, homophily significantly affected tie formation within co-offending networks involving both far-right and Islamic extremists, suggesting that political extremists tend to engage in illegal activities more frequently with other political extremists than non-extremists. However, as noted, this finding should be taken with caution, because it could also be interpreted as the tendency for prosecutors to target ideologically motivated individuals collectively. In other words, this trend may be a byproduct of prosecutorial strategies and their "explicit politicality" rather than an expression of criminal preferences (Smith et al., 2002).

Contrary to what hypothesized, homophily was not a significant predictor of tie formation within familial settings. Co-participation in financial schemes by family members was, in fact, better explained as a function of triadic closure, which stresses the close-knit nature of familial relationships as an important organizing factor regardless of ideological

affiliation. Finally, as hypothesized, business ties were significantly affected by interactions between far-rightists and non-extremists. This suggests that far-rightists did not discriminate between ideologically motivated and profit-driven individuals when looking for fruitful partnerships. Hence, far-right business settings provide indeed ideal venues where crime-extremism connections can flourish. This was not the case for Islamic-related business networks, however, where political extremists appeared to be more careful deciding with whom they associated, and overall preferred not to take risks exposing their belief systems to non-believers.

This pattern emerged also when we compared the far-right anti-tax component with the Islamic terrorism financing one. Heterophily was a significant predictor of tie formation among individuals involved in a tax avoidance scheme, whereas homophily predicted connections among individuals engaging in financing activities to support Hamas and Hezbollah. This suggests that links between extremists and non-extremists were more likely to form if these were involved in a tax avoidance scheme, whereas such interactions were unlikely to happen among individuals involved in terrorism financing activities, or at the least they were sporadic and did not significantly contribute to tie formation.

To further investigate the role of non-extremist associates within financial extremist networks, we conducted an actor-centered analysis, which allowed us to pinpoint key figures in the tax avoidance and terrorism financing networks. Previous research shows that "brokers" play a significant role in covert networks by facilitating information flows and controlling information asymmetries (Bruinsma & Bernasco, 2004; Burt, 2005; Natarajan, 2006; Zhang & Chin, 2002). These "cut-points" are identifiable because they connect otherwise disconnected subsets, and it is argued that their elimination may prove to be an effective way to dismantle the overall network by cutting this "bridge" (Malm, 2006; McGloin, 2004). Studies on criminal networks have found that individuals with

specialized knowledge, skills, or contacts (e.g., financial advisors, money launderers, accountants, lawyers, etc.) oftentimes have brokerage positions (Morselli & Roy, 2008; Williams, 2001). Based on this literature, we expected non-extremist associates to be brokers for other financial scheme participants. Our data, however, did not support this contention.

Compared to political extremists, only a small number of non-extremists were central actors in both the anti-tax and terrorism financing networks. In fact, we did identify individuals with important brokerage roles, however for the most part these were political extremists. One possible explanation for this trend is that political extremists in the two identified networks were already equipped with brokering skills, e.g. they could have been business promoters, financial advisors, lawyers, etc. As we pointed out in our initial descriptive analysis, a majority of far-right extremists were employed in typical white-collar jobs. On the contrary, Islamic extremists in our data set came from various socio-economic backgrounds, and were employed in both low-collar and white-collar jobs. In fact, as suggested by referencing to the open-source documents, the most central actors within the terrorism financing network were the director of an Islamic charitable organization and a senior political figure affiliated with Hamas. It is interesting to notice that, however, according to our descriptive analysis non-extremists included various types of professionals and facilitators, e.g. business promoters, accountants, lawyers, bank employees, etc. To better understand the various roles played by these actors compared to their centrality scores, additional research should be conducted further inspecting the open-source materials.

There is also an alternative methodological explanation, which has to do with the usefulness of centrality measures as regards these specific criminal settings. Although highly used in covert network studies, comparing actor centralities within financial

extremist networks may not be the best way to approach these structures and understand their functioning and flaws. Given the decentralized and clustering patterns discussed above, perhaps individual-level analysis aimed at detecting central actors may not fully capture the complexity inherent in these criminal associations. In other words, arresting either the leader or the broker may not prevent the network of financial scheme participants from continuing to function. We will elaborate on this point in the following sections.

7.2 Conclusions

7.2.1 Theoretical implications

These findings bear significant implications for criminological theories. This dissertation provides the first attempt to develop an empirically based, theoretical framework to understand the convergence of political extremism and profit-driven crime in the financial crime sector by combining opportunity theories with the social network perspective. To review, opportunity theories include a variety of theoretical approaches that share a common underlying theme: crime results from an interaction between a motivated offender and a set of situational opportunities (Clarke & Felson, 1993; Cornish & Clarke, 1986; Cohen & Felson, 1979; Ekblom & Tilley, 2000; Ekblom, 2007). Three main approaches were discussed in this study, i.e. rational choice, routine activity, and conjunction of criminal opportunities (CCO).

The rational choice perspective emphasizes the offender's decision-making process leading to a specific crime event, recognizing the "influence of the environment on

behavior" with respect to everyday life situations (e.g., lifestyle, motives, and needs) as well as "the more particular environment of instrumental action to achieve particular goals" (Cornish & Clarke, 2008, p. 24). In this sense, crime is regarded as rational and purposeful behavior, dependent upon situational contingencies and resulting from a more or less accurate estimation of benefits and costs.

Rational choice theory provides a useful framework for considering the crimes here studied. Differences in the type of financial schemes carried out by American far-rightists compared to Islamic extremists reflect their different objectives and needs, i.e. anti-tax protest for the former, and terrorism financing for the latter. From a micro-level perspective, variations as regards the goals pursued by different suspects highlight the complex nature of criminal motivation, which involves an approximate calculation of benefits and rewards obtained through criminal behavior. The diversity of motives, however, does not change the nature of the crimes, which require specific opportunity structures and decision-making processes. As noted, financial offenders who cheat on their taxes or collect funds to support terrorist organizations may do so for a variety of reasons; however, they all agree on how to achieve their goals, i.e. by making choices based on limited available information and following a specific course of action.

Another indication of the rationality inherent in the crime commission process leading to a financial scheme is reflected in the various techniques used, which varied depending on the type of scheme pursued but also as a result of different efficiency and security concerns (Baker & Faulkner, 1993; Morselli, 2009). Our descriptive analysis showed that some methods were preferred over others, suggesting that not all techniques were equally able to provide maximum results with minimum efforts. For example, the use of nominee entities and shell corporations, which was common in both far-right and Islamic schemes, indicates a carefully planned strategy which aimed at effectively hiding assets

while avoiding detection, and required some level of sophistication. The use of informal value transfer systems (e.g., cash transactions, cash smuggling, etc.) by Islamic extremists engaging in terrorism financing reveal, on the contrary, that some preferred to choose less sophisticated but safer ways to move their funds. Hence, offenders who used these methods were aware of the risks of conducting transactions through formal mechanisms. Following the rational choice approach, we can therefore argue that specificity characterizes financial schemes by political extremists, given that specific schemes require specific methods. This point has important policy implications for prevention purposes, which will be discussed next.

The routine activity approach was originally formulated as a macro-level theory to explain variations in crime and victimization rates as a result of major societal changes (Cohen & Felson, 1979). Its core tenets support the notion that crime is the result of three major co-occurrences, i.e. a likely offender, a suitable target, and the absence of a capable guardian (Felson, 1998 & 2002). Subsequent theoretical advances developed micro-level explanations of offending and victimization, which were applied to a wide range of crime types. Felson (2002) proposed a routine activity theory of white-collar crime describing it as "crime of specialized access" […] "committed by abusing one's job or profession to gain specific access to a crime target" (p. 95). In fact, he criticized the term "white-collar crime" for being too vague and unable to accurately describe the variety of criminal behaviors and offender types falling under this overarching category. In particular, he pointed that "white-collar" criminals do not necessarily have white-collar jobs, and may come from all social strata, racial, ethnic, and religious background. Additionally, different individuals may pursue different goals, such as greed, power, and prestige. Certainly, our descriptive findings support these arguments. Political extremists were not only driven by ideological purposes, but were sometimes driven by monetary concerns; on the other hand, non-

extremists exhibited mixed motives, too. Their socio-economic background was also heterogeneous, and the fact that a large number was employed in white-collar jobs lends support to the specialized access hypothesis.

According to Felson (2002), specialized access to financial crime opportunities is obtained in three ways, i.e.: (1) through "overlapping activity spaces", e.g. taking advantage of the absence of one's boss (i.e. the capable guardian) to commit the crime; (2) through access to information, which offenders may already possess as a result of their profession, work role, or organizational position; and, more importantly for this research, (3) through personal ties, which provide both information about existing crime opportunities as well as co-offending partners. The conjunction of criminal opportunities (CCO) theory further complements this approach by emphasizing the importance of internal and external resources available to the offender, which include moral and cognitive skills as well as material and collaborative facilitators (Ekblom, 2007; Ekblom & Tilley, 2000; Gill, 2005).

In line with these viewpoints, this study found positive evidence that collaborations, both criminal and legitimate, were instrumental for the commission of financial crimes by political extremists in the United States. First, consistently with the extant literature on co-offending patterns, we noticed that most schemes were committed by two or more individuals (Reiss, 1986; Reiss & Farrington, 1991; Warr, 2002). This became even clearer once we included the suspects' informal network of contacts, suggesting that studies on co-offending should not merely focus on collaborative efforts at the time of the criminal act but also include all those who "the offender must rely on before, during and after the crime event in order to make the contemplated crime possible or worthwhile" (Tremblay, 1993, p. 20).

Second, financial offenders found important resources for crime among their business partners and family members, consistently with Felson's argument (2003) that

opportunities for co-offending emerge in "offender convergence settings", where potential co-offenders find one another in the context of their routine activities. Secrecy and security concerns motivate offenders to find accomplices in their circle of trusted relationships, which may include family, friends, and reliable business associates (Erickson, 1981; Krebs, 2002; Morselli & Giguere, 2006; Morselli et al., 2007). However, criminals must also be proactive and increase efficiency while maintaining security by forming new ties with resourceful individuals (Baker & Faulkner, 1993; Morselli, 2009). As Tremblay (1993) clearly pointed out, "the search for suitable co-offenders involves the attempt to combine two goals: the search for the strongest ties possible with co-offenders as to minimize the chances of betrayal and failure; and the search for weak but useful ties so as to increase the scope and value of crime opportunities" (pp. 26-27). As a result, co-offenders must develop two different kinds of networks: "whereas the concern for safety and trust involves the building of a network of strong ties (a community), the concern for wealth involves building a network of useful but less intimate ties (a market)" (p. 28).

These considerations offer a valuable explanation for our findings, particularly as regards the results of our ERGM analysis, which revealed that financial extremist networks in our data set formed loose and leaderless self-organizing structures independent of the suspects' ideological affiliation. This finding lends support to a growing body of criminological literature, which maintains that criminal association occurs within fluid and flexible networks rather than highly centralized, vertical structures, which are popular in media portrayals of organized crime. Confirming this tendency, Tremblay (1993) anticipated that "criminal markets should be populated by small, ephemeral, and local markets and firms", which further "implies that job opportunities for motivated offenders will be intrinsically ephemeral, local, volatile, and unpredictable" (p. 28).

Indeed, our exploratory and statistical network analyses identified a variety of subsets exhibiting low levels of social cohesion where meaningful exchanges occurred within small cliques, which by definition provide a safe environment where all members know and trust each other. Weerman (2003) describes this trend referring to the "instrumental perspective", which borrows from rational choice principles and opportunity-centred decision-making processes (Cornish & Clarke, 1986; Clarke & Felson, 1993). Accordingly, many times "co-offending leads to an easier, more profitable or less risky execution of a crime", and it "is chosen when it is expected to be easier and more rewarding than solo-offending" (p. 403). Criminological studies focusing on criminal careers similarly found that co-offenders usually engage in dyadic or triadic relationships, and more rarely seek more than three partners (Reiss & Farrington, 1991; Walsh, 1986; Waring, 2002). The reason provided by opportunity theorists is that "larger groups do not contribute very much to the execution of offences, while they increase the risks of betrayal and decrease the share in the catch" (Weerman, 2003, p. 403).

Moreover, this dissertation explored the crime-extremism nexus by modelling individual-level interactions between extremists and non-extremists based on the assumption that social selection processes influenced financial extremist networks, and found indeed evidence that these collaborations significantly impacted the network structures in which they were embedded. Social selection was mentioned by Gottfredson and Hirschi in their general theory of crime (1990), which argued that offenders select their peers based on similar personality traits, in particular low self-control. More specifically, this theory maintains that "self-control is a major factor in determining membership in adolescent peer groups" (p. 157). Criminologists that adhere to this perspective, therefore, believe that homophily affects co-offending patterns, because "birds of a feather stick together" (Glueck & Glueck, 1950; Hirschi, 1969).

Using a similar theoretical paradigm, we operationalized the crime-extremism nexus as a process of social selection based on heterophilous suspect status (i.e., extremists choosing non-extremists, and *vice versa*), and hypothesized that this would be prevalent within business networks and a far-right anti-tax subset extracted from the overall network. In addition, we hypothesized the existence of homophilous selection effects within co-offending and family networks as well as within the Islamic terrorism financing subset. As discussed, the results of this analysis were mixed, and provided partial support to our hypotheses. It is important to notice, however, that, despite the analogy with Gottfredson and Hirschi's self-control theory, these findings should not be interpreted as an attempt to test its social selection assumptions. In fact, we did not measure personality traits but rather used a dichotomous variable ("suspect status"), recoded from our strength of association variable used to distinguish extremists from non-extremists, as a predictor of tie formation.

Because this dissertation is concerned with financial crime, which is typically considered white-collar crime (although we have already noticed the limitations inherent in this definition), it is worth notice that Gottfredson and Hirschi (1990) explicitly referred to this crime type to justify their general theory. Briefly, the authors denied that white-collar criminals would be any different from street criminals, as they both seek to achieve immediate satisfaction through risky behaviors. Additionally, they argued that white-collar crime is relatively uncommon and does not require a high-level of specialization. Based on these study findings, however, we cannot agree with these statements. First of all, financial crime cases in our data set, which provided a snapshot of a one-year time period only, were anything but uncommon. Second, we found evidence that different types of financial offenders exist, although a better taxonomy could be developed departing from the traditional simplistic dichotomy based on ideological motive. Third, the variety and

complexity of techniques used to carry out the schemes imply that different levels of sophistication are required. Finally, and importantly, this theoretical perspective does not account for social selection processes based on heterophily, and therefore does not provide plausible explanations for the crime-extremism nexus. Therefore, Gottfredson and Hirschi's general theory may provide a useful framework to explain most crimes; however, its validity as regards financial extremist crime is questionable, as other researchers have already pointed out (Benson & Moore, 1992; Reed & Yeager, 1996).

Opportunity theories and the instrumental perspective provide a valuable explanation of the crime-extremism nexus as a function of heterophily selection effects, which significantly influenced criminal and business networks involving American far-rightists and their non-extremist associates. To quote Tremblay again (1993, p. 17), the "search for suitable co-offenders" is a complex process that affects "a wide range of motivated potential offenders" [...] and can be interpreted as "the intelligible outcome of a pattern of individually reasoned choices and constraints that vary across settings, across crimes, and over a given offender's life cycle" (Tremblay, 1993, p.17). Because co-offending is instrumental to the criminal goal, potential co-offenders are willing to overcome their differences in order to maximize their advantages and increase profitability (Weerman, 2003). We can, therefore, infer that far-rightists considered less risky and overall more advantageous to partner up with a variety of co-offenders, regardless of whether or not they shared the same ideological belief system. Unfortunately, our statistical analysis allows us only to observe that meaningful selection patterns were present, but we do not know *why* these occurred, or in other words what were the qualities extremists sought in non-extremists, and *vice versa*. Based on our descriptive findings, we can hypothesize that non-extremists possibly provided useful resources, in the form of knowledge, skills, specialized access, etc., that political extremists were lacking (and *vice-versa*).

The reference to knowledge and resource sharing immediately brings to mind another set of criminological theories that could be used to explain homophily and heterophily effects as a function of social influence rather than social selection, i.e. differential association and social learning theories. Sutherland's original contention was that criminal behavior is learned from interaction with others (Sutherland & Cressey, 1960). Subsequent reformulations proposed various mechanisms to explain how crime is learned by referring to cognitive psychology and behavioral theory. Akers (1998), in particular, stressed the role of imitation processes and social structure. Kenney (2007) used the social learning framework to explain how drug trafficking networks acquire their *metis,* i.e. the practical skills to conduct criminal business, "by immersion through informal apprenticeships, practical demonstrations and trial and error" or simply by "watching" other drug traffickers (p. 55). Practical knowledge is complemented by *techne,* i.e. abstract technical information that is provided by experts and professionals (e.g. lawyers, accountants, money-launderers, etc.). These learning processes are crucial because they allow drug trafficking networks to constantly progress. Additionally, they do not exclusively pertain to criminal networks, but also influence law enforcers, military units, and prosecutors who modify their strategies in response to criminal advancements. These theories have clear relevance for the criminal behaviors here studied. However, we reserve this inquiry for future research efforts.

In conclusion, it is important to stress the need to better conceptualize the crime-extremism nexus using existing criminological theories and testing their validity through empirically sound research. Although categorizations and theoretical constructs exist, these are usually not based on a systematic analysis of quantitative data but rather an examination and comparison of selected case studies, which have led to "broad and sweeping generalizations" (Biersteker & Eckert, 2008, p. 301). This effort requires that, first

of all, more rigorous methods are developed to collect valid and reliable data. The recent creation of large-scale open-source databases, like the ECDB, GTD, and ATS, is a fundamental step forward in this direction. However, these initiatives should be expanded beyond the study of domestic and international terrorism to investigate other complex criminal phenomena, such as white-collar and organized crime. To our knowledge, no one has yet undertaken this imperative mission, notwithstanding the growing interest in this topic and numerous articles published in recent years. Criminologists must make an effort to move the field forward investing their time and resources in long-term data collection projects, rather than limiting their analysis to conducting case studies, which may provide interesting descriptions and useful starting points, but do not produce generalizable findings and are, therefore, of limited scientific utility.

7.2.2 Policy implications

Besides important theoretical implications, these study findings have significant policy implications for criminal justice and crime prevention strategies. As noted, financial crimes have the potential to cause incredible harm to a wide range of targets, including private citizens, communities, businesses, public institutions, and governments at large. Despite this, until recently, the public and academic interest in these crime types has been notably low compared to other crime problems, such as gangs and violent crime. Except for high-profile scandals, like those involving large corporations (e.g., Enron, WorldCom, Adelphia, etc.) and more recently the Bernie Madoff Ponzi scheme, criminal trials involving financial offenses have been seldom publicized (Friedrichs, 2004). In fact, the FBI puts

white-collar crime at number seven in its top ten priorities list, while terrorism is first (FBI, 2011).

From a criminal justice viewpoint, our descriptive findings highlight two opposite trends in the way criminal cases involving political extremists have been handled at the federal level. On one hand, financial schemes concerning Islamic extremists have been aggressively pursued by federal prosecutors, as suggested by the large number of suspects accused of providing "material support" to terrorists and terrorist organizations in 2004. This was part of a post-9/11 strategy promoted by the U.S. Department of Justice to use "every tool and every tactic in the arsenal of the justice community […], from aggressive enforcement of the criminal code to the deployment of the new and critical tools of the USA Patriot Act, […] to deter, disrupt and destroy terrorist threats" (Ashcroft, 2004).

These alleged terrorism financing cases, however, have sometimes ended with mistrials, acquittals for lack of evidence, or convictions for unrelated charges (e.g., mortgage fraud, immigration violations, etc.), raising concerns that prosecutorial strategies may have become too politicized and that targeted sanctions may "not be as targeted as they might initially appear" (Biersteker & Eckert, 2008, p. 295; see also Biersteker & Eckert, 2006). Some experts have also questioned whether this domestic side of the "war on terrorism" has had any real impact on the prevention of terrorism or the disruption of terrorism financing methods (McCulloch & Pickering, 2005; Passas, 2007; Warde, 2007). Others point to human rights and due process concerns, especially in cases where guilt was inferred "by association", putting several civil rights groups and humanitarian organizations at risk of being prosecuted for supporting terrorist activities (Gunning, 2008; Hardister, 2003).

The opposite trend can be noticed as regards prosecutions of the domestic far right. Compared to the efforts and deployment of resources put in the fight against Islamic-related terrorism financing, it is clear that the problem of financial schemes perpetrated by

American far-rightists has not been a top priority for public authorities. In fact, tax protesters are often treated as common tax cheaters, and their claims are frequently dismissed as "frivolous arguments". Therefore, contrary to what happens with Islamic suspects accused of financing terrorism, the important ideological component of far-right financial offenders is downplayed, and the large-scale impact of this anti-government movement goes almost unnoticed. This dissertation provides evidence that the illegal behaviors of far-right tax protesters, who promote, sell, and purchase anti-tax strategies to sabotage the US government, and organize large-scale pyramid and Ponzi schemes possibly victimizing thousands of people, constitute an actual threat and have the potential to become even a bigger problem if left untreated. Our small sample only included a few cases, but many more are currently being coded in the ECDB, showing that these criminal behaviors are widespread and have been going on for decades without receiving the attention they deserve.

These preliminary findings indicate that criminal justice strategies should be fine-tuned and priorities reassessed based on a more systematic determination of actual and perceived threats. The post-9/11 "war on terrorism" may have overshadowed the significance of dangerous behaviors by domestic extremists engaging in non-violent but equally dangerous criminal activities. Certainly, we do not want to downplay the importance of preventing international terrorism by early detection and prosecution of facilitators based in the United States; however, as recent studies show, the threat of domestic terrorism, both violent and non-violent, should not be underestimated (Belli & Freilich, 2009; Freilich et al., 2009b; Freilich & Chermak, 2009; LaFree & Dugan, 2007; McNab, 2006 & 2010; Pitcavage, 2001; Sanchez, 2009).

One of the primary goals of this research was to produce useful knowledge for policy-makers and justice officials involved in the fight against the growing crime-

extremism nexus. In this regard, probably the most valuable finding is that political extremism and profit-driven crime are indeed intrinsically related, and should therefore be addressed jointly rather than as separate phenomena. As experts have noted, it has become increasingly difficult to distinguish between ideologically motivated and profit-driven offenders, and in fact such a distinction may not be of much practical use (Bovenkerk & Chakra, 2008; Dishman, 2005; Shapiro, 2007). This dissertation clearly highlighted this point, and further revealed that financial schemes involve a variety of individuals who may be variously motivated. Therefore, criminal and terrorist investigations should be conducted collectively, because "a criminal lead could very well trace back to a terrorist" (Dishman, 2005, p. 249). In particular, emphasis should be put on creating task forces that include terrorism experts, criminal investigators and prosecutors with expertise on financial matters and forensic accounting (Breinholt, 2005). As this study shows, both American far-rightists and Islamic extremists engaged in financial schemes using a variety of legitimate and criminal methods that could be easily identified through "follow-the-money" approaches.

Our network analysis uncovered interesting and useful information on how political extremists engaging in financial crimes associate with one another and with non-extremist accomplices. First of all, the findings revealed that, consistently with previous research, financial offenders were linked by multiple types of relational ties (Malm et al., 2010; McGloin, 2004; Sarnecki, 2001). This has evident implications for criminal justice strategies, as it stresses the importance of gaining insight into the nature and type of links existing among criminals, especially as it relates to legitimate relationships, such as family or business ties. Social network analysis is considered a powerful investigative tool because it allows investigators to map out the web of links between co-offenders uncovering suspicious patterns, vulnerabilities, and key figures that could be targeted (i.e. arrested) in

an attempt to disrupt the overall network (Morselli, 2009; Van der Hulst, 2008; Xu et al., 2004). Investigators aiming at disrupting a financial extremist network should, therefore, expand their focus beyond the primary suspects, and include family members or business associates who do not seem to partake in criminal activities but may, in fact, be crucial facilitators. These individuals could be approached in various ways that do not necessarily require criminal justice interventions (McGloin, 2004). For example, these "weak" links could be persuaded to collaborate by offering "amnesty" options (e.g., to accountants that provided tax advice to far-rightists) and social services (e.g. for relatives of Islamic extremists engaged in fund-raising activities to support terrorism organizations).

In addition, investigators should keep in mind that targeting different types of networks may yield different results (Malm et al., 2010). For example, an effective disruption strategy against financial extremist crime should focus on tackling legitimate business networks, which appeared to be the least cohesive in our data set and therefore more vulnerable to external attacks, by removing key individuals who link the loosely connected parts of the network. On the other hand, co-offending networks that are made of individuals linked by family and business ties may be more difficult to dismantle because of the intensity of these overlapping relationships. In fact, preventive strategies that do not require criminal justice interventions may produce better results in this case, as discussed below.

Importantly, our ERGM analysis revealed interesting structural and attribute properties of financial extremist networks which bear implications for criminal justice strategies. In particular, we noticed significant differences across networks as regards interactions between extremists and non-extremists. From a descriptive perspective, both far-right and Islamic extremists appeared to be linked to non-extremist suspects. After modeling these interactions, however, the crime-extremism nexus appeared to be a unique

characteristic of far-right settings, where extremists and non-extremists "mingled" easily. On the contrary, Islamic extremists formed significant bonds only with other extremists, while their connections to non-extremists occurred on a sporadic basis.

From a practical standpoint, these findings can be interpreted as evidence that far-right financial networks are more flexible and volatile compared to Islamic extremist networks. As discussed in the previous section, co-offending appears to be "instrumental" for the commission of a far-right financial scheme, which means that an extremist anti-government and anti-tax ideology is not an essential requirement for the selection of suitable co-offenders (Tremblay, 1993). An effective strategy to disrupt this network type should target key actors in brokering positions that isolate the different network subsets. Because these individuals bring in the opportunity to co-offend, it will be difficult to replace them and the costs of continuing the criminal venture may therefore outweigh the benefits. If instead co-offending patterns occur between individuals who share a stronger bond (i.e. commitment to a political or religious cause), it may be more complicated to cut these connections. Disruption strategies would be more successful if leadership figures were targeted (both in relational as well as attribute terms).

Despite these differences, financial scheme participants operated within similar self-organizing structures, suggesting that perhaps better strategies could be developed by focusing on structural characteristics rather than distinctions based on ideological affiliation. However, the fact that financial extremist networks tend to be decentralized, and are therefore "leaderless", complicate matters for criminal investigators and prosecutors, whose action strategies have traditionally consisted in arresting and convicting the leaders. Since the first large-scale prosecutions of organized crime cases, American prosecutors have focused on taking down the group leaders, based on the belief that criminal collectives were indeed organized and vertically structured. Current research has departed from the

theoretical model of the hierarchical "Mafia", and emphasizes that nowadays criminal (and terrorist) organizations have "fuzzy boundaries" and a flat structure (McGloin, 2004; Morselli, 2008; Natarajan, 2006; Powell, 1990; Sparrow, 1991).

In particular, studies on covert networks highlight the role of secondary players, such as facilitators and brokers, who oftentimes fall below the radar of prosecutors that prefer to choose the "usual suspects" rather than actively pursuing these important mediators (Kenney, 2007; McGloin, 2005; Morselli & Giguere, 2006; Morselli & Roy, 2008). This point was noted in our analysis of the anti-tax far-right subset, which included three brokers that had not been targeted by law enforcement, suggesting that their central role as cut-points had been underestimated (McGloin, 2005; Williams, 2001). However, one of the biggest limitations of law-enforcement centered approaches is that they tend to have a too narrow focus, primarily driven by tactical goals. It is possible, therefore, that they miss the "bigger picture" provided by a more in-depth analysis of criminal networks' topological properties (Xu & Chen, 2008). In this sense, because financial extremist networks are decentralized (i.e. "leaderless") and exchanges of financial goods and services occur within cohesive cliques, conventional individual-level approaches may not provide effective disruption mechanisms.

Based on these arguments and in light of the ERGM analysis findings, which revealed complex self-organizing and self-sufficient structures that may be difficult to dismantle through traditional criminal justice approaches, we propose an alternative approach developing effective situational prevention strategies rather than reacting *ex post facto*. As Felson (2002) noted, we must beware of the "cops-and-courts" fallacy (p. 3), which has shifted the attention from crime before it happens to criminal justice-centered approaches which take care of crime when it is too late. In fact, there is evidence that in some cases prosecutorial strategies may have even contributed to worsen the problem. For

example, some high-profile tax protesters were transformed into "martyr" figures after they were convicted, becoming a symbol of far-right propaganda (Belli & Freilich, 2009).

Situational crime prevention (SCP) is a powerful, pragmatic approach that focuses on the event rather than the agent, arguing that criminal incidents can be prevented or at least reduced by intervening on situational circumstances that facilitate crime instead of trying to change a person's mindset (Clarke, 1997). Accordingly, individual-level motives are irrelevant, and terrorism is simply "crime with a political motive" (Clarke & Newman, 2006). Because the focus is on situational opportunities, different strategies are needed for different crime types. Our descriptive analysis revealed very specific crime problems (i.e., the different financial scheme types) that could be targeted with selected prevention tactics. Additionally, our examination of the different techniques used provides a useful starting point to identify the opportunity structure behind various scheme types.

Previous research has already addressed the problem of ideologically motivated tax refusal by far-rightists, recommending a "soft" approach – as opposed to traditional "hard" situational crime prevention (e.g., target-hardening, etc.) – including strategies to avoid disputes, neutralize peer pressure, and assist compliance (Belli & Freilich, 2009). Since money-dirtying and money-laundering schemes appeared to be the most common types for Islamic extremists, future studies should begin with an assessment of their opportunity structure to identify the "hottest" techniques and devise targeted prevention measures.

Experts argue that post-9/11 anti-terrorism financing initiatives failed because they applied old paradigms from the "war on drugs" to the new "war on terror", focusing on money laundering, which involves hiding and "cleaning" the proceeds of crime in the financial system, instead of money dirtying (Warde, 2007; Williams, 2008). Terrorism financing, in fact, often involves "soiling" clean money which is then used for illegal purposes (hence *money dirtying*). Although there are similarities between these two

financial crimes, there are also important differences in terms of goals, methods, and level of sophistication required: "in money-laundering, capital from illegal channels is repatriated in order to be used 'freely', whereas in money dirtying, the aim is to commit a crime and therefore all traces must be destroyed" (Compin, 2008, p. 599).

Importantly, our analysis highlighted the weaknesses of the legitimate financial sector. Despite international and domestic efforts to adopt *ad-hoc* legislations and enforce strict regulatory procedures (such as the "Suspicious Activity Report" and "Know-your-customer" rules for financial institutions), the banking system appears to be vulnerable to malicious uses. Situational prevention strategies should incorporate these issues and improve effective monitoring and protection mechanisms that directly involve financial institutions and their employees. Although SCP is primarily concerned with the criminal event rather than the criminal agent, a study by Cornish and Clarke (2003) introduced an intriguing taxonomy focusing on the nature of the offender, which could be helpful for devising effective strategies against financial extremist crimes. Incorporating recent advances on the role of situational precipitators (Wortley, 1998, 2001 & 2002), Cornish and Clarke described three types of criminals, i.e.: (a) the predatory offender; (b) the mundane offender; and (c) the provoked offender.

The first type corresponds to the traditional portrayal of the rational, decision-making offender as "an individual bereft of moral scruples", […] "assumed to arrive at the crime setting already motivated and somewhat experienced in committing the crime in question" (Cornish & Clarke, 2008, p. 39). The second type is the "occasional" or "opportunistic" offender, who appears to be "relatively uncommitted" to crime, has a stake in conformity, and uses moral justifications (similar to "neutralization techniques" conceptualized by Sykes and Matza, 1957) to "make excuses" for her conduct (p. 63). The third one, which is less relevant for these study purposes, is referred to as the "precipitated"

or "situational" offender, and is described as an individual who is suddenly prompted to crime by specific situational stimuli.

This distinction is not only significant for theoretical purposes, but it is especially important for its policy implications. Cornish & Clarke (1993) argued that situational prevention strategies should take into account crime type as well as suspect specificities, because the efficacy of such interventions will not be the same across suspect types. In particular, "given the nature of their motivation, and their lack of concern for the effect of their behavior on others, the only situational techniques with much chance of preventing the criminal behavior of predatory offenders will be those that attempt to disrupt instrumental aspects of the crime-commission process: that is, those that increase perceived effort, increase perceived risk, and reduce anticipated rewards" (p. 61). Mundane offenders, on the contrary, may not respond well to "tough" strategies aimed at incapacitating their action, but would probably be more sensitive to situational techniques that remove excuses, reduce permissibility, induce guilt, and facilitate compliance. Although this is only a preliminary discussion, there is evidence that these concepts could be applied to prevent financial crimes by political extremists and non-extremists.

Our descriptive analysis revealed that not all political extremists were equally committed to an ideological cause. In fact, when measuring their strength of ideological association, their scores varied from 1 to 4. According to Cornish and Clarke's taxonomy, we can therefore infer that our dataset included both "predatory" and "mundane" political extremists. The ring-leader of a cigarette smuggling organization collecting money for Hezbollah or the spokesperson of a tax-protesters' organization selling anti-tax packages could be considered examples of the first type. A *hawaladar* that provides money-remittance services without inquiring about the sender's or receiver's identity or the

occasional tax cheater that buys into far-right propaganda could represent examples of the second type.

Although these issues were not considered with respect to non-extremist suspects, we can theorize that they also possibly displayed different levels of commitment to their criminal goals. With reference to white-collar criminals, for example, we could hypothesize that professional fraudsters be "predatory" whereas employees who cheat on their expense reports be "mundane". We could subsequently employ Cornish's (1994) script approach to reveal the crime opportunity structure necessary to commit money-dirtying and money-laundering and develop a two-pronged prevention strategy, i.e. one that involved traditional "hard" SCP tactics for predatory offenders, and another one using "soft" SCP measures targeting mundane offenders.

In conclusion, we argue that counterstrategies may benefit from a new classification of financial offenders based on the intensity of ideological or criminal motive rather than a distinction based on specific ideological belief systems. At the very least, this taxonomy would be more useful for developing targeted situational prevention measures than the traditional dichotomy between ideologically motivated and profit-driven offenders.

7.2.3 Methodological implications

From a methodological perspective, this dissertation makes an important contribution to the criminology field across multiple domains, ranging from the study of white-collar and organized crime to political extremism and terrorism. As mentioned, this is the first empirical study that systematically examines financial crime cases involving political extremists (i.e., American far-rightists and Islamic extremists) and non-extremist

offenders by quantitatively analyzing attribute and relational data obtained from a variety of open sources. By focusing on financial crimes, it expands our knowledge of criminal behaviors that have traditionally been associated with white-collar and organized crime. By comparing similarities and differences between American far-rightists and Islamic extremists, it adds to the terrorism literature, which has neglected the significant role of non-violent, ideological crimes. Finally, by exploring and modeling the relational patterns between political extremists and non-extremists, it provides a fundamental contribution to the literature on the crime-extremism nexus, which remains largely unempirical.

As discussed, in the criminology literature there is no universally accepted definition of financial crime. Since Sutherland's seminal piece on white-collar crime (1939), several studies have been conducted in an attempt to shed light on topics such as: offense types (Albanese, 2005; Block & Griffin, 2002; Doig, 2006; Levi, 1994), offender types (Gill et al., 1994; Hobbs, 1994; Friedrichs, 2004; Levi, 2003; Weisburd et al., 1991), motivational differences (Croall, 2001; Dean & Melrose, 1995; Naylor, 2000; Rowlingson et al., 1997), and magnitude of the problem (Biagioli, 2008; Nelken, 2002; Ruggiero, 2003). Although these studies provide substantial knowledge concerning a variety of important aspects, the absence of uniform definitions, variations in unit of analysis, and lack of valid and reliable data provide a fragmented picture with limited scientific utility.

The complexity of financial crimes, which may span over an extended period of time, involve several jurisdictions, and victimize hundreds of people (think of the Madoff scandal and his decades-long Ponzi scheme as an example), makes them a difficult topic to study. Choosing the unit of analysis to collect quantitative data is especially problematic, and certainly more complicated than studying, for example, violent incidents (e.g. homicide, terrorist attacks, etc.), which usually have specific geospatial and temporal characteristics. Relying on legal definitions may not be the best choice either, considering that laws vary

across jurisdictions and over time, and legal provisions do not accurately represent the variety of behaviors carried out by the suspects.

To overcome these problems and capture the nuances inherent in financial crime cases, we developed a pioneering methodology that borrows from opportunity theories and the "script approach". As discussed, opportunity theorists argue that crime is goal-oriented behavior resulting from an interaction between a rational, decision-making offender and a set of available opportunities (Clarke & Felson, 1993; Cohen & Felson, 1979; Cornish & Clarke, 1986). The "script approach", developed by Cornish (1994), simplifies crime analysis by breaking down the crime-commission process in a sequence of steps to identify opportunity structures and intervention points for the development of situational prevention measures. By combining these theoretical and analytic frameworks, we developed three key concepts: (a) *financial scheme*, i.e. the overall illicit financial operation involving a set of perpetrators aiming at an unlawful economic advantage through the use of deliberate deception; (b) *criminal offenses*, i.e. the specific offenses suspects were charged and convicted with (legal component); and (c) *techniques*, i.e. the specific activities or methods used in the crime-commission process (behavioral component).

This important distinction provided the conceptual basis on which the "Extremist Crime Database (ECDB) – Financial Crimes" was built. Our descriptive analysis of financial schemes, crimes, and techniques allowed us to examine and compare far-rightists and Islamic extremists' *modus operandi* as well as legal strategies used to prosecute these cases. Even though our sample was small, we were able to draw interesting comparisons which could drive future research efforts. Additionally, researchers interested in the study of conventional white-collar crime now have a model that they can borrow to develop their own database and test a variety of research questions concerning financial schemes from a legal and behavioral perspective.

In addition to examining scheme-level variables, we also compared suspect characteristics focusing on available socio-economic, behavioral and legal attributes. Although merely descriptive, this analysis revealed the existence of a diverse group of offenders who were variously motivated and received different criminal justice treatments. Importantly, the findings highlighted variations in their degree of ideological involvement, which was measured using a 4-point scale variable, suggesting the existence of different types of political extremists. This shows, first of all, that the traditional dichotomy between ideologically motivated political extremists and profit-driven criminals is overly simplistic and misleading. Additionally, it calls for researchers to develop better categorizations that take into account variations in the strength of ideological association by operationalizing suspect extremist status as a continuous rather than a dichotomous variable, distinguishing for example between "highly motivated" and "lowly motivated" extremists. Hopefully, these findings will inspire future terrorism researchers to reconsider their operational definitions and come up with more accurate ways to classify political extremists.

The most important contribution of this study, however, lies in developing an inventive methodology to collect and analyze network data on multiplex relationships from open sources. The difficulty in obtaining official data and the limitations inherent in self-reported studies have prompted terrorism researchers to explore new data collection methods by using publicly available open sources. As Chermak et al. (2011) point out, recently developed open-source databases, such as the ECDB, GTD, and ATS, improve data collection methods by adopting rigorous protocols that allow for identifying relevant cases using predefined inclusion criteria, searching a variety of open-source materials, and developing more accurate and comprehensive incident- and suspect-based datasets for statistical analysis. Additionally, by relying on multiple source types to generate their study universe, these databases are more likely to prevent the problem of source selectivity bias,

and therefore increase their chances to get close to capturing the entire universe of existing cases.

In particular, the ECDB is unique compared to other terrorism databases because it includes structural variables capturing three types of ties between coded suspects (*egos*) and accomplices (*alters*). This dissertation drew relational data from the ECDB and employed an ego-centered design to construct the overall network of criminal and legitimate contacts that participated in a financial scheme using court documents, government reports, newspaper articles, watchdog publications, etc. As noted, this approach has several advantages. First of all, by including all individuals connected to the primary suspects and collecting information on multiplex ties we were able to move beyond criminal justice representations to truly reveal the structure of financial extremist networks. Additionally, by using multiple source types and including multiplex relationships we reduced the problem of boundary specification and missing data, which affects research on hard-to-reach populations such as criminals and terrorists.

This dissertation is an important addition to the growing body of research that employs social network analysis to study covert networks. As noted, social network analysis has tremendous potential for criminologists, and in fact more and more scholars are experimenting with it. Like crime mapping and GIS methods, it provides a powerful visualization tool that allows for exploring relational patterns by simply inspecting graphs. Additionally, it provides a variety of measures to describe social dynamics as a function of relational distances. These study findings are in line with previous research suggesting that covert networks are seldom organized, and form instead loose and flexible subsets following self-organizing principles determined by specific needs and objectives. Furthermore, they highlighted the existence of meaningful individual-level interactions between far-rightists, Islamic extremists, and non-extremist accomplices.

This point has particular relevance for the crime-terror nexus literature, which so far has primarily focused on group-level representations through analyses of case studies. Although experts argue that organized crime and terrorism can no longer be interpreted as hierarchical and static organizations, when researchers refer to existing or presumed social entities by their name (e.g. FARC, IRA, Hamas) comparing incidents when terrorists and criminals shared methods or conducted joint ventures, they implicitly assume the existence of an organization, which can be variously structured but is essentially defined by preexisting boundaries. This labeling process may be an artifact of popular media representations or determinations by public authorities, which tend to simplify structures to better "sell" them to their respective audiences, i.e. the public or the court. If researchers were truly interested in understanding the connections between criminals and terrorists, they should refrain from adopting preconceived notions and "seek rather than assume structure" (Morselli, 2009).

Finally, it is important to notice that the potential of social network analysis for criminological research today goes far beyond its descriptive power. Recent advances in statistical modeling allow researchers to conduct more sophisticated analyses testing hypotheses on criminal behavior taking into account its relational aspects. In fact, conventional statistical methods should no longer be used with network data because they violate basic statistical assumptions (Wasserman & Faust, 1994). Drawing conclusions from such analyses is dangerous "because the non-independence of network observations will usually result in under-estimates of true sampling variability – and hence, too much confidence in our results" (Hanneman & Riddle, 2005).

This dissertation showed how structural and attribute predictors can be modeled to test hypotheses concerning structural patterning and social selection processes within financial extremist networks. Although our analysis was perhaps simplistic because it

included one covariate only (i.e. suspect status), it provides a first attempt to explore differences across networks which are imputable to the presence of particular local configurations in combination with actor-level characteristics. For instance, we noted how homophily influenced business tie formation in Islamic extremist networks, whereas heterophily significantly impacted far-right networks. Additionally, we were also able to determine that social selection processes did not affect the structural configuration of family networks, which appeared to be close-knit and cohesive regardless of the individual members' ideological affiliation.

Statistical network modeling has a lot to offer to criminologists beyond the study of covert networks. The criminology literature abounds with theories that aim to explain crime as a function of social relationships. For instance, control theories initially theorized that delinquency would be inversely related to social bonds (Hirschi, 1969), and subsequently hypothesized that personality traits (i.e. self-control) would influence peer behavior so that "birds of a feather flock together" (Glueck & Glueck, 1950; Gottfredson & Hirschi, 1990). Although empirical research supports the correlation between self-control and friend selection, these studies constitute mere indirect tests, since none of them used actual social ties as the dependent variable. In fact, as Young (2010) noted, "the interpretation that correlated behavior is caused by selection ignores the role of additional processes which influence social networks. If processes that influence friendship formation are excluded from analysis, the explanation for correlated behavior may be incorrect".

In conclusion, criminological theories that assume a correlation between crime and social relationships should be put to test again to verify whether their findings are the result of their initial theoretical assumptions or whether there are other mechanisms at play that were not captured using attribute data alone. P* class models, including Exponential

Random Graph Modeling, provide a promising venue for criminologists to test old and new theoretical paradigms using sophisticated and sound statistical methods.

7.2.4 Limitations and next steps

As with any empirical research exploring uncharted territory, this dissertation has a number of methodological limitations that were anticipated and will be discussed more in depth in light of the research findings. In particular, these limitations concern three sets of issues: (a) the identification of the study population; (b) the problem of missing data within and beyond the final network representation; and (c) the analytic strategy, in particular as regards the goodness-of-fit estimation of the ERG models to the observed networks. This final discussion will also serve as an outline for our future research agenda, and hopefully provide useful insight to motivate other researchers to take up on where we left it.

Concerning our study population, perhaps the most obvious limitation relates to the small sample of cases examined. As noted, we decided to focus on a one-year period and provide a snapshot of all prosecutions initiated in 2004 concerning financial schemes involving at least one American far-rightist or Islamic extremist. To obtain our study universe we followed a multi-step procedure starting with the creation of a list of political extremists charged with a financial offense in 2004, which led us to identify a total of 54 related financial schemes and 164 suspects, including those who were indicted at a different time.

These numbers were deemed sufficient for the type of analysis we wanted to conduct. Given the absence of empirical research on this study area, this dissertation aimed at providing a descriptive analysis of financials schemes, crimes, and techniques, before

moving into a social network analysis of financial extremist networks using a convenient sample of connected suspects. However, because neither the schemes nor the suspects were sampled at random, we were unable to perform conventional inferential analyses and, therefore, draw meaningful generalizations. In short, the descriptive section of this dissertation cannot be generalized to the overall population of financial extremist schemes and suspects. As a consequence, it is possible that future research endeavors may reveal a partially different picture of the financial criminality of American far-rightists and Islamic extremists in the United States.

It is important to notice that data collection for the ECDB, which aims at creating the most comprehensive data set of financial extremist crimes since 1990, is currently ongoing. Therefore, in the future we intend to further shed light on differences and similarities between far-right and Islamic extremist financial crime by conducting multivariate analyses using random sampling procedures. Following up on these study findings, for example, it will be interesting to examine prosecutorial strategies and trial outcomes comparing a random sample of far-rightists, Islamic extremists, and profit-driven offenders prosecuted between 1990 and 2010. As noted, Islamic extremists overall received harsher punishments in comparison to far-rightists and non-extremists involved in financial schemes. A possible explanation may be related to an increased politicization of terrorism prosecutions, especially after 9/11. To examine this hypothesis, we will test the impact of anti-terrorism financing strategies introduced by the USA Patriot Act, such as the "material support" provisions (U.S.C. 18:2339), on prosecutorial strategies and trial outcomes. Despite criticisms related to this legislation's vagueness and broadness, federal prosecutors have used it extensively to prosecute individuals and organizations (e.g., Islamic charities) with alleged ties to terrorist groups (e.g., Hamas and Al-Qaeda) by inferring "guilt by association".

Second, the decision to use criminal investigations and judicial cases as the starting point to identify our study population is another important limitation. It is possible that, instead of capturing the behavior of political extremists engaging in financial crimes, we may have simply provided a picture of criminal justice initiatives on particular issues of concern. This limitation is well known to criminologists, who "rarely have access to ideal data in the 'real world'', and often have to rely on official data to conduct *ex post-facto* analyses (McGloin, 2004, p. 137). Additionally, by focusing on federal cases only, we may have missed financial schemes that were prosecuted at the state-level, especially as regards far-right suspects who may not always commit federal-level tax offenses. Finally, because of the political sensitivity of these topics and the unique historical circumstances, it is possible that our study universe did not accurately portray financial extremist crimes by Islamic extremists but rather a byproduct of the post-9/11 anti-terrorism strategy pursued by the US government through the criminal justice system. We must also notice that the current scenario may be different as a result of the time gap and changes in the political agenda.

To control for these problems and guarantee the validity and reliability of our data, especially vis-à-vis the subsequent network analysis, we took various steps, which we have already discussed and will briefly summarize here. First of all, the ECDB was created following a rigorous protocol that involved repeated open-source searching phases to ensure that: (1) all existing cases be identified; (2) any new case be promptly added to the database; (3) all publicly available information be collected and coded; and (4) targeted follow-up searches be conducted to fill out missing variables and correct data-entry errors. Second, in conclusion of our descriptive analysis, we compared open-source materials retrieved during data collection by source type between far-right and Islamic extremist schemes, and decided to drop those that appeared to be controversial because none of the participants scored higher than 2 in our strength of ideological association variable. As

mentioned, these cases should not be considered any less important. On the contrary, future research efforts should examine them more in depth to improve our understanding of this complex phenomenon and, in particular, the impact of certain prosecutorial strategies on terrorism research.

Regarding the collection of relational data to construct financial extremist networks, this dissertation suffers from the same problems every researcher interested in the study of covert networks must face, i.e. "fuzzy boundaries" and missing data (Malm et al., 2010; Morselli, 2009; Sparrow, 1991; Xu & Chen, 2008). Clearly, criminologists rarely have access to "whole networks" of criminals and terrorists with full knowledge of their identities and links. Therefore, they must be creative and explore various strategies to specify population boundaries and build networks from the available information, with the unavoidable consequence that these networks will be incomplete.

Missing data may affect *nodes*, when a network participant is either missed or included in the network by mistake, or *edges,* when the relationship between two people is missed or erroneously reported. If either nodes or edges are missed, there are significant consequences as regards the generalizability of research findings. For example, missing actors could be key players whose addition might change the overall network functioning as regards the links between other network participants. Descriptive measures, such as density and actor-centrality, are especially sensitive to missing data. This problem also affects statistical models estimated through ERGM simulations, which assume that the observed network is complete, i.e. it includes all nodes and edges (Malm et al., 2010).

With respect to our research design, one of the possible causes of missing data is that, by relying on criminal justice records to identify criminal ties, we may have both undercounted and overcounted the number of criminal associates. By including co-suspects in separate but related judicial cases in addition to co-defendants in the same proceedings,

we have partially taken care of the undercounting problem. However, it is possible that we may have overestimated the size of the co-offending network, especially the Islamic extremist one, whose composition may be an artifact of prosecutorial strategies designed to charge as many suspects as possible in the initial indictment. Therefore, we cannot exclude that the final network representation may be biased by law enforcement directives and initiatives.

Despite this obvious limitation, this approach is consistent with previous research efforts, which have primarily relied on law enforcement intelligence to extract network data, either in the form of written documents or through personal interviews (Malm et al., 2010; McGloin, 2004; Morselli & Roy, 2008). Additionally, we have already made considerable advances compared to this research by including two additional relational tie types between *egos* and *alters*, i.e. family and business ties, for which information was not only obtained through court documents but also through a meticulous process of data mining using 22 Internet engines. In this sense, although perhaps we did describe only financial criminal networks that "failed" (Morselli, 2009), we made a step forward by expanding our study universe beyond the "usual suspects" and including non-prosecuted accomplices identified through a variety of open sources.

A related problem concerns the temporal dimension of the network representation. By collecting and analyzing relational data cross-sectionally, we have implicitly assumed that the observed networks were static entities "frozen" in time. This was a necessary artifact that goes, however, against what we have discussed at length, i.e. that networks are flexible self-organizing structures in constant evolution. As noted, we may have captured this property when describing the far-right anti-tax subset, which included peripheral members who seemed to be expanding outside the original network boundaries and possibly joined others to form a spin-off scheme. The study of how networks evolve

longitudinally is, in fact, the new frontier of social network analysis, and methodological advances in statistical modeling have been made which allow researchers to explore new hypotheses concerning network dynamics (Snijders, 2005; Snijders, Steglich, & Schweinberger, 2007; Steglich, Snijders, & Pearson, 2010). This research is still in its infancy, but it is clear that it will be undoubtedly beneficial for criminological research.

Finally, we must discuss methodological issues concerning our analytic strategy and, in particular, the use of ERG (p*) modeling. First, there is something to be said about the analysis of multiplexity as proposed in this research. Although we made important advances compared to previous studies by including multiplex relationships in our exploratory and statistical network analyses, the separation by tie type is perhaps too simplistic and artificial. Suspects in our data set were linked by multiple tie types, which means that the co-offending, business, and family networks overlapped. Similarly to what Malm et al. did (2010), we then assessed the relative structure of each network type, and found interesting differences and similarities. However, to fully understand the role of multiplexity in financial extremist networks, it would be interesting to combine the three separate ties into a scale measuring the strength of multiplexity (Hanneman & Riddle, 2005). This new interval variable would allow us to explore important research questions concerning, for example, the type and intensity of the bond between extremists and non-extremists, which will have important theoretical and policy implications.

Focusing on our ERGM analysis, the goodness-of-fit estimation highlighted some problems that may affect our findings and should be taken into consideration for future research purposes. As noted, ERGM (p*) provides a sophisticated method to assess the simultaneous impact of structural and attribute properties on a given network and further estimate the fit of the model. With respect to our data, although the models provided a good fit for the parameters that were selected for inclusion in the stochastic analysis, they did not

uniformly account for other important structural processes observed in the networks, suggesting that a different combination of structural configurations and attribute parameters may provide a better model (Robins et al., 2007b; Snijders et al., 2006).

It is possible that this be related to the relative novelty of this method, particularly as regards the effect of "higher order" parameters that were developed to improve statistical modeling of complex networks but still need to be clarified and are undergoing continuous revisions (Snijders et al., 2006). On the other hand, the inability of the model to fully explain non-parameterized structures may be due to the incompleteness of the network, given that ERG (p*) models are sensitive to missing data. However, considering the small size of our networks and the comprehensiveness of our data collection strategy, it is unlikely that the observed networks have sufficiently large structural holes to negate the utility of these research findings (Malm, et al., 2010; Xu & Chen, 2008).

There are definitely ways in which we can improve these stochastic models in the future. For example, we could experiment with more sophisticated configurations that subsume dyadic selection effects based on similarity (i.e., homophily) in combination with higher order parameters (e.g., alternating-*k*-triangles to account for transitivity effects), which would translate into structural balance (Robins et al., 2001). In simple terms, a more complex model that includes a combination of actor attributes and structural properties would be able to better explain how two similar actors meet a third one with the same trait and form a clique. In addition, it would be helpful to include other dichotomous and continuous variables as covariates to test their impact on network structures. For instance, it would be interesting to examine how suspects' role in the scheme (e.g. leader vs. subordinate) affect tie formation, or whether highly committed extremists associate with extremists exhibiting lower commitment levels or with non-extremists, using the new

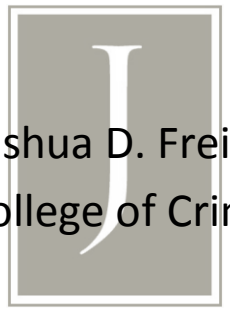
taxonomy based on the strength of ideological association scores proposed in this dissertation.

To conclude, we realize that this study has many limitations, which are in part related to these author's choices concerning research design and analytic method, and in part due to more general issues inherent in the newness of this topic and limited methodological advances. However, we believe this dissertation makes an important contribution to the criminology literature and the study of financial extremist crime and criminal networks for the very same reasons. Ultimately, it is our hope that whatever mistake we made will provide an opportunity for improvement in the future.

U.S. Extremist Crime Database (ECDB)

Codebook & Additional Project Documentation

Principal Investigators



Joshua D. Freilich
John Jay College of Criminal Justice

Steven M. Chermak
Michigan State University

Introduction

Since 2006, the Department of Homeland Security (DHS) directly, as well as through the National Consortium for the Study of Terrorism and Responses to Terrorism (START), has funded the United States Extremist Crime Database (ECDB). The ECDB is a relational database on the (violent) incidents & (financial) schemes, suspects, victims & targets, suspects & victims' social ties, and group characteristics (as well as an assessment of the quality of the open-source information used to code the database) committed by far-rightists, jihadists & Arab nationalists, and animal and environmental rights extremists in the U.S. since 1990. The ECDB is the first of its kind database and it is a valuable resource for policymakers and researchers.

The ECDB began in 2006 and originally only focused on violent & financial crimes committed by far-rightists. In 2009, the ECDB expanded to include financial & violent crimes committed by jihadists, secular Arab nationalists and animal and environmental rights extremists. The ECDB grew out of Freilich's participation in the 2005 DHS Faculty and Student Summer Research Team Program. Freilich spent the summer in residence as a START fellow and with Chermak began a comprehensive literature review on right-wing extremism and political crimes (Gruenewald, Freilich, and Chermak 2009).

The ECDB expands the universe of cases relevant to the study of terrorism. Unlike other terrorism-focused databases, the ECDB includes ideological and non-ideological crimes, violent and non-violent (e.g., financial) crimes, terrorist and non-terrorist acts, crimes committed by groups and lone wolves, and cases prosecuted federally and under state-jurisdictions.

The unique data collected by the ECDB allows us to examine important policy-relevant questions not previously addressed. The data will be used to investigate the connections across different types of offenses, whether divergent crimes covary on the micro or macro-levels, whether these patterns have changed over time, and whether there are individual or regional variations in activity. The data allow for the study of whether offenders "escalate" (e.g., from non-violent tax refusal cases to violent racist attacks or terrorist bombings), and whether comparisons of criminal activity exist by group type, ideology, structure, recruitment, or organizing characteristics. Importantly, the data allows for the comparison of criminal and extremist groups that do not employ "terrorist" methods with those that do. In addition, the ECDB is uniquely positioned to study the "criminal careers" of the suspects it codes. Once a suspect is included any prior or subsequent criminal incident (s)he committed are also noted in the study.

The data will also be used to examine important theoretical questions such as whether ideologically motivated offenders also commit non-ideological routine crimes. Finally, the ECDB's exhaustive methodology will allow us to identify the strengths and weaknesses of using open source materials because we systematically document what types of data are available from specific types of open sources for specific variables.

These findings will advance the state of knowledge and will be useful to scholars, law enforcement and funding agencies. The "process" of creating this database will identify an important data compilation process that will be transferable to scholars investigating the criminal activities of other types of extremists and terrorists.

The strategy used to construct the ECDB was the compilation and analysis of open source information across several units of analysis. As a relational database using Microsoft ACCESS, the ECDB allows for analysis across the variables found in the various codebooks. For example, if a researcher wants to compare the gender of the suspects to the gender of the victims, the ECDB takes into account that there may be two suspects and three victims. Similarly, the ECDB could limit its analysis to investigate complicated issues such as incidents where law enforcement officers were killed by skinhead suspects to examine if weapon type varies between homicide incidents that involved local, state, or federal law enforcement officers. A non-relational database does not have the capabilities to answer such questions. To make the ECDB relational, unique ID numbers were given to each incident and these numbers were connected to any suspects, victims, or groups also associated with the incident. Although all the variables were collected around the incident, the relational database allows us to analyze data between all codebooks, even if an incident codebook variable is not part of the analysis. The major benefit of using ACCESS and making the ECDB relational is to offer researchers the tools to ask very specific and complicated questions of their data.

The ECDB was developed in three-related stages.

IDENTIFYING CASES

The first stage was a multi-tiered data collection effort to identify violent and financial crimes committed by right-wing, jihadist, Arab nationalist, and animal/environmental rights extremists from 1990 to the present. Incidents were identified from existing terrorism databases, official records, scholarly works, newspaper accounts and watch-group reports:

A. **Existing Terrorism Databases.** Incidents were extracted from databases such as the *American Terrorism Study* (ATS), *Global Terrorism Database* (GTD), *Monterey Institute*'s database on chemical, biological, nuclear cases of the far-right, and the *RAND-MIBT* database. The RAND-MIBT database includes a large number of relevant incidents and rich data on indictments and other court proceeding documents. In addition, PI Chermak was involved in a project to create a national archive of terrorism databases. This project archived and made available all known databases on international and domestic terrorism activities. Relevant incidents were extracted for the ECDB.

B. **Official Sources.** Incidents were collected from several law enforcement reports, such as the FBI's *Terrorism in the United States* annual report, and government agency reports that contained useful data. These included *congressional hearing reports* (e.g., the House and Senate have conducted hearings on the militia movement and anti-government groups, jihadists and animal/environmental rights extremists that featured testimony that included listings- and details- of crimes committed by these extremists). In addition, ideologically motivated tax refusal cases were documented from the *Internal Revenue Service* (IRS), and the Department of Justice. Similarly, material support and other financial crime cases involving extremists were documented from the Department of Justice. The IRS maintains a tax evasion database and various DOJ agencies issue press releases about (and sometimes provide links to) the civil actions, indictments, and convictions about a wide range of illegal acts.

C. **Scholarly and Journalist Accounts**. Since 2005, the PIs have reviewed, and critiqued hundreds of *scholarly and journalistic accounts* on the far right, jihadist, and animal/environmental rights extremists. Similarly, there are published case studies that provided both chronologies and a wealth of information about specific events, suspects, victims and groups related to crimes committed by these extremists.

D. **Watch-group Reports.** Watch-groups, such as the *Southern Poverty Law Center*, the *Anti-Defamation League*, *the Militia Watchdog Organization*, *the Center for Democratic Renewal*, and *Political Resource Associates*, provide chronological and incident information via the WWW, reports, and press releases. For example, many scholars, law enforcement personnel, watch-group employees and reporters belong to a listserv affiliated with the militia watchdog website. Members circulate newspaper clippings, reports, and documents about

militia groups and other far right activities as well as jihadist and environmental rights extremist activities across the country almost daily. Since 1995 PI Freilich has downloaded and stored these materials.

E. Media Searches. Media publications provide important open source materials. PI Chermak's (2002) study on the militia movement, for example, included a national search of media stories (in several databases) published between 1990 and 1998 on patriot, tax, environmental, and militia crimes. We also conducted systematic searches for additional incidents in a variety of general newspaper and locally archived newspaper databases.

These sources were used to create a listing of all known violent and financial crimes committed by far-rightists, jihadists, Arab nationalists and animal/environmental rights extremists in the United States since 1990.

SEARCHING CASES

Each identified incident and group was treated as a case study with the goal of compiling as much open source information as possible. Each case & group was systematically searched in existing terrorism databases, official sources, watch-group reports, as well as 26 web-engines grouped within a primary and secondary open-source search.[12] These searches uncover all published open source materials on each case & group. Additional criminal cases uncovered during these searches were treated as separate incidents and added to the database.

The information uncovered includes media accounts; government documents; court records- indictments; appeals; videos; blogs; books; watch-group reports, movement produced materials and scholarly accounts.

The primary open source search accesses the following seven resources:

1. Lexis-Nexis
2. Proquest
3. Yahoo
4. Google
5. Copernic
6. News Library
7. Westlaw

The secondary open source search accesses the following resources:

8. Google Scholar (Both Articles & Legal Opinions)

[12] From March 2006 to March 2009, a 27th search engine- infotrac- was also searched. This engine was then removed from the JJC & MSU online libraries. Infotrac focused on health issues & was used for cases that implicated chemical, biological, nuclear, or radiological weapons.

9. Amazon
10. Google U.S. Government
11. Federation of American Scientists
12. Google Video
13. Center for the Study of Intelligence
14. Surf Wax
15. Dogpile
16. Mamma
17. Librarians' Internet Index
18. Scirus
19. All the Web
20. Google News
21. Google Blog
22. Homeland Security Digital Library

Coders (see below) searched each suspect in four additional search engines to uncover prior and/or subsequent crimes they may have committed:

23. Vinelink
24. The inmate locator
25. Individual State Department of Corrections (DOCs)
26. Blackbookonline.info

Open-Source Search Protocol

***Primary Search Engines**:* Every case should FIRST be CAREFULLY searched in these PRIMARY search engines:

1. Lexis-Nexis: Lexis-Nexis will only open in a new browser window or tab, but will not search. The searchers will be responsible for limiting the source material to the location of the case and then searching using keywords. Be careful to search all the following options:

    a. NEWS >> For Lexis-Nexis to return the most relevant results, it is important to search newspapers that are specific to the region where the incident occurred. To do this, (1) click on the 'Source' tab in the top left hand corner of the page. (2) Filter by Country, selecting United States and (3) then narrow the region to the state(s) or area where the incident occurred. (4) Under publication type, click on the 'News' folder and the check the box beside the state news sources. (5) Click 'OK Continue.' You will be returned to the main search page, but now Lexis-Nexis will focus on only publications within the region where the incident occurred. This is important because the default Lexis-Nexis search only searches major world publications, ignoring smaller, localized publications that cover "typical" criminal acts. HOWEVER, the above is only applicable to searches involving specific crimes & incidents.

    For searches focused on GROUPS you should *NOT narrow your <u>initial</u> search*. Instead, you should begin with the default lexis-nexis & "globally" search the specific group. These searches will uncover general information about the group as well as specific events & persons related to the group.

    If specific events or individuals related to the group are identified, you must conduct targeted follow up searchers. You should narrow these searches to the specific region/person and follow the procedures outlined above-- For Lexis-Nexis to return the most relevant results, it is important to search newspapers that are specific to the region where the incident occurred (see above).

    Finally, searches focused on groups SHOULD NOT limit their searches to 1990 & subsequently. Instead, they should search earlier time periods too.

b. LEGAL >> **federal and state cases** (the link is on the top left), and then, as appropriate, search through FEDERAL, SPECIFIC STATE, BOTH, TAX, OR OTHER, i.e. where the crime was prosecuted, from the drop-down menu. We are interested in all court documents (i.e., indictments, injunctions, complaints, briefs, decisions, appeals, etc.)

2. Proquest: (AKA John Jay's "Criminal Justice Periodicals") provides useful information from smaller stories in local papers.

3. Yahoo

4. Google

5. Copernic

6. News Library: News Library will place the original search terms in their search box, but you will have to click on the "search" button to initiate the search. You should not pay for articles yet. Instead, the abstract should be cut & pasted into the MS word search file.
   In many cases, articles found through News Library are also available through Lexis-nexis, Proquest & Westlaw. You must investigate whether articles found through News Library are also available from these engines.

7. Westlaw : Searchers should search each suspect to uncover any appellate court decision that may have been published on their case.

Secondary Search Engines: Following the primary search engines, each case should be CAREFULLY searched in our SECOND LEVEL of search engines:

8. Google Scholar

9. Amazon

10. Google U.S. Government
11. Federation of American Scientists
12. Google Video
13. Center for the Study of Intelligence
14. Surf Wax
15. Dogpile
16. Mamma
17. Librarians' Internet Index
18. Scirus: This engine is useful for cases that implicate chemical, biological, nuclear, or radiological weapons.
19. All the Web
20. Google News
21. Google Blog
22. Homeland Security Digital Library: While Homeland Security Digital Library is normally password protected, ON JOHN JAY'S CAMPUS searchers can access it (from any college computer) without a password: https://www.hsdl.org/. However, off John

Jay's campus a password is required. THUS, all searchers must email the Homeland Security Digital Library to request personal account & receive a password.

23. Vinelink

24. The inmate locator

25. Individual State Department of Corrections (DOCs)

26. Blackbookonline.info

Browser, Webpage, & Search Specifics

1. *Browser settings*: There are technical limitations surrounding the searches in regards to opening new browsers or new tabs for each resource. If a searcher wishes to open new tabs in the same browser, they will need to use the Mozilla Firefox browser and do the following:

    - Under Tools --> Options ---> Tabs. Select the "a new tab" option under "New pages should be opened in;"
    - In the location bar, type "about:config" This will take you to the browser's advanced preferences. Under "Preference Name"
    - Look for " browser.link.open_newwindow.restriction" and change the value to "0"
    - Make sure that "browser.link.open_newwindow" has a value of "3" and "browser.link.open_external" also has a value of "3"

2. *Primary & Secondary Search Pages:* Make sure to search ALL of the listed search engines. While tedious it is necessary. Each engine may provide information that is lacking in the others. There is an open source literature that finds, that while yahoo & google overlap, each uncovers information that the other does not. The minority of results that are unique to each search engine will be important. This is especially true for the specialized search engines found in the secondary searches.

3. In your searches include key information about the crime, suspect names, victim names, & group names, etc.

4. ***Saving files:*** Each case should be saved as a MS word file under the case number from the Excel master file (e.g., 2312). Simply copy and paste the information you find into this word document. Do NOT summarize the information. For videos or audios related to the case or group, copy & paste its link. If the case has 2 master-file numbers then it should be saved under both (e.g., 2213-6615).

5. ***Include web link:*** Make sure to ALWAYS include the source/cite/**weblink** for each story (e.g., NY Times, headline, author, link, page number, etc) & to **highlight this link for the coder IN RED**, the date in bold and to also include any short descriptions of the case that were sent to you from the Master-file.

6. ***Organizing the materials:*** Searchers should **organize all search materials by source type**, starting with the most reliable. For example, all court documents should be listed under a section titled "Court Documents;" Next all media reports should be listed under a section titled "Media Reports; Similarly, all watch-group materials should be listed under a section titled "Watch-group Reports, etc.
   Importantly, anytime information related to a criminal incident or group is found from a specific source type- e.g., court document; media report; or watch-group publication- **at least one such piece of information from *each* source type must be saved & included in the search file**. One goal of our study is to uncover which source types have identified the incidents in our database. In other words, we are interested in knowing, for e.g., which source types documented a murder committed by "Jihadi Johnny"--- was it only captured by the media? Watch-groups? All of them? Some of them, etc?

   Finally, within each section (e.g., court documents, media reports, etc) in the search files, the searchers should list the information chronologically.

7. You are searching for information about the SPECIFIC CASE/INCIDENT- anything related to the event, suspects, victims or group (i.e., see the codebooks), *as well as all additional prior or subsequent crimes* the suspects may have committed. Thus, incidents with multiple suspects and victims may take considerable time to search. For example, an assault case with 12 Skinhead suspects and three victims will require searches to uncover information about the assault itself, each suspect- including their possible criminal histories, and each victim.

Importantly, if additional prior or subsequent crimes are identified searchers must make a listing. Searchers must treat each identified case as a new incident & search each through the web-engines. Finally, searches focused on priors committed by far-right, jihadi, or environmental or animal rights extremists are not limited to 1990 & subsequently. All prior crimes- including those before 1990- must be searched.

8. In some cases, searchers will find little information initially. Keep looking- try different spellings of the first & last names. The Lexis-Nexis & Proquest engines, for e.g., are particular about spelling and won't produce results unless you have the name 100% correct. Try including a middle name, or a middle initial, & try it without the middle name or initial... etc.
   Thus, if the name you have is Phillip Timothy Smith and you enter/search & find nothing, also try/search "Philip (ONLY ONE "L") Timothy Smith," & try "Philip Tim Smith," & "Philip T. Smith," & "Philip Smith," & "Phil Smith." etc. Make sure to try all of these permutations with Phillip (2 "L"s) as well.

   Similarly, for cases with multiple suspects, make sure to search each suspect individually—again, with different spellings, if necessary- to maximize & exhaust the search.

   In other cases, you will find a lot. If there are many stories about a case you should only include one AP or UPI story about that story from each day, unless each story has unique/additional information. Focus on the major national outlets (NY Times, LA Times, WA Post, etc) & local newspapers. For e.g., if the case involves a bombing of an abortion clinic in Salt Lake City, focus first on the national papers, the 2 Salt Lake City papers, & skim the other papers to see if they include useful or additional info.

   When searching pay attention to the date of each article or source. Different dated articles may provide different/updated/useful information about the suspects or profile the victim, or provide facts about the crime) and should be recorded.

9. ***Include all sources (including repeat information):*** While most of what comes up will be newspapers you will come across other sources as well- a website, court document - e.g., an indictment- commentary, book summary, book review, watch-group material, MY SPACE pages, blogs, information about the case on a movement- i.e., far-right website...etc. ALL this information must also be included. Extremist websites, for example, may discuss certain crimes or suspects & provide information that may not be found in newspaper articles, but are useful to us.

10. ***Unrelated cases:*** In some cases, you will come across other movement related cases (i.e., possible additional far-right crimes, incidents & events) that are mentioned in passing & ARE NOT related to the case you are searching. In this situation, you should notify the PIs and send them the information. The PIs will review the case and decide if it falls within the universe of our study.

CODING CASES

The next stage of the data collection process was to code our ACCESS "files":

1. The coder is responsible for coding the cases sent to him/her from the master file. The master file contains information on the case & lists the person who open source searched the case. The coder should contact one of the project managers or the PIs so that they can access the SECURE SERVER & download the search files.

2. The master file contains information about our cases. BUT it is not a complete incident by incident listing where each case number corresponds to a single incident. Instead, *the master-file is both over-inclusive and under-inclusive*. Over-inclusive because one case number could contain a listing of 5 criminal events committed by suspect "X." Under-inclusive because sometimes the same case was entered more than once and each time was assigned a DIFFERENT case number

3. Coders first reviewed the open source material and created a timeline and a listing of exactly how many (and which) incidents, suspects, victims & groups met our inclusion criteria and were to be coded. If an incident has multiple victims each victim is coded. If an incident has multiple suspects each suspect is coded. If an incident involves multiple groups each group is coded. If an assigned incident, suspect, victim or group does not meet the inclusion criteria it is NOT to be coded & the incident/suspect/victim/group should be sent back to the PIs for further review.

   NOTE: If a suspect OR victim is connected to multiple (i.e., more than one) incidents a SEPARATE codebook must be filled out for the suspect or victim for each of the distinct incidents they were involved in. For example, if "A" and "B" together commit one bombing a month for 12 months then 12 incident codebooks and 24 suspect codebooks must be filled out (12 suspect codebooks for A, and 12 for B). Similarly, if C is victimized in 1991 with D, in 1992 with E, & 3 times in 1994, in addition to the 5 incident codebooks, 7 victim codebooks must be filled out (5 for C and one each for D & E).

4. Coders searched these incidents, suspects, and victims using the engines listed above to double-check that the original searches were complete & did not miss important information. Importantly, if the original search materials were incomplete the coder conducted "targeted follow up searches" to fill in missing values.

The coders also searched four additional engines to find information about any prior or subsequent crimes the suspects may have committed. First the coders searched the state (where the crime was committed) DOC website. These websites contain information about the state's inmates, such as an offender's date of birth, and the history of all the charges they have been convicted of in the state, and how long they have been in prison. For example, for the state of Ohio the site is http://www.drc.state.oh.us/OffenderSearch/Search.aspx - type in the name of your suspect. HOWEVER, data is not available on people that have left the system.

Second, the website "vinelink" has information on inmates for the 50 states: https://www.vinelink.com/vinelink/initMap.do, Third, the website http://www.theinmatelocator.com was searched for similar information. However, for some states vinelink did not work or provide the needed information. Instead, for these cases we went to that state's department of corrections website and obtained the contact information of the necessary official to call to attempt to obtain that offender's information. Fourth, our coders also examined www.blackbookonline.info for additional websites that contained public record information related to their incidents. Black Book Online only allows coders to search for the web sites of public institutions in specific geographic areas that contain public information. Once connected to these sites, the coders can then search by specific names for suspects and victims.

5. Sometimes, the search files contain information about prior crimes committed by the extremist suspect or victim, or about related crimes/incidents. In these situations, the coder is responsible for noting these incidents by only coding a "skeleton" incident for each prior. A skeleton record will capture basic incident level information (I1- I5); suspect & victim information (I10 & I11); when the incident occurred (I17- I19); where it occurred (I33-I34); and the types of crimes committed (I43- I136). For example, XX was in the MASTER FILE for shooting a police officer in Ohio. The open source materials indicated that he committed tens of prior criminal incidents. The coder therefore coded a skeleton incident for each of the prior incidents.

6. Sometimes the open source information will refer to additional crimes committed by movement members that are UNRELATED to the incident, suspect or victim at hand. For example XX, a skinhead, murders a minority. A newspaper article that reports on the murder references 3 OTHER murders committed by different skinheads that are UNRELATED to the XX skinhead case. The coder must notify the PIs about these additional cases/incidents/events. They will search the master file to see if the case was already collected by the project. If the case was not already collected by the project and it satisfies our inclusion criteria they will assign it to be open source searched.

7. Often coders will obtain information about the case that is NOT in the original search files. For example, (i) coders usually obtain additional information from their follow up/targeted searches, or (ii) the PIs obtain articles or materials (from the watchdog listserv or the SPLC, etc) about the case that were NOT in the original search files. This material is either (i) placed in cells in the master file, or (ii) forwarded to the coder for review. Thus, coders may have materials that were not in the original search files. These materials must be integrated into the search files. Coders (after reviewing the master file for information not already in the original search files, reviewing the yield from their follow up searches and any information received from the PIs) should create a section at the end of the original search file document titled: ADDITIONAL SEARCH FILES UNCOVERED BY PIS AND/OR CODERS and copy & paste the information in it. On the first of every month, if necessary, coders should send all the search files they updated that month to one of the project managers so they can be updated on the server AND to the PIs so they can update their files. For cases that were coded & searched before this rule, coders should rename their file specifying it as an update to the original search file, like this for example, 2099_UPDATE_06/06/08_RB, and send it to a project manager who will add it to the related incident folder on our secure server.

8. Sometimes coders receive cases that have NO NAMED SUSPECTS IN THE MASTER FILE but which were assigned to our open source searchers. In this case, coders must follow the below steps:

    a. Must review the search files to see whether the names of the suspects or victims were uncovered.

    b. If the search files have the names of the suspects or victims the coder must contact the PIs or a project manager to search the master file to see whether we already have those suspects in the master file (i.e., check for duplications).

    c. If the case is NOT in the master file the coders should code it.

    d. If we already have the case in the master file & it is unassigned the PIs must be notified to place the two cases next to each other the master file (& note that the coder is coding both); forward to the coder the search files from the unassigned case, and the coder will code the case.

    e. If we already have the case in the master file & it is already assigned the PIs must be notified to place the cases next to each other in the master file; list the original coder as the coder of both cases & send that original coder the new search files to update their previous coding. See also Comment #15 below

9. Coders must review both the American Terrorism Study (ATS) and the Global Terrorism Database (GTD) to determine if these databases include the incidents or the suspects they are coding for our project. If yes, coders must extract this information & use it for their coding. Both the Global Terrorism Database and the American Terrorism Study are available through ICPSR. In addition, as work on the Integrated United States Security Database (IUSSD) progresses, the ECDB team will have access to ATS and GTD data that will allow more rigorous searching and identification of incidents.

10. The coders reviewed the collected open source materials so that they could fill in variables in our ACCESS files. Importantly, as the coding has progressed we have periodically conducted substantive reviews of both our search and coding protocols. We have clarified our search strategies, and clarified and revised our variables by modifying values for existing variables and adding additional variables.

    Often the search materials contained documents from different types of sources (e.g., court documents vs. watch-group report vs. a media account) that contained conflicting information. In these situations, greater weight was granted to the more "trusted" sources as defined by the empirical terrorism literature. Similar to Sageman (2004: 65) "in decreasing degrees of reliability… [we will favor] … court proceedings subject to cross examination, followed by reports of court proceedings, then corroborated information from people with direct access to information provided, uncorroborated statements from people with that access, and finally statements from people who had heard the information secondhand" (see also Damphousse, 2007). Similarly, court records were favored over media reports and media reports were favored over watch group reports. The table below lists the various types of sources in decreasing degrees of reliability:

Appellate Court decisions
Court proceedings subject to cross examination (trial transcripts)
Reports of appellate court decisions & court proceedings subject to cross examination
Corroborated information from people with direct access to information provided (i.e., key informants)
Uncorroborated statements from people with that access (i.e., key informants); Indictments; and other court documents not subject

to cross examination; and law enforcement documents
Other Media reports
Watch-group Reports
Personal views expressed in blogs, websites, editorials or Op-Ed, etc

If two media accounts disagree the following criteria was applied: First, if one source is a reliable national newspaper, for example the New York Times, and the second is an unheard of publication, credence should go to the NY Times, (though the conflicting age noted in the assessment codebook). Second, if one source is national and the other is the LOCAL newspaper (e.g., Staten Island Advance) for a crime committed on Staten Island, the local newspaper should have priority (though again the discrepancy should be noted in the assessment codebook). Finally, if there are only two competing sources, (for e.g., the NY Post vs the NY Daily News) that are of equal weight the conflicting values should be averaged. But, the discrepancy must be noted in the assessment codebook. Ultimately, we hope to contact key informants (e.g., a law enforcement agent, prosecutor or reporter who worked on a specific case) to resolve discrepancies & fill in missing data.

11. Many of our variables require a coding of either "yes," "no," or "don't know." Often, the open source materials will not mention a particular fact unless it was present. It is difficult to discern when to check "no" & when to check "don't know." For e.g., should the question "was racist music found in home/car of the suspect?" be marked no if nothing about music is mentioned in the search materials? Or should it be marked not known? The correct coding is "not known." Only check "no" when it is a clear no (which will only occur in a minority of situations). DO NOT assume anything unless it is explicitly stated.

    EXAMPLE: XX was originally a member of the Latin Kings who committed a crime spree- homicide & other crimes. During his imprisonment he joined the Aryan Brotherhood. While in the AB he murdered a black prisoner but it is unclear if this was an ideological killing or due to a personal beef. However, no article mentions XX's race. Although one would suspect he was white because it is not explicitly stated that he was white, the race of the suspect should be left blank.

NOTE: If the “don’t know” option is not provided for a variable then NOT CODING THE VARIABLE & leaving it blank will be the equivalent of coding “don’t know.”

12. What do we mean by “prevailing source” (which is a variable in all our codebooks): Quantity or quality?

    ANSWER: Both. The prevailing source is the one which overall produced the largest number of documents that were either in the search files (quantity) and that were used for coding (quality) in that it provided the most information.

13. Each coder has his/her own ACCESS files. Coders will update previously coded cases and enter their new cases into their own ACCESS files. On the first of every month coders must submit their individual ACCESS files to a project manager who will merge the individual coder files and thus update our single project ACCESS file.

CODING FINANCIAL CASES

This stage of the process involves coding financial cases in four ACCESS “files”: (1) scheme, (2) suspect, (3) business entity, and (4) quality of the open source information used. Coders must first review the open source materials to create a timeline and a listing of exactly how many (and which) schemes, suspects, and business entities meet our inclusion criteria to be coded. Importantly, if the original search materials are incomplete or if information is missing, coders must conduct "targeted follow up searches” to fill in missing values using our 26 web engines.

Scheme Codebook: Coding Issues

NOTE: This document should be in front of the coders as they code. If an assigned case does not meet the inclusion criteria it is NOT to be coded and the case should be sent back to the PIs for further review.

(1) KEY DEFINITIONS: FINANCIAL SCHEMES, CRIMES & TECHNIQUES

This phase of the ECDB project involves coding financial crimes committed by far-rightists, ELF/ALF, jihadist extremists, and Arab secular nationalists in the United States since 1995. Because of the characteristics of these crime types, several changes have been made to the codebooks to capture all relevant information. The main unit of analysis is the ***scheme*** (which replaces the “incident” for violent crime cases).

We define a *financial scheme* as an illicit financial operation involving a set of activities (i.e. *techniques*) aiming at a specific goal to obtain unlawful gain or other economic advantage through the use of deliberate deception. These activities may amount to a variety of federal offenses punishable under the provisions of the U.S. Criminal Code (e.g., money-laundering, Title 18 U.S.C., sections 1956-1957; material support to terrorists, Title 18 U.S.C., section 2339A, etc.).

The distinction between (a) scheme, (b) crime, and (c) technique is an important one, and should be clear to the coder when approaching a case to be coded. The scheme is the overall financial operation which is characterized by a set number of perpetrators aiming at a specific objective (e.g., financing of a terrorist attack) over a specific period of time (see below for additional explanations of what constitutes a “discrete” scheme).

Each perpetrator may have a distinct role in the execution of the scheme, and engage in a variety of different activities, or "techniques", to further the overall operation (e.g., 3 suspects involved in a money-laundering operation: one is the "fund-raiser", collecting money by committing other crimes, such as drug dealing; one is the "carrier", smuggling U.S. currency abroad; one is the "launderer", investing money in offshore bank accounts).

When the suspects are apprehended and brought to justice, the prosecutor may decide, for strategic purposes, to charge them with criminal offenses which may not necessarily reflect the "techniques" used (e.g. suspects are charged with the general formula "material support to a designated terrorist organization", Title 18 U.S.C., section 2339A).

To capture the nuances existing in these complex crime cases, we have created separate variables for each of these 3 key aspects:

(a) Scheme type (Q23 in "Scheme" codebook);

(b) Criminal charges (Q35-90 in "Scheme" codebook; Q298-305 in "Suspect 2" codebook);

(c) Activities/Techniques (Q125-181 in "Suspect 1" codebook).

As a general rule, coders should first identify what scheme type(s) was (or were) pursued in the assigned case, and then code all criminal charges mentioned in the indictment. Subsequently, coders should focus on the specific role each perpetrator played in the context of the scheme, and indicate what techniques were used as well as the specific charges he/she was indicted for and convicted with.

(2) SCHEMES TYPOLOGY

At present, there exists a variety of financial schemes that target citizens, businesses, financial markets, and government institutions, and are subject to federal investigation and prosecution. The following is a preliminary typology that includes fraudulent scheme types identified by the FBI, CIA, IRS, and other governmental agencies, as well as examples of tactics used by political extremists.

Coders will need to refer to these definitions when they decide what scheme or schemes are involved in the case study they have been assigned. Most times, the open source materials will have clear information on the scheme type(s) (e.g., a Ponzi scheme and a pyramid scheme). However, sometimes it may not be obvious. If coders cannot identify a specific scheme among those listed, they will choose "others" and describe the details of the scheme. In this case, coders will need to consult with the Project Manager (Roberta Belli) and/or the other team members to

decide which option applies. Eventually, these incidents will (1) either be identified as one of the listed types, or (2) used as a reference to create a new scheme type.

(i) Investment schemes

Some financial schemes are based on the promise of high rewards to individuals or companies who invest their money in various high- or (allegedly) low-risk activities. Among these, Pyramid and "Ponzi" schemes are most common and highly dangerous:

- Pyramid schemes, also referred to as franchise fraud, or chain referral schemes, are marketing and investment frauds in which an individual is offered a distributorship or franchise to market a particular product. The real profit is earned not by the sale of the product, but by the sale of new distributorships. Emphasis on selling franchises rather than the product eventually leads to a point where the supply of potential investors is exhausted and the pyramid collapses (FBI, 2009).

  A typical pyramid scheme involves members who pay a subscription price to join. Each member is promised a reward (in cash or kind, and typically large relative to subscription) for recruiting more members. For example, each member may be required to recruit five others who each recruit five more and so on to get the reward. While the promised large reward draws in members, the number of recruits required to be ultimately rewarded grows exponentially, and quickly exceeds the target population, leaving most members empty handed (IMF, 2009).

- A "Ponzi" scheme is an investment fraud wherein the operator promises high financial returns or "dividends" that are not available through traditional investments. However, instead of investing victims' funds as promised, the operator pays the "dividends" to initial investors using the principle amounts "invested" by subsequent investors. The scheme generally falls apart when the operator flees with all of the proceeds, or when a sufficient number of new investors cannot be found to allow the continued payment of "dividends" (FBI, 2009).

  A Ponzi scheme is similar to a pyramid scheme in that both are based on using new investors' funds to pay the earlier backers. One difference between the two schemes is that the Ponzi mastermind gathers all relevant funds from new investors and then distributes them. Pyramid schemes, on the other hand, allow each investor to directly benefit depending on how many new investors are recruited. In this case, the person on the top of the pyramid does not at any point have access to all the money in the system. In other

words, Ponzi investors are usually unaware of the fraudulent operation, whereas pyramid ones may be aware of some (if not all) parts of the scheme functioning.

Both pyramids and Ponzis typically have no true business activity or investments to generate the promised high returns, although some business, product, or service may be used as a front. In addition, fraudulent operators may use separate schemes, incorporating Ponzi and pyramid characteristics, to prolong operations (IMF, 2009).

(ii) Telemarketing schemes

Telemarketing schemes have become very popular with the advent of the Internet. So-called “advanced fee schemes” and “Nigerian letter scams” are two typical examples of this scheme type.

- An advanced fee scheme occurs when the victim pays money to someone in anticipation of receiving something of greater value, such as a loan, contract, investment, or gift, and then receives little or nothing in return. The variety of advance fee schemes is limited only by the imagination of the con artists who offer them. They may involve the sale of products or services, the offering of investments, lottery winnings, "found money," or many other "opportunities” (FBI, 2009).

- Nigerian letter scams combine the threat of impersonation fraud with a variation of an advance fee scheme in which a letter, mailed from Nigeria, offers the recipient the "opportunity" to share in a percentage of millions of dollars that the author, a self-proclaimed government official, is trying to transfer illegally out of Nigeria. The recipient is encouraged to send information to the author, such as blank letterhead stationery, bank name and account numbers and other identifying information using a facsimile number provided in the letter. Some of these letters have also been received via e-mail through the Internet. The scheme relies on convincing a willing victim, who has demonstrated a "propensity for larceny" by responding to the invitation, to send money to the author of the letter in Nigeria in several installments of increasing amounts for a variety of reasons.

(iii) ID fraud schemes

Impersonation fraud (or ID fraud) schemes occur when someone assumes another person's identity to perform a fraud or other criminal act. There are various ways in which criminals can get the information they need on someone's identity from a variety of sources, such as the theft of personal belongings (e.g., wallet, trash, credit cards, etc.). Victims may be approached in person, by telephone, or on the Internet and asked for sensitive information.

- "Phishing" is a tactic used by Internet-based thieves to trick unsuspecting victims into revealing personal information they can then use to access the victims' financial accounts. These criminals use the information obtained to empty the victims' bank accounts, run up credit card charges and apply for loans or credit in the victims' names. Phishing scams often take the form of an e-mail that appears to come from a legitimate source.

(iv) Tax avoidance schemes

Every year an undefined number of US citizens – estimated in the hundreds of thousands – use abusive schemes to circumvent tax laws or evade taxes. These schemes include various kinds of activities, which can be very simple or very complex, evidently illegal or carefully constructed to disguise the illegality of the scheme. Known cases involve the use of abusive tax shelters, exempt organizations, and strategies based on misinterpretations and distortions of federal tax obligations.

The IRS publishes annually a list of the most popular tax avoidance scams (the "Dirty Dozen"). The following are some examples of common tax avoidance schemes and tactics:

- Hiding Income Offshore. Some individuals try to avoid paying U.S. taxes by illegally hiding income in offshore bank and brokerage accounts or using offshore debit cards, credit cards, wire transfers, foreign trusts, employee leasing schemes, private annuities or life insurance plans. These funds are later wired back to the U.S. as a foreign investment of some type, e.g., loans or capital investment. Tax authorities and accountants call most of these foreign countries tax havens.

- Disguised Corporate Ownership/Nominees. Also called "shell" corporations, these exist on paper but transact either no business or minimal business. Some people use nominees (i.e. a person designated to act for another as an agent or trustee) and form domestic or offshore shell corporations for the purpose of disguising the ownership of a business or financial activity. Once formed, these anonymous entities can be used to facilitate underreporting of income, non-filing of tax returns, engaging in listed transactions, money

laundering, financial crimes and terrorist financing. Oftentimes, the nominees are close relatives or professionals such as corporate stakeholders, employees, attorneys, accountants, etc.

- Misuse of Trusts. Promoters of abusive tax schemes are increasingly urging taxpayers to transfer assets into trusts. The promoters promise a variety of benefits, such as the reduction of income subject to tax, deductions for personal expenses paid by the trust and reduction of gift or estate taxes. Taxpayers should be aware that abusive trust arrangements will not produce the tax benefits advertised by their promoters and that the IRS is actively examining these types of trust arrangements. More than a dozen injunctions have been obtained against promoters, and numerous promoters and their clients have been criminally prosecuted. Before entering any trust arrangements, taxpayers should seek the advice of a trusted tax professional.

- Tax refusal. Individuals who refuse to pay taxes for ideological reasons share similar anti-government ideas concerning tax laws, which they believe have been made needlessly complex to keep people from investigating and finding the loopholes in the system. Tax protesters, however, have utilized different ways to avoid tax liability (Sanger-Katz, 2006). Some file bogus tax returns, indicating for example all zeros on their Form 1040 (using the so-called "Zero-return scheme"), or claiming so many exemptions that an employer does not have to withhold payroll taxes. Others say the simple act of filling out a tax return means you are entering a contract with the government. They express their refusal to comply with tax laws by not filing any income return, and instead begin sending letters filled with questions and objections to the IRS.

- Frivolous Arguments. Promoters of frivolous schemes encourage people to make unreasonable and unfounded claims to avoid paying the taxes they owe. Most recently, the IRS expanded its list of frivolous legal positions that taxpayers should stay away from. The most recent update of the list of frivolous positions includes: misinterpretation of the 9th Amendment to the U.S. Constitution regarding objections to military spending, erroneous claims that taxes are owed only by persons with a fiduciary relationship to the United States, a nonexistent "Mariner's Tax Deduction" related to invalid deductions for meals and the misuse of the fuel tax credit (IRS, 2009).

- Zero Wages. Filing a phony wage- or income-related information return to replace a legitimate information return has been used as an illegal method to lower the amount of taxes owed. Typically, a Form 4852 (Substitute Form W-2) or a "corrected" Form 1099 is used as a way to improperly reduce taxable income to zero. The taxpayer also may submit a statement rebutting wages and taxes reported by a payer to the IRS. Sometimes fraudsters even include an explanation on their Form 4852 that cites statutory language on the definition of wages or may include some reference to a paying company that refuses to issue a corrected Form W-2 for fear of IRS retaliation (IRS, 2009).

- Return Preparer Fraud. Dishonest tax return preparers can cause many problems for taxpayers who fall victim to their schemes. These scam artists make their money by skimming a portion of their clients' refunds and charging inflated fees for return preparation services. They attract new clients by promising large refunds. Some preparers promote the filing of fraudulent claims for refunds on items such as fuel tax credits to recover taxes paid in prior years (IRS, 2009).

- Abuse of Charitable Organizations and Deductions. The IRS continues to observe the misuse of tax-exempt organizations. Misuse includes arrangements to improperly shield income or assets from taxation, attempts by donors to maintain control over donated assets or income from donated property and overvaluation of contributed property (IRS, 2009).

- Form 843 Tax Abatement. This scam rests on faulty interpretation of the Internal Revenue Code. It involves the filer requesting abatement of previously assessed tax using Form 843. Many using this scam have not previously filed tax returns and the tax they are trying to have abated has been assessed by the IRS through the Substitute for Return Program. The filer uses the Form 843 to list reasons for the request. Often, one of the reasons is: "Failed to properly compute and/or calculate IRC Sec 83-Property Transferred in Connection with Performance of Service" (IRS, 2009).

- Employment Tax Evasion. The IRS has seen a number of illegal schemes that instruct employers not to withhold federal income tax or other employment taxes from wages paid to their employees. Such advice is based on an incorrect interpretation of Section 861 and other parts of the tax law and has been refuted in court. Lately, the IRS has seen an increase in activity in the area of "double-dip" parking and medical reimbursement issues. Employer participants can also be held responsible for back payments of employment taxes, plus penalties and interest. It is worth noting that employees who have nothing withheld from their wages are still responsible for payment of their personal taxes (IRS, 2009).

- Corporation Sole. Participants apply for incorporation under the pretext of being a "bishop" or "overseer" of a one-person, phony religious organization or society with the idea that this entitles the individual to exemption from federal income taxes as a nonprofit, religious organization. When used as intended, Corporation Sole statutes enable religious leaders to separate themselves legally from the control and ownership of church assets. But the rules have been twisted at seminars where taxpayers are charged fees of $1,000 or more and incorrectly told that Corporation Sole laws provide a "legal" way to escape paying federal income taxes, child support and other personal debts (IRS, 2009).

(v) Money-laundering schemes

Money-laundering is the conversion of illicit incomes into assets that cannot be traced back to the underlying criminal activity that generated them (Reuter and Truman, 2004). Money-laundering typically involves three consecutive phases, i.e. (1) placement, (2) layering, and (3) integration (Masciandaro et al., 2007).

The first phase ("placement" or "pre-wash" phase) involves the collection and deposit of "dirty" money in a legitimate financial institution (e.g. a bank). In the second phase ("layering" or "main wash" phase), the money is transferred to accounts or investment options all around the world to disguise its illicit origin. The third phase ("integration") serves to reintegrate the now "clean" money back into the legitimate economy by purchasing, for example, real estate or luxury items (e.g. expensive cars, ships, diamonds, etc.).

At each stage, various techniques are used which largely depend on the predicate offense (e.g. drug trafficking, smuggling of counterfeited goods, Internet fraud, etc.). The following are examples of money-laundering tactics:

- Structuring financial transactions ("smurfing"). This technique is frequently used in the first stage ("placement") and it involves breaking down cash deposits from illegal activities into amounts below the reporting threshold of $10,000. Couriers ("smurfs") go to various financial institutions and make cash deposits or obtain cashier's checks, money orders, traveler's checks, etc., on the same day or consecutive days.

- Wire or other electronic wire transfers. "Dirty" money can be moved around the world by ordering banks to transfer its control sending notification to another institution by cable or electronically. Such transfers remain a primary tool in the money-laundering process, as funds can be transferred through different banks in several jurisdictions in order to blur the trail to the source of the funds (Reuter and Truman, 2004).

- Converting "dirty" money into monetary instruments. This technique is typical of the second phase ("layering"), and it involves converting cash into monetary instruments, such as cashier's checks, money orders, traveler's checks, stocks, bonds, etc.

- Real estate transactions, overvalued exports, etc. The money launderer needs to provide an explanation for his wealth that appears to be legitimate. "Integration" is the process of routing money into the banking system to make it appear that it comes from normal business earnings (third phase of money-laundering). Using front companies, sham loans, and false export–import invoices commonly does this. Money launderers will purchase property at high cost with partial payment (down payment) made in cash. The purchase documents are prepared showing a lower price by excluding the down payment or under-the-table payments. Overvaluation of exports is used to justify deposits as funds from foreign sources.

- Currency exchange bureaus. These are not as heavily regulated as banks, and may sometimes not be regulated at all and instead used for money-laundering. Substantial foreign exchange transactions are said to be shifting from banks to these small enterprises. Currency exchange bureaus are used for two main laundering techniques. The first is to change large amounts of criminal proceeds in local currency into low-bulk currency for physical smuggling out of the country, and the second is electronic funds transfer to offshore centers. In one reported case, a currency bureau reportedly exchanged the equivalent of more than $50 million through a foreign bank without registering transactions in its official records (Reuter and Truman, 2004).

(vi) "Money-dirtying" schemes

"Money-dirtying" is similar to money laundering (i.e. the techniques used are often the same), although there are important differences.

The term "money-dirtying" was coined with reference to terrorism financing activities that did not necessarily originate from predicate crimes (Masciandaro et al., 2007). In this sense, money-dirtying (also called the "reverse" of money-laundering) refers to the process of using money raised legitimately (e.g. through donations or legitimate investments) for illicit purposes (i.e. funding of terrorist operations). In some instances, money laundering and money dirtying overlap, for example when illegally obtained capital is used for terrorism financing purposes (i.e. money from drug trafficking activities).

There are two main differences between money laundering and money dirtying: (1) the source of the money, i.e. criminal in the former, either legitimate or criminal in the latter; (2) the goal of the financial operation, i.e. transforming "dirty" money into expendable income vs. channeling funds of any origin to individuals or groups to enable acts of terrorism.

Many terrorism-financing cases involving money-dirtying and money-laundering activities are prosecuted as *"material support"* cases. Notice that, for the purposes of this database, we will only code "material support" cases that involve financial operations (i.e. movement of money).

The same techniques discussed above can be used in the context of money-dirtying operations. After 9/11 other methods have been under scrutiny for their possible use in terrorism financing, e.g.:

- Informal value transfer systems (e.g. Hawala). A hawala is a money transfer without the movement of money. A person gives funds to another person (called a hawala) for transfer to another country. The hawala sends a fax or calls his contact in another country to provide funds to someone there. The person gives the funds to the other person in the other country. The hawala in this country charges a commission for making the transfer and keeps a record of the amount owed to the person in the other country. The person in the

other country shows a receivable on his books. In time, the two hawalas' books will be balanced by either settling up or other transactions. This scheme requires a great amount of trust between the two hawalas.

(3) INCLUSION CRITERIA

To qualify as a scheme to be coded in our database the following criteria must be met:

(i) The scheme involved illegal financial activity (i.e. at least one financial crime as listed in the "Scheme codebook").

(ii) The scheme has allegedly been carried out in specific locations during a certain time period as opposed to a vague allegation. In other words, rumors/hearsay/unsubstantiated allegations are not enough. For example**,** we will NOT code facts that state "X laundered money for a drug gang in the past" because the allegation is too vague/general. BUT we will code this in the suspect codebook under previous criminal history.

(iii) The act led to a *criminal investigation* by federal or state (e.g., New York State, Vermont, etc) authorities. It is important to note that some financial investigations may be started civilly (e.g. with an injunction against a financial consultancy company). At this moment, however, we do not code cases that were only prosecuted by civil or administrative courts. Coders must review the search materials to determine whether the case was eventually prosecuted by a criminal court. If the answer is no, then the coder should not code the case.

What to do with allegations of illegal behavior that were not substantiated by law enforcement or court officials, i.e. police/prosecutor did not pursue the case because no actual crime occurred or there is no sufficient evidence to proceed?

If the decision is made by the police or prosecutor in the initial phase of an investigation, the case should not be coded because this indicates that the charges were not substantiated, i.e. no incident that we are interested in occurred.

However, once charges are initiated and criminal proceedings have begun, we code it. This is because an investigation concluded that something happened and we are interested in the court results (even if the jury eventually acquits the defendant or the prosecutor drops the charges).

As a general rule: charges dropped by the police – WE DO NOT CODE; charges dropped by the prosecutor or further in the process – WE DO CODE.

(iv) The scheme, or any portion of it, was committed inside the United States. Some schemes may involve several different countries. This is fine, as long as the scheme had basis on U.S. territory at some point (e.g. perpetrators owned trust funds in the U.S.). See section below for more information on what constitutes a discrete scheme.

(v) The scheme was committed between 2000 & the present.

(vi)The scheme was committed in whole or in part by at least one far-rightist, local or global jihadist, secular Arab nationalist, or animal/environmental rights extremist (unless it is a "prior" or "subsequent"):

The **far-right** is composed of individuals or groups that subscribe to aspects of the following ideals: They are fiercely nationalistic (as opposed to universal and international in orientation), anti-global, suspicious of centralized federal authority, reverent of individual liberty (especially their right to own guns, be free of taxes), believe in conspiracy theories that involve a grave threat to national sovereignty and/or personal liberty and a belief that one's personal and/or national "way of life" is under attack and is either already lost or that the threat is imminent (sometimes such beliefs are amorphous and vague, but for some the threat is from a specific ethnic, racial, or religious group), and a belief in the need to be prepared for an attack either by participating in or supporting the need for paramilitary preparations and training or survivalism.

Note: The mainstream conservative movement and the mainstream Christian right are not included.

The **Islamic Jihadist** movement is composed of individuals or groups that subscribe to aspects of the following ideals:

- Only acceptance of the Islamic faith promotes human dignity as well as affirms God's authority;
- Rejection of the traditional Muslim respect for "People of the Book," i.e., Christians & Jews;
- "Jihad" (defined as to struggle in the path of God in the example of the Prophet Muhammad & his early companions)" is a defining belief in Islam. This belief includes the "lesser Jihad" that endorses violence against a corrupt other;
- the Islamic faith and or one's people are oppressed and under attack in both "local and nominally Muslim" Middle-Eastern/North African/Asian governments that are corrupt & authoritarian, as well as in non-Islamic nations (e.g., Israel/Palestine, Russia//Chechnya; India/Kashmir, etc) that occupy indigenous Islamic populations (an argument for political & military mobilization);
- the West in general & the U.S. in particular supports the corruption, oppression & humiliation of Islam, and exploits the region's resources;

- the culture of the West in general & the U.S. in particular (e.g., gay-rights, feminism, sexual permissiveness, alcohol abuse, racism, etc) has a corrosive effect on social & religious values;
- the people of the West in general and the US in particular are responsible for the actions of their governments and culture (NOTE: this is an important element that distinguishes jihadists from other Muslims critical of Western states because it could justify the killing of innocents);
- it is a religious obligation is to promote a violent Islamic revolution to combat this assault on Islam, oppression, corruption & the values of the West by targeting nonbelievers (both Muslims and non-Muslims);
- Jihad will remain an individual obligation until all lands that were once Muslim (e.g., Andalusia- Southern Spain, Palestine, Philippines, etc) are returned & Islam again reigns supreme in those countries;
- Islamic law- Sharia- provides the ideal blueprint for a modern Muslim society and should be implemented in all "Muslim" countries by force

NOTE: *Global jihadists* are most concerned with combating the West in general & the United States in particular, while *local jihadists* are focused on a specific conflict such as Somalia; Russia/Chechnya; India/Kashmir; Israel/Palestine; China/Uighur; Philippines/Moro, etc.

NOTE: Global versus local jihad refers to the goals/ideology the suspect subscribes to and NOT the suspect's activities. For e.g., a suspect supporting Hamas would be coded as a local jihadist (even if the suspect's activities were transnational, e.g., laundering money across multiple continents) because Hamas disavows support for a global struggle versus the West & is only concerned with Israel/Palestine. The key point is the ideological goals of the suspect and not the suspect's individual activities.

Secular Arab nationalists are composed of individuals or groups that subscribe to aspects of the following ideals:

- the suspect's nation (either Muslim or Middle Eastern) that he identifies with is either oppressed by a "local usurper" Middle-Eastern/North African/Asian government that is corrupt & authoritarian, or the nation is occupied and/or under attack from the West in general or the United States in particular;
- the West in general & the U.S. in particular supports the corruption, oppression & humiliation of this nation and exploits its resources;
- the people of the West in general and the US in particular are responsible for the actions of their governments and culture;
- Action must be taken to combat this assault, oppression, & corruption;

- The goal is true independence from the West in general & the United States in particular

Environmental and animal rights extremists are individuals or groups that subscribe to aspects of the following ideals:

- Support for biodiversity and bio-centric equality (i.e., that humans are no greater than any other form of life and have no legitimate claim to dominate earth);
- the earth and/or animals are in imminent danger;
- the government and /or parts of society such as corporations are responsible for this danger;
- this danger will ultimately result in the destruction of the modern environment and/or whole species;
- the political system is incapable and/or unwilling to fix the crisis by taking actions to preserve American wilderness, protect the environment and support biological diversity;
- there is a need to defend the environment and/or animals

NOTE: *Environmental rights extremists* (primarily) are most focused on the environment while *animal rights extremists* (primarily) are most concerned with the rights of animals.

NOTE: There might be cases where non-financial crimes are committed by suspects involved in the scheme (e.g. drug dealing, violent crimes, etc.). We will capture this information by coding the crime in a separate variable in the scheme codebook, i.e. "other non-financial crime – specify" (e.g. attempt to kidnap hostages).

In this case, coders should contact one of the PIs or senior research assistants so they can check whether the incident is already in the ECDB (for violent incidents). If it is, coders will code this information in a separate variable in the EFCDB database ("Incident in ECDB?" N/Y). If it is not, they will conduct targeted searches to locate relevant information on the non-financial incident committed before or after the scheme, and code it in the ECDB database (for violent incidents).

Coders should refer to the inclusion criteria for the ECDB before coding the new incident. If the targeted searches do not bring up relevant or sufficient information on the non-financial crimes, coders will simply code these as "priors" in the EFCDB codebooks.

(3) WHAT CONSTITUTES A DISCRETE SCHEME?

Similar to the UCR and the definition of "incident" used in the first phase of the ECDB project which focused on violent crimes, a "scheme" may involve more than one financial crime (e.g. mail fraud, tax evasion, and money-laundering) as well as multiple techniques (e.g. wire transfers, use of shell companies, offshore bank accounts, etc.).

It is important that coders learn to distinguish between *a financial scheme* (e.g. tax avoidance scheme*), a financial crime* (e.g., the failure to file an income return, punishable under Title 26 of the US Tax Code*), and the techniques used to further scheme* (e.g. use of offshore bank accounts) as they are coded in separate variables in the Scheme and Suspect codebook (as detailed in the sections above). In addition, similar to the "incident", a "scheme" involves different perpetrators (who are usually identifiable persons) and victims (who could be persons as well as business entities).

"Schemes", however, are different from "incidents" because they cannot always be identified by specific spatial and temporal coordinates. Instead, financial schemes are usually committed over a prolonged period of time (for which it is often possible to identify start and end dates, e.g. from 1995 to 2002) and may involve multiple locations inside and, sometimes, outside the U.S. borders (e.g., in countries with lax regulatory systems or considered "tax havens", like the Cayman Islands or the Bahamas).

The following criteria determine what constitutes a discrete financial scheme for the purposes of this study:

(i) A discrete scheme usually happens over a prolonged period of time and has specific start and end dates (e.g. started in 1999, ended in 2002). Thus, schemes that have different start or end dates should be coded as DISTINCT SCHEMES.
EXAMPLE: Perpetrators started scheme "A" (e.g., Ponzi) in 1998, which collapsed in March 2003 after FBI investigation. The same perpetrators started scheme "B" (e.g. pyramid scheme) in 2000, which also ended in March 2003. These should be coded as 2 discrete (though linked) schemes, i.e. 2 codebooks.

(ii) A discrete scheme may involve activities carried out in one or multiple locations, which must be identified as specific US cities, counties, and states, or in foreign countries. However, to be coded in our database, the primary site where the scheme was perpetrated must be identified as a location in any of the 50 U.S. states (e.g. perpetrators operated a phony business from shell companies located in the U.S. and Costa Rica, targeting mostly American and Canadian customers/victims).

(iii) Situations that involve different crimes and techniques, different goals, different suspects, and occur during different time frames & different places are also usually distinct schemes.

EXAMPLE: Four suspects started a Ponzi scheme in 1998, which victimized 60 investors. At the same time, the same suspects plus two more started a pyramid scheme, in which 100 persons were involved including some of the previous investors. These should be coded as 2 discrete (though linked) schemes, i.e. 2 codebooks.

(iv) PLANNED/CONSPIRACY ACTIONS will be counted as separate schemes. However, to be considered a separate scheme, each plan/intended/conspiracy MUST have a concrete/firm goal, as well as overt acts committed to begin carrying out the crime(s).

Q#	Variable Name	Variable ID	Values	Description
IF1	Scheme ID	IF_id	Numeric	List the scheme identification number based on the coder's personal identification number.
IF2	Masterfile ID	IF_id2	Numeric	List master-file identification number. If listing more than one number, separate with a semicolon.
IF3	Relational ID	IF_id3	Numeric	Relational ID (Scheme ID + Mastefile ID)
IF4	Scheme description	IF_name	Text	Describe who, what, where and when of scheme
IF5	Scheme start year	IF_startyr	Numeric	Time Period: Start Date Year
IF5	Scheme start month	IF_startmth	Numeric	Time Period: Start Date Month
IF5	Scheme start day	IF_startday	Numeric	Time Period: Start Date Day
IF6	Scheme end year	IF_endyr	Numeric	Time Period: End Date Year
IF6	Scheme end month	IF_endmth	Numeric	Time Period: End Date Month
IF6	Scheme end year	IF_endday	Numeric	Time Period: End Date Day
IF7	Length	IF_length	Numeric	Length of scheme in months
IF8	# Suspects	IF_#susp	Numeric	Total number of suspects

Q#	Variable Name	Variable ID	Values	Description
IF9	Related suspect ids	IF_rsusp	String	Related Suspect ID numbers
IF10	# Victims	IF_#vics	Numeric	Estimated number of victims
IF11	# Related businesses	IF_#comp	Numeric	Total number of related businesses/companies
IF12	Related business IDs	IF_comps	String	List related business IDs
IF13	Why discrete scheme?	IF_why	String	Why is this scheme discrete? Refer to inclusion criteria
IF14	GTD?	IF_gtd	(0)No; (1)Yes; (-99)Missing	Is the scheme in the GTD?
IF15	ATS?	IF_ats	(0)No; (1)Yes; (-99)Missing	Is the schemein the ATS?
IF16	FBI definition	IF_terdef	(0)No; (1)Yes; (-99)Missing	Does the scheme meet FBI/ATS definition of terrorism?
IF17	Labeled terrorism?	IF_tergov	(0)No; (1)Yes; (-99)Missing	Was scheme labeled terrorism by government or law enforcement according to the open source materials?
IF18	Coder	IF_coder	String	Source Coder Identifier

Q#	Variable Name	Variable ID	Values	Description
IF19	Primary source	IF_dsor	(1)Police; (2)Court; (3)Other Govnt; (4)Militia Watchdog; (5)ADL; (6)SPLC; (7)Other Watchdog Pub; (8)News-Journalist; (9)Scholarly Work; (10)Scholarly Database; (11)Nonscholarly Work; (12)Website; (13)Key Informant; (14)Other Source (-99)Missing	Using the assessment codebook, identify which data source is most prevalent. This source should be the most frequently occurring unless the majority of information stems from a prominent single source (e.g. indictment).
IF20	Case status	IF_stat	(1)closed; (2)open; (-99)Missing	Is this case open or closed?
IF21	Status description	IF_statd	String	If case is still open, please explain why (i.e. suspect waiting for trial or appeal)
IF22	Last updated?	IF_updated	MM/DD/YY	Last date database was modified

Q#	Variable Name	Variable ID	Values	Description
IF23	Scheme type	IF_scheme	(1)Pyramid scheme (2)Ponzi scheme (3)Other investment scheme (4)Advanced fee scheme (5)“Nigerian letter” scam (6)Other telemarketing scheme (7)ID theft/fraud scheme (8)Other Internet-based scheme (9)Tax avoidance/refusal (10)Money-laundering scheme (11)Money-dirtying scheme (12)Other scheme	What type of scheme? Refer to scheme typology in this codebook
IF24	If other, specify	IF_scheme2	String	If no existing scheme type is identified, describe scheme
IF25	Relevance of scheme	IF_reliv	(1)Incident ideological (2)Preparatory crime (3)General terrorism financing (4)Other criminal activity movement related (5)Other criminal activity non-movement related	Relevance of scheme . Examples: (1) incident ideological = tax refusal for pure ideological purposes; (2) preparatory crime = scheme to finance a specific terrorist mission; (3) general terrorism financing = scheme to support terrorist group, no reference to specific incident; (4) other crime but movement related = mixed ideological/profit motive (5) other crime non-movement related = pure profit-oriented scheme.

Q#	Variable Name	Variable ID	Values	Description
IF26	Primary categorization	IF_pissue	(1)anti-global (2)anti-federal government (3)anti-lower level of government (4)anti-immigration (5)anti-tax (6)gun related (7)land use related (8)farming related (9)environmental related (10)anti-leftist and other ideological enemies (11)pro global jihad (anti-West in general) (12)pro global jihad (anti-US) (13)pro local jihad (14)non-ideological/profit (15)non-ideological/instrumental to predicate crime	Primary categorization of scheme
IF27	Secondary categorization	IF_pisue2	String	List all other categorizations, if any
IF28	Motive	IF_motinc	String	Explain motive(s) for scheme
IF29	Isolated or linked	IF_typinc	(1)Isolated (2)Linked to financial scheme (3)Linked to non-financial incident (4)Linked to financial and non-financial incidents	Is this scheme isolated or linked to other schemes or incidents?

Q#	Variable Name	Variable ID	Values	Description
IF30	If linked, how?	IF_linked	String	Describe how schemes/incidents are linked (e.g. primary scheme involves laundering money to fund terrorist attack)
IF31	# related schemes/incidents	IF_totinc	Numeric	Number of related schemes/incidents, excluding current
IF32	Related scheme/incident IDs	IF_otrein	String	List related schemes/incidents IDs
IF33	Indictment ID	IF_indictid	String	Criminal Indictment ID number
IF34	Legal category	IF_legcat	(1)Incident (2)Attempt (3)Conspiracy (4)Suspected	Legal categorization
IF35	Mail fraud	IF_mail	(0)No; (1)Yes; (-99)Missing	Did the scheme involve mail fraud?
IF36	# Counts	IF_mail2	Numeric	If yes, how many counts?
IF37	USC provisions	IF_mail3	String	List all criminal provisions from the U.S. Criminal Code, if known
IF38	Wire fraud	IF_wire	(0)No; (1)Yes; (-99)Missing	Did the scheme involve wire fraud?
IF39	# counts	IF_wire2	Numeric	If yes, how many counts?

Q#	Variable Name	Variable ID	Values	Description
IF40	USC provisions	IF_wire3	String	List all criminal provisions from the U.S. Criminal Code, if known
IF41	Investment fraud	IF_invest	(0)No; (1)Yes; (-99)Missing	Did the scheme involve investment fraud?
IF42	# counts	IF_invest2	Numeric	If yes, how many counts?
IF43	USC provisions	IF_invest3	String	List all criminal provisions from the U.S. Criminal Code, if known
IF44	Securities fraud	IF_secure	(0)No; (1)Yes; (-99)Missing	Did the scheme involve securities and commodities fraud?
IF45	# counts	IF_secure2	Numeric	If yes, how many counts?
IF46	USC provisions	IF_secure3	String	List all criminal provisions from the U.S. Criminal Code, if known
IF47	Identity theft	IF_ident	(0)No; (1)Yes; (-99)Missing	Did the scheme involve identity theft?
IF48	# counts	IF_ident2	Numeric	If yes, how many counts?
IF49	USC provisions	IF_ident3	String	List all criminal provisions from the U.S. Criminal Code, if known

Q#	Variable Name	Variable ID	Values	Description
IF50	Credit card fraud	IF_credit	(0)No; (1)Yes; (-99)Missing	Did the scheme involve credit card fraud?
IF51	# counts	IF_credit2	Numeric	If yes, how many counts?
IF52	USC provisions	IF_credit3	String	List all criminal provisions from the U.S. Criminal Code, if known
IF53	Insurance fraud	IF_insur	(0)No; (1)Yes; (-99)Missing	Did the scheme involve insurance fraud?
IF54	# counts	IF_insur2	Numeric	If yes, how many counts?
IF55	USC provisions	IF_insur3	String	List all criminal provisions from the U.S. Criminal Code, if known
IF56	Bank fraud	IF_bank	(0)No; (1)Yes; (-99)Missing	Did the scheme involve bank fraud?
IF57	# counts	IF_bank2	Numeric	If yes, how many counts?
IF58	USC provisions	IF_bank3	String	List all criminal provisions from the U.S. Criminal Code, if known
IF59	Money laundering	IF_money	(0)No; (1)Yes; (-99)Missing	Did the scheme involve money laundering?
IF60	# counts	IF_money2	Numeric	If yes, how many counts?

Q#	Variable Name	Variable ID	Values	Description
IF61	USC provisions	IF_money3	String	List all criminal provisions from the U.S. Criminal Code, if known
IF62	Tax fraud	IF_tax	(0)No; (1)Yes; (-99)Missing	Did the scheme involve tax fraud?
IF63	# counts	IF_tax2	Numeric	If yes, how many counts?
IF64	USC provisions	IF_tax3	String	List all criminal provisions from the U.S. Criminal Code, if known
IF65	Failure to file tax return	IF_failure	(0)No; (1)Yes; (-99)Missing	Did the scheme involve a failure to file an income tax return?
IF66	# counts	IF_failure2	Numeric	If yes, how many counts?
IF67	USC provisions	IF_failure3	String	List all criminal provisions from the U.S. Criminal Code, if known
IF68	Other financial	IF_othfin	(0)No; (1)Yes; (-99)Missing	Did the scheme involve any other type of financial fraud?
IF69	If yes, specify	IF_othfin1	String	If yes, specify
IF70	# counts	IF_othfin2	Numeric	If yes, how many counts?
IF71	USC provisions	IF_othfin3	String	List all criminal provisions from the U.S. Criminal Code, if known

Q#	Variable Name	Variable ID	Values	Description
IF72	Immigration fraud	IF_immig	(0)No; (1)Yes; (-99)Missing	Did the scheme involve immigration fraud?
IF73	# counts	IF_immig2	Numeric	If yes, how many counts?
IF74	USC provisions	IF_immig3	String	List all criminal provisions from the U.S. Criminal Code, if known
IF75	Computer crime	IF_comp	(0)No; (1)Yes; (-99)Missing	Did the scheme involve a computer crime?
IF76	# counts	IF_comp2	Numeric	If yes, how many counts?
IF77	USC provisions	IF_comp3	String	List all criminal provisions from the U.S. Criminal Code, if known
IF78	Support FTO	IF_fto	(0)No; (1)Yes; (-99)Missing	Did the scheme provide material support to a foreign terrorist organization?
IF79	If yes, which FTO	IF_fto2	String	If yes, which designated foreign terrorist organization (FTO)?
IF80	# counts	IF_fto3	Numeric	If yes, how many counts?
IF81	USC provisions	IF_fto4	String	List all criminal provisions from the U.S. Criminal Code, if known

Q#	Variable Name	Variable ID	Values	Description
IF82	Supports terrorists	IF_matsupp	(0)No; (1)Yes; (-99)Missing	Did the scheme involve providing material support to terrorists?
IF83	# counts	IF_matsupp2	Numeric	If yes, how many counts?
IF84	USC provisions	IF_matsupp3	String	List all criminal provisions from the U.S. Criminal Code, if known
IF85	RICO conspiracy	IF_intelprop	(0)No; (1)Yes; (-99)Missing	Did the scheme involve a RICO conspiracy?
IF86	# counts	IF_intelprop2	Numeric	If yes, how many counts?
IF87	USC provisions	IF_intelprop3	String	List all criminal provisions from the U.S. Criminal Code, if known
IF88	Other non-financial	IF_nonfin	(0)No; (1)Yes; (-99)Missing	Did the scheme involve immigration fraud?
IF89	# counts	IF_nonfin2	Numeric	If yes, how many counts?
IF90	USC provisions	IF_nonfin3	String	List all criminal provisions from the U.S. Criminal Code, if known
IF91	# Deaths	IF_totdth	Numeric	Number of deaths
IF92	# Deaths w/ suspects	IF_dthprp	Numeric	Number of deaths including suspects
IF93	# Suicides	IF_suicide	Numeric	Number of suicides

Q#	Variable Name	Variable ID	Values	Description
IF94	# Suicides w/ suspects	IF_suicsusp	Numeric	Number of suicides including suspects
IF95	Government loss	IF_govloss	(1)Minor (2)Moderate (3)Substantial (4)Very substantial	Estimated government/societal loss
IF96	Min amount	IF_govmin	Numeric	Minimum amount of government loss, if known
IF97	Max amount	IF_govmax	Numeric	Maximum amount of government loss, if known
IF98	Victim loss	IF_victloss	(1)Minor (2)Moderate (3)Substantial (4)Very substantial	Estimated victim loss
IF99	Amount	IF_victamnt	Numeric	Specific amount of victim loss, if known
IF100	Illicit revenue	IF_illpro	(1)Minor (2)Moderate (3)Substantial (4)Very substantial	Estimated illicit revenue/profits
IF101	Amount	IF_illpro2	Numeric	Specific amount of illicit revenue/profits, if known
IF102	Civil injunction	IF_cvlinj	(0)No; (1)Yes; (-99)Missing	Did criminal investigations start with a civil injunction against suspects?

Q#	Variable Name	Variable ID	Values	Description
IF103	If yes, explain	IF_cvlinj2	String	If yes, explain how
IF104	Civil action	IF_cjcvl	(1)No civil action taken (2)"Civil action taken by government (injunction, civil suits, etc)" (3)Civil action by watch-group (4)Civil action by victim (5)Civil action by other private party	Was civil action taken against the suspects?
IF105	Investigative agency	IF_agency	String	Investigative agency
IF106	Investigative agency 2	IF_agency2	String	Investigative agency 2
IF107	Investigative agency 3	IF_agency3	String	Investigative agency 3
IF108	District code	IF_district	String	Prosecuting U.S. Attorney district code
IF109	Court type	IF_fedsta	(1)Bankruptcy (2)Court of appeals (3)U.S. district court (4)U.S. supreme court (5)State court	Federal or state court?
IF110	If federal, specify	IF_court	String	If federal court, list court
IF111	If state, specify	IF_court2	String	If state court, list county and prosecutor

Q#	Variable Name	Variable ID	Values	Description
IF112	Foreign cooperation	IF_forauth	(0)No; (1)Yes; (-99)Missing	Did foreign agencies cooperate with investigative and/or prosecuting authorities?
IF113	Foreign agencies	IF_forauth2	String	List foreign agencies, if any
IF114	Total number of suspects	IF_persus	Numeric	Total number of suspects
IF115	Far-right suspects	IF_frsus	Numeric	Far-right suspects
IF116	Far-left suspects	IF_flsus	Numeric	Far-left suspects
IF117	ALF/ELF suspects	IF_alfsus	Numeric	ALF/ELF suspects
IF118	Global jihad suspects	IF_gjsus	Numeric	Global jihad suspects
IF119	Local jihad suspects	IF_ljsus	Numeric	Local jihad suspects
IF120	Secular Arab suspects	IF_secsus	Numeric	Secular Arab suspects
IF121	Other suspects	IF_othsus	Numeric	Other suspects
IF122	If other, specify	IF_othsus2	String	If other, specify
IF123	Total number arrested	IF_perarr	Numeric	Total number arrested
IF124	Far-right arrested	IF_frarr	Numeric	Far-right arrested
IF125	Far-left arrested	IF_flarr	Numeric	Far-left arrested
IF126	ALF/ELF arrested	IF_alfarr	Numeric	ALF/ELF arrested
IF127	Global jihad arrested	IF_gjarr	Numeric	Global jihad arrested

Q#	Variable Name	Variable ID	Values	Description
IF128	Local jihad arrested	IF_ljarr	Numeric	Local jihad arrested
IF129	Secular Arab arrested	IF_secarr	Numeric	Secular Arab arrested
IF130	Other arrested	IF_otharr	Numeric	Other arrested
IF131	If other, specify	IF_otharr2	String	If other, specify
IF132	Total number indicted	IF_perind	Numeric	Total number indicted
IF133	Far-right indicted	IF_frind	Numeric	Far-right indicted
IF134	Far-left indicted	IF_flind	Numeric	Far-left indicted
IF135	ALF/ELF indicted	IF_alfind	Numeric	ALF/ELF indicted
IF136	Global jihad indicted	IF_gjind	Numeric	Global jihad indicted
IF137	Local jihad indicted	IF_ljind	Numeric	Local jihad indicted
IF138	Secular Arab indicted	IF_secind	Numeric	Secular Arab indicted
IF139	Other indicted	IF_othind	Numeric	Other indicted
IF140	If other, specify	IF_othind2	String	If other, specify
IF141	Total number pled guilty	IF_perplg	Numeric	Total number pled guilty
IF142	Far-right pled guilty	IF_frplg	Numeric	Far-right pled guilty
IF143	Far-left pled guilty	IF_flplg	Numeric	Far-left pled guilty
IF144	ALF/ELF pled guilty	IF_alfplg	Numeric	ALF/ELF pled guilty

Q#	Variable Name	Variable ID	Values	Description
IF145	Global jihad pled guilty	IF_gjplg	Numeric	Global jihad pled guilty
IF146	Local jihad pled guilty	IF_ljplg	Numeric	Local jihad pled guilty
IF147	Secular Arab pled guilty	IF_secplg	Numeric	Secular Arab pled guilty
IF148	Other pled guilty	IF_othplg	Numeric	Other pled guilty
IF149	If other, specify	IF_othplg2	String	If other, specify
IF150	Total number pled not guilty	IF_perpng	Numeric	Total number pled not guilty
IF151	Far-right pled not guilty	IF_frng	Numeric	Far-right pled not guilty
IF152	Far-left pled not guilty	IF_flng	Numeric	Far-left pled not guilty
IF153	ALF/ELF pled not guilty	IF_alfng	Numeric	ALF/ELF pled not guilty
IF154	Global jihad pled not guilty	IF_gjng	Numeric	Global jihad pled not guilty
IF155	Local jihad pled not guilty	IF_ljng	Numeric	Local jihad pled not guilty
IF156	Secular Arab pled not guilty	IF_secng	Numeric	Secular Arab pled not guilty
IF157	Other pled not guilty	IF_othng	Numeric	Other pled not guilty
IF158	If other, specify	IF_othng2	String	If other, specify
IF159	Total number NGRI	IF_perpngri	Numeric	Total number NGRI
IF160	Far-right NGRI	IF_frngri	Numeric	Far-right NGRI
IF161	Far-left NGRI	IF_flngri	Numeric	Far-left NGRI

Q#	Variable Name	Variable ID	Values	Description
IF162	ALF/ELF NGRI	IF_alfngri	Numeric	ALF/ELF NGRI
IF163	Global jihad NGRI	IF_gjngri	Numeric	Global jihad NGRI
IF164	Local jihad NGRI	IF_ljngri	Numeric	Local jihad NGRI
IF165	Secular Arab NGRI	IF_secngri	Numeric	Secular Arab NGRI
IF166	Other NGRI	IF_othngri	Numeric	Other NGRI
IF167	If other, specify	IF_othngri2	String	If other, specify
IF168	Total number convicted	IF_perpconv	Numeric	Total number convicted
IF169	Far-right convicted	IF_frconv	Numeric	Far-right convicted
IF170	Far-left convicted	IF_flconv	Numeric	Far-left convicted
IF171	ALF/ELF convicted	IF_alfconv	Numeric	ALF/ELF convicted
IF172	Global jihad convicted	IF_gjconv	Numeric	Global jihad convicted
IF173	Local jihad convicted	IF_ljconv	Numeric	Local jihad convicted
IF174	Secular Arab convicted	IF_secconv	Numeric	Secular Arab convicted
IF175	Other convicted	IF_othconv	Numeric	Other convicted
IF176	If other, specify	IF_othconv2	String	If other, specify
IF177	Total number nondecisions	IF_perpnd	Numeric	Total number non decisions
IF178	Far-right nondecisions	IF_frnd	Numeric	Far-right non decisions

Q#	Variable Name	Variable ID	Values	Description
IF179	Far-left nondecisions	IF_flnd	Numeric	Far-left non decisions
IF180	ALF/ELF nondecisions	IF_alfnd	Numeric	ALF/ELF non decisions
IF181	Global jihad nondecisions	IF_gjnd	Numeric	Global jihad non decisions
IF182	Local jihad nondecisions	IF_ljnd	Numeric	Local jihad non decisions
IF183	Secular Arab nondecisions	IF_secnd	Numeric	Secular Arab non decisions
IF184	Other nondecisions	IF_othnd	Numeric	Other nondecisions
IF185	If other, specify	IF_othnd2	String	If other, specify
IF186	Total number retrial	IF_perprt	Numeric	Total number retrial
IF187	Far-right retrial	IF_frrt	Numeric	Far-right retrial
IF188	Far-left retrial	IF_flrt	Numeric	Far-left retrial
IF189	ALF/ELF retrial	IF_alfrt	Numeric	ALF/ELF retrial
IF190	Global jihad retrial	IF_gjrt	Numeric	Global jihad retrial
IF191	Local jihad retrial	IF_ljrt	Numeric	Local jihad retrial
IF192	Secular Arab retrial	IF_secrt	Numeric	Secular Arab retrial
IF193	Other retrial	IF_othrt	Numeric	Other retrial
IF194	If other, specify	IF_othrt2	String	If other, specify
IF195	Total number of appeals	IF_perpapp	Numeric	Total number of appeals

Q#	Variable Name	Variable ID	Values	Description
IF196	Far-right appeals	IF_frpapp	Numeric	Far-right appeals
IF197	Far-left appeals	IF_flapp	Numeric	Far-left appeals
IF198	ALF/ELF appeals	IF_alfapp	Numeric	ALF/ELF appeals
IF199	Global jihad appeals	IF_gjapp	Numeric	Global jihad appeals
IF200	Local jihad appeals	IF_ljapp	Numeric	Local jihad appeals
IF201	Secular Arab appeals	IF_secapp	Numeric	Secular Arab appeals
IF202	Other appeals	IF_othapp	Numeric	Other appeals
IF203	If other, specify	IF_othapp2	String	If other, specify
IF204	Total number community corrections	IF_perpcorr	Numeric	Total number community corrections
IF205	Far-right community corrections	IF_frcorr	Numeric	Far-right community corrections
IF206	Far-left community corrections	IF_flcorr	Numeric	Far-left community corrections
IF207	ALF/ELF community corrections	IF_alfcorr	Numeric	ALF/ELF community corrections
IF208	Global jihad community corrections	IF_gjcorr	Numeric	Global jihad community corrections
IF209	Local jihad community corrections	IF_ljcorr	Numeric	Local jihad community corrections
IF210	Secular Arab community	IF_seccorr	Numeric	Secular Arab community corrections

Q#	Variable Name	Variable ID	Values	Description
	corrections			
IF211	Other community corrections	IF_othcorr	Numeric	Other community corrections
IF212	If other, specify	IF_othcorr2	String	If other, specify
IF213	Total number in prison	IF_perppri	Numeric	Total number in prison
IF214	Far-right prison	IF_frpri	Numeric	Far-right prison
IF215	Far-left prison	IF_flpri	Numeric	Far-left prison
IF216	ALF/ELF prison	IF_alfpri	Numeric	ALF/ELF prison
IF217	Global jihad prison	IF_gjpri	Numeric	Global jihad prison
IF218	Local jihad prison	IF_ljpri	Numeric	Local jihad prison
IF219	Secular Arab prison	IF_secpri	Numeric	Secular Arab prison
IF220	Other prison	IF_othpri	Numeric	Other prison
IF221	If other, specify	IF_othpri2	String	If other, specify
IF222	Total number sentenced to death	IF_perpdth	Numeric	Total number sentenced to death
IF223	Far-right sentenced to death	IF_frdth	Numeric	Far-right sentenced to death
IF224	Far-left sentenced to death	IF_fldth	Numeric	Far-left sentenced to death
IF225	ALF/ELF sentenced to death	IF_alfdth	Numeric	ALF/ELF sentenced to death

Q#	Variable Name	Variable ID	Values	Description
IF226	Global jihad sentenced to death	IF_gjdth	Numeric	Global jihad sentenced to death
IF227	Local jihad sentenced to death	IF_ljdth	Numeric	Local jihad sentenced to death
IF228	Secular Arab sentenced to death	IF_secdth	Numeric	Secular Arab sentenced to death
IF229	Other sentenced to death	IF_othdth	Numeric	Other sentenced to death
IF230	If other, specify	IF_othdth2	String	If other, specify
IF231	Total number executed	IF_perpex	Numeric	Total number executed
IF232	Far-right executed	IF_frex	Numeric	Far-right executed
IF233	Far-left executed	IF_flex	Numeric	Far-left executed
IF234	ALF/ELF executed	IF_alfex	Numeric	ALF/ELF executed
IF235	Global jihad executed	IF_gjex	Numeric	Global jihad executed
IF236	Local jihad executed	IF_ljex	Numeric	Local jihad executed
IF237	Secular Arab executed	IF_secex	Numeric	Secular Arab executed
IF238	Other executed	IF_othex	Numeric	Other executed
IF239	If other, specify	IF_othex2	String	If other, specify
IF240	Total number served time and freed	IF_perpstf	Numeric	Total number served time and freed
IF241	Far-right served time and	IF_frstf	Numeric	Far-right served time and freed

Q#	Variable Name	Variable ID	Values	Description
	freed			
IF242	Far-left served time and freed	IF_flstf	Numeric	Far-left served time and freed
IF243	ALF/ELF served time and freed	IF_alfstf	Numeric	ALF/ELF served time and freed
IF244	Global jihad served time and freed	IF_gjstf	Numeric	Global jihad served time and freed
IF245	Local jihad served time and freed	IF_ljstf	Numeric	Local jihad served time and freed
IF246	Secular Arab served time and freed	IF_secstf	Numeric	Secular Arab served time and freed
IF247	Other served time and freed	IF_othstf	Numeric	Other served time and freed
IF248	If other, specify	IF_othstf2	String	If other, specify
IF249	Scheme ideology ID	SI_ID	Numeric	Scheme ID
IF250	Strength ideological motivation	SI_bond	(0)0 (1)1 (2)2 (3)3 (4)4	How strong was the ideological motivation to the commission of the scheme (1 lowest, 4 highest)?
IF251	Pro evidence 1	SI_proevid1	String	Evidence supporting ideological motivation
IF252	Pro source 1	SI_prosrc1	String	Source of evidence

Q#	Variable Name	Variable ID	Values	Description
IF253	Pro evidence 2	SI_proevid2	String	Evidence supporting ideological motivation
IF254	Pro source 2	SI_prosrc2	String	Source of evidence
IF255	Pro evidence 3	SI_proevid3	String	Evidence supporting ideological motivation
IF256	Pro source 3	SI_prosrc3	String	Source of evidence
IF257	Pro evidence 4	SI_proevid4	String	Evidence supporting ideological motivation
IF258	Pro source 4	SI_prosrc4	String	Source of evidence
IF259	Pro evidence 5	SI_proevid5	String	Evidence supporting ideological motivation
IF260	Pro source 5	SI_prosrc5	String	Source of evidence
IF261	Con evidence 1	SI_conevid1	String	Evidence contradicting ideological motivation
IF262	Con source 1	SI_consrc1	String	Source of evidence
IF263	Con evidence 2	SI_conevid2	String	Evidence contradicting ideological motivation
IF264	Con source 2	SI_consrc2	String	Source of evidence
IF265	Con evidence 3	SI_conevid3	String	Evidence contradicting ideological motivation
IF266	Con source 3	SI_consrc3	String	Source of evidence

Q#	Variable Name	Variable ID	Values	Description
IF267	Con evidence 4	SI_conevid4	String	Evidence contradicting ideological motivation
IF268	Con source 4	SI_consrc4	String	Source of evidence
IF269	Con evidence 5	SI_conevid5	String	Evidence contradicting ideological motivation
IF270	Con source 5	SI_consrc5	String	Source of evidence
	Scheme location ID	IF_ID_Country	Numeric	Relational ID (Scheme ID + Masterfile ID)
	Scheme in Afghanistan	IF_Afghanistan	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Albania	IF_Albania	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Algeria	IF_Algeria	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Andorra	IF_Andorra	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Angola	IF_Angola	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Antigua Barbuda	IF_AntiguaBarbuda	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Argentina	IF_Argentina	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Armenia	IF_Armenia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Aruba	IF_Aruba	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Australia	IF_Australia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Austria	IF_Austria	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Azerbaijan	IF_Azerbaijan	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Bahamas	IF_Bahamas	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Bahrain	IF_Bahrain	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Bangladesh	IF_Bangladesh	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Barbados	IF_Barbados	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Belarus	IF_Belarus	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Belgium	IF_Belgium	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Belize	IF_Belize	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Benin	IF_Benin	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Bermuda	IF_Bermuda	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Bhutan	IF_Bhutan	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Bolivia	IF_Bolivia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Bosnia-Herzegovina	IF_BosniaHerzegovina	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Botswana	IF_Botswana	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Brazil	IF_Brazil	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in British Virgin Islands	IF_BritishVirginIslands	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Brunei Darussalam	IF_BrueneiDarussalam	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Bulgaria	IF_Bulgaria	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Burkina Faso	IF_BurkinaFaso	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Burundi	IF_Burundi	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Cambodia	IF_Cambodia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Cameroon	IF_Cameroon	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Canada	IF_Canada	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Cape Verde	IF_CapeVerde	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Cayman Islands	IF_CaymanIslands	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Central African Republic	IF_CentralAfricanRepublic	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Chad	IF_Chad	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Chile	IF_Chile	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in China	IF_China	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Colombia	IF_Colombia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Comoros	IF_Comoros	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Congo	IF_Congo	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Costa Rica	IF_CostaRica	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Cote D'Ivoire	IF_CoteDIvoire	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Croatia	IF_Croatia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Cuba	IF_Cuba	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Cyprus	IF_Cyprus	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Czech Republic	IF_CzechRepublic	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Democratic Republic of Congo	IF_DRCongo	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Denmark	IF_Denmark	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Djibouti	IF_Djibouti	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Dominica	IF_Dominica	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Dominican Republic	IF_DominicanRepublic	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in East Timor	IF_EastTimor	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Ecuador	IF_Ecuador	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Egypt	IF_Egypt	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in El Salvador	IF_ElSalvador	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Equatorial Guinea	IF_EquatorialGuinea	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Eritrea	IF_Eritrea	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Estonia	IF_Estonia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Ethiopia	IF_Ethiopia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Fiji	IF_Fiji	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Finland	IF_Finland	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in France	IF_France	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Gabon	IF_Gabon	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Gambia	IF_Gambia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Georgia	IF_Georgia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Germany	IF_Germany	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Ghana	IF_Ghana	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Greece	IF_Greece	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Grenada	IF_Grenada	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Guatemala	IF_Guatemala	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Guinea	IF_Guinea	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Guinea Bissau	IF_GuineaBissau	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Guyana	IF_Guyana	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Haiti	IF_Haiti	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Honduras	IF_Honduras	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Hungary	IF_Hungary	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Iceland	IF_Iceland	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in India	IF_India	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Indonesia	IF_Indonesia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Iran	IF_Iran	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Iraq	IF_Iraq	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Ireland	IF_Ireland	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Isle of Man	IF_IsleofMan	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Israel	IF_Israel	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Italy	IF_Italy	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Jamaica	IF_Jamaica	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Japan	IF_Japan	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Jordan	IF_Jordan	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Kazakhstan	IF_Kazakstan	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Kenya	IF_Kenya	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Kiribati	IF_Kiribati	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in North Korea	IF_KoreaNorth	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in South Korea	IF_KoreaSouth	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Kuwait	IF_Kuwait	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Kyrgyzstan	IF_Kyrgyzstan	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Laos	IF_Laos	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Latvia	IF_Latvia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Lebanon	IF_Lebanon	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Lesotho	IF_Lesotho	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Liberia	IF_Liberia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Libya	IF_Libya	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Liechtenstein	IF_Liechtenstein	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Lithuania	IF_Lithuania	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Luxembourg	IF_Luxembourg	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Macedonia	IF_Macedonia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Madagascar	IF_Madagascar	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Malawi	IF_Malawi	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Malaysia	IF_Malaysia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Maldives	IF_Maldives	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Mali	IF_Mali	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Malta	IF_Malta	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Marshall Islands	IF_Marshall Islands	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Mauritania	IF_Mauritania	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Mauritius	IF_Mauritius	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Mexico	IF_Mexico	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Micronesia	IF_Micronesia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Moldova	IF_Moldova	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Monaco	IF_Monaco	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Mongolia	IF_Mongolia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Montenegro	IF_Montenegro	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Morocco	IF_Morocco	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Mozambique	IF_Mozambique	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Myanmar	IF_Myanmar	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Namibia	IF_Namibia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Nauru	IF_Nauru	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Nepal	IF_Nepal	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Netherlands	IF_Netherlands	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Netherlands Antilles	IF_NetherlandsAntilles	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in New Zealand	IF_NewZealand	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Nicaragua	IF_Nicaragua	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Niger	IF_Niger	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Nigeria	IF_Nigeria	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Norway	IF_Norway	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Oman	IF_Oman	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Pakistan	IF_Pakistan	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Palau	IF_Palau	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Palestine	IF_Palestiine	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Panama	IF_Panama	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Papua New Guinea	IF_PapuaNewGuinea	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Paraguay	IF_Paraguay	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Peru	IF_Peru	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Philippines	IF_Philippines	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Poland	IF_Poland	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Portugal	IF_Portugal	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Puerto Rico	IF_PuertoRico	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Qatar	IF_Qatar	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Romania	IF_Romania	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Russian Federation	IF_RussianFederation	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Rwanda	IF_Rwanda	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in St. Kitts Nevis	IF_StKittsNevis	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Saint Lucia	IF_SaintLucia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Saint Vincent	IF_SaintVincent	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Samoa	IF_Samoa	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in San Marino	IF_SanMarino	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Sao Tome Principe	IF_SaoTomePrincipe	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Saudi Arabia	IF_SaudiArabia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Senegal	IF_Senegal	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Seychelles	IF_Seychelles	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Sierra Leone	IF_SierraLeone	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Singapore	IF_Singapore	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Slovakia	IF_Slovakia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Slovenia	IF_Slovenia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Solomon Islands	IF_SolomonIslands	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Somalia	IF_Somalia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in South Africa	IF_SouthAfrica	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Spain	IF_Spain	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Sri Lanka	IF_SriLanka	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Sudan	IF_Sudan	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Suriname	IF_Suriname	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Swaziland	IF_Swaziland	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Sweden	IF_Sweden	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Switzerland	IF_Switzerland	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Syria	IF_Syria	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Taiwan	IF_Taiwan	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Tajikistan	IF_Tajikistan	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Tanzania	IF_Tanzania	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Thailand	IF_Thailand	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Togo	IF_Togo	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Tonga	IF_Tonga	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Trinidad Tobago	IF_TrinidadTobago	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Tunisia	IF_Tunisia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Turkey	IF_Turkey	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Turkmenistan	IF_Turkmenistan	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Tuvalu	IF_Tuvalu	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Uganda	IF_Uganda	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Ukraine	IF_Ukraine	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in United Arab Emirates	IF_UnitedArabEmirates	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in United Kingdom	IF_UnitedKingdom	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in US Virgin Islands	IF_USVirginIslands	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Uruguay	IF_Uruguay	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Uzbekistan	IF_Uzbekistan	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Vanuatu	IF_Vanuatu	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Vatican City	IF_VaticanCity	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Venezuela	IF_Venezuela	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Vietnam	IF_Vietnam	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Yemen	IF_Yemen	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Yugoslavia	IF_Yugoslavia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Zambia	IF_Zambia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Zimbabwe	IF_Zimbabwe	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this country?
	Scheme in Alabama	IF_Alabama	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Alaska	IF_Alaska	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Arizona	IF_Arizona	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Arkansas	IF_Arkansas	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in California	IF_California	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Colorado	IF_Colorado	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Connecticut	IF_Connecticut	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Delaware	IF_Delaware	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in District of Columbia	IF_DistrictofColumbia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Florida	IF_Florida	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Georgia	IF_Georgia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Hawaii	IF_Hawaii	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Idaho	IF_Idaho	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Illinois	IF_Illinois	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Indiana	IF_Indiana	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Iowa	IF_Iowa	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Kansas	IF_Kansas	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Kentucky	IF_Kentucky	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Louisiana	IF_Lousiana	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Maine	IF_Maine	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Maryland	IF_Maryland	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Massachusetts	IF_Massachusetts	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Michigan	IF_Michigan	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Minnesota	IF_Minnesota	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Mississippi	IF_Mississipi	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Missouri	IF_Missouri	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Montana	IF_Montana	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in Nebraska	IF_Nebraska	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Nevada	IF_Nevada	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in New Hampshire	IF_NewHampshire	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in New Jersey	IF_NewJersey	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in New Mexico	IF_NewMexico	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in New York	IF_NewYork	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in North Carolina	IF_NorthCarolina	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in North Dakota	IF_NorthDakota	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Ohio	IF_Ohio	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Oklahoma	IF_Oklahoma	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Oregon	IF_Oregon	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Pennsylvania	IF_Pennsylvania	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Rhode Island	IF_RhodeIsland	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in South Carolina	IF_SouthCarolina	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in South Dakota	IF_SouthDakota	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Tennessee	IF_Tennessee	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Texas	IF_Texas	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Utah	IF_Utah	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Vermont	IF_Vermont	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Virginia	IF_Virginia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Washington	IF_Washington	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?

Q#	Variable Name	Variable ID	Values	Description
	Scheme in West Virginia	IF_WestVirginia	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Wisconsin	IF_Wisconsin	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?
	Scheme in Wyoming	IF_Wyoming	(0)No; (1)Yes; (-99)Missing	Did the financial scheme take place in this state?

Financial - Suspect Codebook: Coding Issues

NOTE: This document should be in front of the coder as they code. If an assigned suspect does not meet the inclusion criteria it is NOT to be coded & the suspect should be sent back to the PIs for further review.

(1) INCLUSION CRITERIA – WHO IS A SUSPECT?

A suspect is any individual who the open source information indicates:

(i) Participated at least in part in the scheme at issue & the scheme met our inclusion criteria above

(ii) was either a far-rightist, jihadi, secular Arab nationalist, or ELF/ALF extremist at the time of the scheme OR this is a prior or a subsequent scheme for a suspect that was involved in a scheme that met our criteria; or

(iii) is NOT far-rightist, jihadi, secular Arab nationalist or ELF/ALF extremist BUT was involved in a scheme where at least one of the other suspects was a far-right jihadi or ELF/ALF member/supporter.

(2) INCLUSION CRITERIA – The variable "WHY EXTREMIST" is very important.

Some schemes may involve different types of suspects, whose extremist affiliation is unclear (e.g. a person can be a racist without being a FR supporter). Thus, coders must be especially careful to specify whether the suspect is an extremist or not, and why. Coders must have our description/definitions of far-rightist, jihadist, Arab nationalist or animal/environmental rights extremist in front of them (**SEE PP. 124- 127**) and explain how the suspect FITS/MEETS this description/definition. In other words, we are trying to decide what the suspect's beliefs are. Thus, "words/quotes/ideas" from the suspect are quite useful.

A more complicated issue is what to make of "actions" by the suspect. Based upon their actions, can we make decisions about their beliefs? The answer is *it depends*:

- Membership in an ideological group is an "easy call." While not 100% full-proof, for our project's purposes, it is evidence of an extremist belief system.

- It becomes tricky, however, when we focus particularly on the crimes/actions of the suspects. Can we infer beliefs from this??? This is an important issue, because we need to think about the coding process.

  We code suspects if at the time of the crime they had an extremist belief system—the sequence is—(1) belief, (2) crime.

  HOWEVER, in some cases, it may be tempting to (1) look at the crime/act, (2) & based upon the crime infer a belief system, (3) which in turn allows us to code the crime. THIS could be CIRCULAR REASONING.

- Some examples of this are: (1) Hewitt's anti-abortion crimes, (2) some tax-refusal crimes or honor killings, (3) certain cases, like one coded by Belli where 2 suspects shot at FBI agents searching for Eric Rudolph, or (4) a heinous hate crime.

THUS THIS VARIABLE IS EXTREMELY IMPORTANT, CODERS MUST FULLY EXPLAIN HOW/WHY THE SUSPECT MEETS OUR EXTREMIST CRITERIA, & SPECIFIC STATEMENTS & ACTIONS SHOULD BE NOTED.

NOTE: Christopher Hewitt's "Political Violence and Terrorism in Modern America: A Chronology" 2005, New York: Praeger Security: PVII*): "Evidence of political or social motivation includes membership in an extremist organization or other links to extremist movements, such as possession of extremist literature. In addition, an individual's statements or writings may provide evidence of political or social motivation"*

FREILICH ADDS: Similarly, tattoos may also provide evidence of motivation.

(3) *SOCIAL NETWORKING TAB:* INCLUSION CRITERIA

In "Suspect 1" codebook, a section is devoted to collecting data on the suspects' social networks. Social network analysis examines patterns of relational ties among interdependent individuals (Wasserman and Faust, 1994). The *Social Networking* tab employs a so-called "ego-centric" design to identify and collect information on coded suspects (*egos*) and their ties with related individuals (*alters*). In other words, for each coded suspect, we collect information on any individual he/she associates with and the type(s) of relationship that bind them.

If a scheme involves multiple perpetrators, each person will be coded both as *ego* and *alter* (when focusing on links between pairs of coded suspects). In addition, we will also code as *alters* individuals who are not considered suspects according to our inclusion criteria, but belong to the suspect's social network based on a set of criteria.

An "*alter"* is any individual who the open source information indicates:

(i) Took part in the same financial scheme as the primary suspect (*ego*) OR in a related criminal incident which the suspect was also involved in regardless of whether the incident has already been coded or not (e.g., a conspiracy to assassinate the U.S. President).

(ii) Is directly connected to the suspect (*ego*) based on AT LEAST one of three possible types of relational ties, defined as follows:

(a) <u>Family tie</u>

- Q187 – "Immediate family" (e.g., spouse, parents, siblings, children, etc.)
- Q188 – "Non-immediate family" (e.g., cousins, aunts, uncles, etc.)

(b) <u>Criminal tie</u>

- Q189 – "Co-defendant" (e.g., persons prosecuted in same judicial case, aka *egos*)
- Q190 – "Co-suspect" (e.g., persons involved in same scheme but prosecuted in different judicial case, or involved in related criminal incident but not prosecuted, etc.)

(c) <u>Business tie</u>

- Q191 – "Business at time of scheme" (i.e., persons with whom *egos* engaged in legitimate business activities at the time when scheme was perpetrated, e.g. business partners, company's accountant, etc.)
- Q192 – "Business in the past" (i.e., persons with whom *egos* used to engage in legitimate business activities before scheme was perpetrated).

In addition to the mentioned criteria, coders must also determine whether or not the related person (*alter)* was a political extremist, and if so, what type (see Q186a-b). If the person is not an extremist, coders must determine what is the person's status (i.e. criminal, if *alter* was also prosecuted, or non criminal). Finally, it is important that coders indicate the primary and secondary sources that provided information on the relational ties between the coded *egos* and *alters*.

Q#	Variable Name	Variable ID	Values	Description
SF1	Suspect name	SF_Name	String	Suspect's full name, including aliases and nicknames
SF2	Suspect ID - Unique	SF_ID	Numeric	Suspect ID - Unique
SF3	Relational ID	SF_id3	Numeric	Relational ID (Scheme ID + Masterfile ID)
SF3-1	Suspect ID – Primary	SF_id4	Numeric	Suspect ID - Primary
	Note: SF2 must always be a different ID number. For example, if Tom Brown has three separate Suspect records because he was involved in three schemes, then SF2 in those three records might be 4001, 4002, 4003. S3-1 is based on Tom Brown's first suspect record. That is to say that for all three of the aforementioned schemes, Tom Brown's Suspect ID – Primary (S3-1) will be 4001. In addition, if a suspect in a violent incident is related to a financial incident, the Suspect ID –Primary must be the same across the violence and financial suspect codebooks.			
SF4	DOB day	SF_dobdy	Numeric	What day was suspect born?
SF4	DOB month	SF_dobmnth	Numeric	What month was suspect born?
SF4	DOB year	SF_dobyr	Numeric	What year was suspect born?
SF5	Gender	SF_Sex	(0)Female (1)Male	Suspect's gender

Q#	Variable Name	Variable ID	Values	Description
SF6	Race/Ethnicity	SF_Race	(1)White/Caucasian non-Hispanic; (2)Black/African American non-Hispanic; (3)Hispanic (any race); (4)Asian; (5)Arab; (6)Native American/American Indian; (7)Mixed; (8)Other	Suspect's race or ethnicity
SF7	Sexual orientation	SF_Sexor	(1)heterosexual; (2)homosexual; (3)bisexual	Suspect's sexual orientation
SF8	Alienage	SF_Aleg	(1)native born; (2)foreign born	Suspect's alienage
SF9	If foreign, specify	SF_Aleg2	String	If suspect was not born in the U.S., specify in what country
SF10	Citizenship	SF_citizen	String	If suspect is not a U.S. citizen at time of scheme, specify citizenship
SF11	County of birth	SF_CoBir2	String	Specify suspect's county of birth
SF12	State of birth	SF_StaB2	String	Specify suspect's state of birth
SF13	Address 1	SF_addrest1	String	Address 1 where suspect resided at time of scheme
SF14	Address 2	SF_addrest2	String	Address 2 where suspect resided

Q#	Variable Name	Variable ID	Values	Description
				at time of scheme
SF15	City of residence	SF_cityrest	String	City of residence at time of scheme
SF16	County of residence	SF_CoRest	String	County of residence at time of incident
SF17	State of residence	SF_Strest	String	State of residence at time of scheme
SF18	Zip code	SF_ziprest	Numeric	Zip code of residence at time of scheme
SF19	Foreign residence	SF_CoRest2	String	Country of residence at time of scheme (if other than U.S.)
SF20	Place of residence	SF_Prest	(1)urban; (2)suburban; (3)rural	Place of residence at time of scheme
SF21	Past states	SF_Strest2	String	Other states where suspect resided
SF22	Past countries	SF_country	String	Other countries where suspect resided

Q#	Variable Name	Variable ID	Values	Description
SF23	Religion	SF_Relig	(1)jewish; (2)catholic; (3)protestant/christian; (4)christian identity; (5)odinism; (6)National Alliance/Cosmotheism; (7)other cult; (8)world church of creator; (9)other racist faith; (10)islamic; (11)atheist/agnostic (12)other	Religion at time of scheme, if known
SF24	If other, specify	SF_Relg2	String	If other religion, specify
SF25	Religious intensity	SF_Rint	(1)low; (2)medium (3)high	Religious Intensity
SF26	Religious involvement	SF_Rinvol	(1)member of religious institution; (2)leadership position in religious institution; (3)other	Level of religious involvement
SF27	Preaches	SF_Prech	(0)No; (1)Yes; (-99)Missing	Does suspect preach?

Q#	Variable Name	Variable ID	Values	Description
SF28	Convert to Sunni Islam	SF_Convert1a	(0)No; (1)Yes; (-99)Missing	Did suspect convert to Sunni Islam?
SF29	Convert to Shiite Islam	SF_Convert1b	(0)No; (1)Yes; (-99)Missing	Did suspect convert to Shiite Islam?
SF30	Covert to other	SF_convert2	(0)No; (1)Yes; (-99)Missing	Did suspect convert to other religion?
SF31	If other, specify	SF_convert3	String	What religion did suspect convert to?
SF32	Marital status	SF_Marry	(1)married monogamous; (2)married polygamous; (3)single; (4)divorced (5)separated; (6)widow; (7)cohabitation; (8)boyfriend_girlfriend	Marital status
SF33	Children	SF_Child	(0)No; (1)Yes; (-99)Missing	Does suspect have children?
SF34	If yes, number	SF_child2	Numeric	Number of children, if applicable

Q#	Variable Name	Variable ID	Values	Description
SF35	Education	SF_Ed	(1)home schooled; (2)less than 8th grade; (3)completed 8th grade; (4)some hs; (5)ged; (6)hs diploma; (7)some college or vocational; (8)vocational graduate or associates degree; (9)college graduate; (10)post-graduate work	Suspect's highest level of education
SF36	Income	SF_incom	(1)low; (2)middle; (3)high; (4)0-5000; (5)5001-10000; (6)10001-15000; (7)15001-20000; (8)20001-30000; (9)30001-40000; (10)40001-50000; (11)50001-75000; (12)75001-100000; (13)100000-150000; (14)above 150000	Suspect's income

Q#	Variable Name	Variable ID	Values	Description
SF37	Community ties	SF_Comtie	(1)lived with spouse/children; (2)lived with parents/other family; (3)lived alone; (4)lived with non-family; (5)in custody serving sentence; (6)in temporary/pre-trial custody; (7)no stable residence	Suspect's community ties at time of scheme
SF38	Family background	SF_fambak	(1)parents married; (2)parents divorced; (3)parents separated; (4)mother died; (5)father died; (6)both parents died	Suspect's family background/history
SF39	Family involved	SF_faminv	(1)parents; (2)siblings; (3)spouse/partner; (4)children; (5)extended family; (6)multiple members; (7)no	Family involved in extremist movement (i.e. far-right, far-left, global jihad, local jihad, secular Arab nationalism)?
SF40	Community status	SF_Comstt	(0)low status/prestige; (1)high status/prestige	Suspect's community status

Q#	Variable Name	Variable ID	Values	Description
SF41	Occupation	SF_Occup	(1)agricultural; (2)transportation; (3)medical; (4)blue collar employee; (5)self-employed; (6)small business owner; (7)cj related; (8)private security; (9)religious; (10)cultural; (11)student; (12)government employee; (13)employed by some extremist movement; (14)unemployed; (15)retired; (16)accountant; (17)tax preparer; (18)financial advisor; (19)criminal attorney; (20)business attorney; (21)director; (22)CEO; (23)other white-collar; (24)other - specify	Suspect's occupation at time of scheme
SF42	If other, specify	SF_occup2	Sting	If other, specify

Q#	Variable Name	Variable ID	Values	Description
SF43	Military background	SF_Milt	(1)no; (2)yes-present; (3)yes-past	Does suspect have military background?
SF44	Branch of service	SF_mbrnch	(1)army; (2)navy; (3)air-force; (4)marine corps; (5)coast guard; (6)other/combined; (7)foreign military	Branch of service
SF45	Years in service	SF_mlen	Numeric	Length of years in service
SF46	Military training	SF_mtrain	String	Military training, specified
SF47	If yes, where	SF_mtrain2	String	If yes, where?
SF48	Saw combat	SF_mcom	(0)No; (1)Yes; (-99)Missing	Military combat?
SF49	Medals	SF_medal	(0)No; (1)Yes; (-99)Missing	Did suspect receive any awards or medals?
SF50	If yes, specify	SF_medals2	String	If yes, specify

Q#	Variable Name	Variable ID	Values	Description
SF51	Discharge	SF_mdis	(1)dishonor/deserted; (2)honorable; (3)other	Military discharge?
SF52	Law enforcement background	SF_lawen	(1)none; (2)federal-present; (3)federal-past; (4)state-present; (5)state-past; (6)local-present; (7)local-past	Does suspect have law enforcement background?
SF53	Alcohol/drug abuse	SF_alcsb	String	Is suspect alcohol or drug abuser?
SF54	If yes, specify	SF_alcsb2	String	If yes, specify alcohol or drugs
SF55	Mental illness	SF_mntlil	(0)No; (1)Yes; (-99)Missing	Does suspect have a documented history of mental illness?
SF56	Victimization	SF_victim	(0)No; (1)Yes; (-99)Missing	Has suspect ever been victimized?
SF57	If yes, specify	SF_victim2	String	If yes, explain
SF58	Last updated	SF_updated	MM/DD/YYYY	Last date database was modified
SF59	Other suspect codebooks	SF_orscb	String	Other related suspect codebooks

Q#	Variable Name	Variable ID	Values	Description
SF60	Suspect extremist	SF_polex	(0)No; (1)Yes; (-99)Missing	Was suspect a political extremist at time of scheme?
SF61	If yes, specify	SF_polex2	(1)Far-rightist; (2)ALF-ELF; (3)Global Jihadi; (4)Local Jihadi; (5)Non-religious/secular Arab nationalist; ((6)Other international terrorist	If political extremist, specify
SF62	Not extremist	SF_polex3	(1)White-collar offender; (2)Blue-collar offender; (3)Organized crime/drugs; (4)Organized crime/other; (5)Other status	If suspect is not a political extremist, what is suspect status?
SF63	If other, specify	SF_polex4	String	If none of the above, specify

Q#	Variable Name	Variable ID	Values	Description
SF64	Main belief	SF_belif	(1)Suspect believes whites are racially superior to all other races; (2)Suspect believes we are in or near the apocalypse; (3)Suspect claims to belong to an unrecognized or made up nation; (4)Suspect claims a willingness to die for freedom; (5)Suspect believes in conspiracy theories; (6)Suspect views figures as martyrs; (7)Suspect believes the country is nearing time of civil war; (8)Suspect has a hot-button issue; (9)Suspect used redemption; (10)Suspect supports global jihad; (11)Suspect supports local jihad; (12)Suspect supports animal rights extremism; (13)Suspect supports environmental rights extremism	Main belief system (1)
SF65	Additional beliefs	SF_belif2	String	List additional beliefs or beliefs not listed

Q#	Variable Name	Variable ID	Values	Description
SF66	Primary issue	SF_pissue	(1)anti-global; (2)anti-federal govnt; (3)anti lower level of govnt; (4)anti-immigration; (5)tax related; (6)gun related; (7)land use related; (8)farming related; (9)financial scheme/false lien; (10)environmental related; (11)abortion related; (12)anti-race general; (13)bi-racial; (14)anti-black; (15)anti-asian; (16)anti-hispanic; (17)anti-native american; (18)anti-jewish; (19)anti-arab; (20)anti-islamic; (21)anti-female; (22)anti-gay; (23)anti-pornography; (24)anti-leftist and other ideological enemies; (25)anti-sex offender; (26)anti-opponents within the movement; (27)anti-homeless; (28)pro-global Jihad (anti-West); (29)pro-global Jihad (anti-US); (30)pro-local Jihad; (31)other	Primary ideological issue of concern

Q#	Variable Name	Variable ID	Values	Description
SF67	Secondary issue	SF_pisue2	(1)anti-global; (2)anti-federal govnt; (3)anti lower level of govnt; (4)anti-immigration; (5)tax related; (6)gun related; (7)land use related; (8)farming related; (9)financial scheme/false lien; (10)environmental related; (11)abortion related; (12)anti-race general; (13)bi-racial; (14)anti-black; (15)anti-asian; (16)anti-hispanic; (17)anti-native american; (18)anti-jewish; (19)anti-arab; (20)anti-islamic; (21)anti-female; (22)anti-gay; (23)anti-pornography; (24)anti-leftist and other ideological enemies; (25)anti-sex offender; (26)anti-opponents within the movement; (27)anti-homeless; (28)pro-global Jihad (anti-West); (29)pro-global Jihad (anti-US); (30)pro-local Jihad; (31)other	List all other ideological issues of concern

Q#	Variable Name	Variable ID	Values	Description
SF68	Main affiliation	SF_maing	(1)KKK; (2)skinhead; (3)white supremacist; (4)Christian identity groups; (5)freemen/sovereign citizens; (6)neo-nazi groups; (7)militia/patriotism; (8)reconstructed traditions; (9)idiosyncratic sectarians; (10)single issues constituencies/lone guided missiles; (11)youth counter culture; (12)other	Group mainly affiliated
SF69	Other affiliations	SF_secgro	String	Other groups affiliated
SF70	Past affiliations	SF_pgrp	(1)KKK; (2)skinhead; (3)white supremacist; (4)Christian identity groups; (5)freemen/sovereign citizens; (6)neo-nazi groups; (7)militia/patriotism; (8)reconstructed traditions; (9)idiosyncratic sectarians; (10)single issues constituencies/lone guided missiles; (11)youth counter culture; (12)other	Past groups mainly affiliated

Q#	Variable Name	Variable ID	Values	Description
SF71	Other past affiliations	SF_pgrp2	String	Other past affiliations
SF72	Movement materials	SF_movmnt	(0)No; (1)Yes; (-99)Missing	Movement materials found during investigations?
SF73	If yes, specify	SF_mater	String	List all materials/literature found
SF74	Tax protester	SF_taxpro	(0)No; (1)Yes; (-99)Missing	Tax protester?
SF75	Survivalist	SF_surviv	(0)No; (1)Yes; (-99)Missing	Survivalist?
SF76	Strength of association	SF_bond	(0)0; (1)1; (2)2; (3)3; (4)4	Estimate the strength of the suspect's association to his/her extremist movement (1 lowest, 4 highest)?
SF77	Pro evidence 1	SF_proevid1	String	Evidence supporting extremist link
SF78	Pro source 1	SF_prosrc1	String	Source of evidence supporting extremist link
SF79	Pro evidence 2	SF_proevid2	String	Evidence supporting extremist link
SF80	Pro source 2	SF_prosrc2	String	Source of evidence supporting

Q#	Variable Name	Variable ID	Values	Description
				extremist link
SF81	Pro evidence 3	SF_proevid3	String	Evidence supporting extremist link
SF82	Pro source 3	SF_prosrc3	String	Source of evidence supporting extremist link
SF83	Pro evidence 4	SF_proevid4	String	Evidence supporting extremist link
SF84	Pro source 4	SF_prosrc4	String	Source of evidence supporting extremist link
SF85	Pro evidence 5	SF_proevid5	String	Evidence supporting extremist link
SF86	Pro source 5	SF_prosrc5	String	Source of evidence supporting extremist link
SF87	Con evidence 1	SF_conevid1	String	Evidence contrary to extremist link
SF88	Con source 1	SF_consrc1	String	Source of evidence contrary to extremist link
SF89	Con evidence 2	SF_conevid2	String	Evidence contrary to extremist link
SF90	Con source 2	SF_consrc2	String	Source of evidence contrary to extremist link
SF91	Con evidence 3	SF_conevid3	String	Evidence contrary to extremist link
SF92	Con source 3	SF_consrc3	String	Source of evidence contrary to

Q#	Variable Name	Variable ID	Values	Description
				extremist link
SF93	Con evidence 4	SF_conevid4	String	Evidence contrary to extremist link
SF94	Con source 4	SF_consrc4	String	Source of evidence contrary to extremist link
SF95	Con evidence 5	SF_conevid5	String	Evidence contrary to extremist link
SF96	Con source 5	SF_consrc5	String	Source of evidence contrary to extremist link
SF97	Role in scheme	SF_rolescehme	String	Describe suspect's role in scheme
SF98	Joined scheme day	SF_joindy	Numeric	What day did suspect join scheme?
SF98	Joined scheme month	SF_joinmnth	Numeric	What month did suspect join scheme?
SF98	Joined scheme year	SF_joinyr	Numeric	What year did suspect join scheme?
SF99	Leaved scheme day	SF_leavedy	Numeric	What day did suspect leave scheme?
SF99	Leaved scheme month	SF_leavemnth	Numeric	What month did suspect leave scheme?
SF99	Leaved scheme year	SF_leaveyr	Numeric	What year did suspect leave scheme?

Q#	Variable Name	Variable ID	Values	Description
SF100	Personal motivation	SF_pergre	(1)ideological/political grievance; (2)profit/greed; (3)both greed & grievance; (4)other	What was the suspect's primary motive for involvement in the scheme?
SF101	If motive, specify	SF_pergre2	String	Provide information on suspect's personal motive in the scheme
SF102	Avoids publicity	SF_avoid	(0)avoid; (1)generate publicity	Did suspect attempt to avoid publicity?
SF103	In media prior?	SF_pmed	(0)No; (1)Yes; (-99)Missing	Was suspect in the media prior to the scheme?
SF104	Reason in the media	SF_mresn	(1)general descriptive story about group; (2)protest activities; (3)political activities; (4)meeting announcements; (5)other activities; (6)involved in other criminal incidents	For what reason?
SF105	Weapon found (1)	SF_gunwep	(1)no; (2)legal guns; (3)illegal guns; (4)explosives; (5)knives/shank; (6)other weapons	Weapons found during investigations?

Q#	Variable Name	Variable ID	Values	Description
SF106	Additional weapons	SF_gunwep2	String	List all additional weapons found
SF107	Explosives found	SF_explo	(0)No; (1)Yes; (-99)Missing	Explosives or materials to build explosives found during investigations?
SF108	If yes, describe	SF_explo2	String	If yes, explain
SF109	Illicit revenue	SF_revenue	String	Estimated amount of illicit revenues earned by suspect from scheme
SF110	Government losses	SF_govloss	String	Estimated amount of government losses by suspect
SF111	Lone wolf	SF_wlf	(1)acted alone; (2)part of formal group; (3)part of informal group; (4)acting with others no clear group boundaries	Lone wolf or member of extremist group?
SF112	If group, specify	SF_wlf2	String	If member of extremist group, specify main group
SF113	Group connection	SF_grpconx	(1)crime committed under direct orders from group leadership; (2)crime not committed under direct leadership but still committed to further groups interests; (3)crime not related to group's cause/interests	Group connection to crime

Q#	Variable Name	Variable ID	Values	Description
SF114	3 current groups	SF_grpadd	String	List up to three additional groups suspect is involved in
SF115	3 past groups	SF_grpadd2	String	List three additional groups that suspect was involved in prior to scheme
SF116	Age joining group	SF_agrp	Numeric	Age when suspect joined group

Q#	Variable Name	Variable ID	Values	Description
SF117	Role in group	SF_roleg	(1)Other subordinate; (2)leader; (3)munitions expert; (4)safe-house expert; (5)intermediate leader; (6)special skill-voice stress; (7)intelligence officer; (8)special skill-bomb maker; (9)nonmember but party to conspiracy; (10)not known; (11)special skill-biological weapons; (12)special skill-chemical weapons; (13)second in command; (14)secretary; (15)security group; (16)affiliated and/or sympathizer; (17)fundraiser; (18)financial administrator; (19)money-launderer; (20)money-courier; (21)other	Suspect's role in the group
SF118	Length membership	SF_lngth	Numeric	Length of membership in months

Q#	Variable Name	Variable ID	Values	Description
SF119	How recruited	SF_rcrt	(1)prison/jail; (2)university/school; (3)newsletter/movement propaganda; (4)personal friend/neighbor/family member; (5)religious institution gathering; (6)military; (7)internet; (8)self-started; (9)personal visit by member; (10)charismatic leader; (11)targeted system of recruited; (12)by chance; (13)attended meetings; (14)individual decision	How was suspect recruited?
SF120	Recruited alone	SF_rcrtaln	(1)yes-recruited individually; (2)no-recruited w/group; (3)unknown	Recruited alone?
SF121	Participates in recruitment	SF_prtrcrt	(0)No; (1)Yes; (-99)Missing	Has suspect actively participated in recruiting?
SF122	How long movement	SF_yrsin	Numeric	Years involved in movement activities
SF123	Movement at scheme	SF_invol	(0)No; (1)Yes; (-99)Missing	Involved in movement activities at time of the offense?

Q#	Variable Name	Variable ID	Values	Description
SF124	Web site address	SF_web	String	Address of suspect's ideological web site
SF125	Share on WWW	SF_share	(0)No; (1)Yes; (-99)Missing	Has the suspect ever shared movement materials on the Internet?
SF126	Write essays	SF_essy	(0)No; (1)Yes; (-99)Missing	Has the suspect ever written essays related to the movement?
SF127	Write books	SF_book	(0)No; (1)Yes; (-99)Missing	Has the suspect ever written books related to the movement?
SF128	Host radio show	SF_radio	(0)No; (1)Yes; (-99)Missing	Has the suspect ever hosted radio shows?
SF129	Host TV show	SF_tv	(0)No; (1)Yes; (-99)Missing	Has the suspect ever hosted TV shows?
SF130	Give speech	SF_spech	(0)No; (1)Yes; (-99)Missing	Has the suspect ever given movement-related speeches?
SF131	Interview	SF_media	(0)No; (1)Yes; (-99)Missing	Has the suspect ever been interviewed by the media for movement related reasons?

Q#	Variable Name	Variable ID	Values	Description
SF132	Organize movement	SF_protst	(0)No; (1)Yes; (-99)Missing	Has the suspect ever organized movement-related activities?
SF133	Attend any event	SF_atpro	(0)No; (1)Yes; (-99)Missing	Has the suspect ever attended any movement-related events?
SF134	Influence politics	SF_pol	(0)No; (1)Yes; (-99)Missing	Has the suspect ever attempted to influence politics?
SF135	Organize conference	SF_conf	(0)No; (1)Yes; (-99)Missing	Has the suspect ever organized movement-related conferences?
SF136	Attend conference	SF_aconf	(0)No; (1)Yes; (-99)Missing	Has the suspect ever attended movement-related conferences?
SF137	Publicize event	SF_pub	(0)No; (1)Yes; (-99)Missing	Has the suspect ever publicized movement-related events?
SF138	Letters to media	SF_letr	(0)No; (1)Yes; (-99)Missing	Has the suspect ever sent letters to newspaper, magazine, or other media outlet about movement?

Q#	Variable Name	Variable ID	Values	Description
SF139	Clothing/tattoos	SF_cloth	(0)No; (1)Yes; (-99)Missing	Has the suspect ever worn clothes characteristic of extremist group, had extremist tattoos, etc.?
SF140	Attend protest	SF_61pro	(0)No; (1)Yes; (-99)Missing	Has the suspect ever attended movement-related protests?
SF141	Attend meetings	SF_attmet	(0)No; (1)Yes; (-99)Missing	Has the suspect ever attended movement-related meetings?
SF142	Leafletting	SF_leaf	(0)No; (1)Yes; (-99)Missing	Has the suspect ever been involved in pro movement leaf-letting?
SF143	Attend festivals	SF_atfest	(0)No; (1)Yes; (-99)Missing	Has the suspect ever attended movement-related festival?
SF144	Recruit others	SF_recrui	(0)No; (1)Yes; (-99)Missing	Has the suspect ever attempted to recruit others?
SF145	Other, specify	SF_othr	String	If other movement-related activities, specify

Q#	Variable Name	Variable ID	Values	Description
SF146	Sell domestic bogus trusts	SF_sedobo	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect sell domestic bogus trusts?
SF147	Sell foreign bogus trusts	SF_sefobo	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect sell foreign bogus trusts?
SF148	Use domestic bogus trusts	SF_usedobo	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect use domestic bogus trusts?
SF149	Use foreign bogus trusts	SF_usefobo	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect use foreign bogus trusts?
SF150	Purchase securities	SF_pursec	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect purchase securities?
SF151	Sell securities	SF_sellsec	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect sell securities?
SF152	Promote/market tax shleter packages	SF_protax	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect promote or market tax shelter packages?

Q#	Variable Name	Variable ID	Values	Description
SF153	Purchase tax shelter packages	SF_purtax	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect purchase tax shelter packages?
SF154	Fail to file an income tax return	SF_failfi	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect fail to file an income tax return?
SF155	Fail to report part of income/properties	SF_failrepinc	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect fail to report part of income/properties?
SF156	Fail to pay employment taxes	SF_failpay	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect fail to pay employment taxes?
SF157	Fail to report currency requirements	SF_failrepcur	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect fail to report currency requirements?
SF158	Use "corporation sole" laws/arguments	SF_corpso	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect use "corporation sole" laws or arguments?
SF159	Use "frivolous arguments"/"common law"	SF_frivarg	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect use frivolous arguments" or other "common law" arguments in court?

Q#	Variable Name	Variable ID	Values	Description
SF160	File "zero wages" return form	SF_zerowage	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect file a "zero wages" return form?
SF161	Use "form 843" tax abatement	SF_form843	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect use "form 843" for illegal tax abatement?
SF162	File false/misleading tax forms	SF_falsetax	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect file false or misleading tax forms?
SF163	Abuse charitable organizations and deductions	SF_charorg	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect abuse the status of charitable organizations and deductions?
SF164	File false claims for refund and abatement	SF_falcla	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect file false claims for tax refund and/or abatement?
SF165	File false liens	SF_falie	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect file false liens or bonds?
SF166	Set up domestic "shell" corporation(s)	SF_domshell	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect set up domestic "shell? corporation(s)?

Q#	Variable Name	Variable ID	Values	Description
SF167	Set up foreign "shell" corporation(s)	SF_forshell	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect set up foreign "shell? corporation(s)?
SF168	Use a nominee entity	SF_noment	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect use a nominee person or entity?
SF169	Use mail drops to conceal business location	SF_maildrop	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect use mail drops to conceal business location?
SF170	Discourage the use of SSN	SF_ssn	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect discourage the use of SSN?
SF171	Use false SSN	SF_fakeSSN	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect make use of false SSN?
SF172	Use conterfeit ID/credit card	SF_fakeID	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect use counterfeited ID, credit card or other?
SF173a	Deposit funds in domestic bank accounts	SF_fundsdomestic	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect deposit funds in domestic bank accounts?

Q#	Variable Name	Variable ID	Values	Description
SF173b	Deposit funds in foreign bank accounts	SF_forbank	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect deposit funds in foreign bank accounts?
SF174	Conceal foreign bank accounts	SF_concbank	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect conceal foreign bank accounts?
SF175a	Use domestic debit/credit cards	SF_domesticcredit	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect use domestic debit or credit cards?
SF175b	Use foreign debit/credit cards	SF_forcards	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect use foreign debit or credit cards?
SF176	Conduct financial transactions in cash	SF_cash	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect conduct financial transactions in cash?
SF177	Engage in prohibited financial transactions	SF_prohfintr	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect engage in prohibited financial transactions?
SF178	Conduct real estate transactions	SF_realest	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect conduct real estate transactions?

Q#	Variable Name	Variable ID	Values	Description
SF179	Structure financial transactions	SF_structfin	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect structure financial transactions?
SF180	Smuggle currency abroad	SF_physcur	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect smuggle currency abroad?
SF181	Move funds via wire transfer w/in US	SF_wirein	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect move funds via wire transfer within the US?
SF182	Move funds via wire transfer w/out US	SF_wireout	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect move funds via wire transfer outside the US?
SF183	Use cashier's check	SF_cashcheck	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect use cashier's checks?
SF184	Use currency exchange bureaus	SF_curexbu	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect use currency exchange bureaus?
SF185	Use informal value transfer system (Hawala)	SF_hawala	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect use informal value transfer system (e.g. Hawala)?

Q#	Variable Name	Variable ID	Values	Description
SF186	Other technique	SF_othertec	(0)No; (1)Yes; (-99)Missing	In the context of the scheme, did the suspect use other techniques not listed above?
SF187	If other, specify	SF_othertec2	String	If yes, specify
SF188	Suspect ID#	SNF_SuspectID	Numeric	Suspect ID# for primary suspect (same as Q#2 above)
SF189	Related person/business name	SNF_Name	String	Name of person/business related to suspect
SF190	If coded, suspect/business ID#	SNF_SuspectID2	Number	If related person/business is also coded, suspect/business ID#
SF191	Involved in same scheme?	SNF_Involvement	(0)No; (1)Yes; (-99)Missing	Is related person involved in same scheme as primary suspect?
SF192	Involved in related incident?	SNF_otherinc	(0)No; (1)Yes; (-99)Missing	Is related person involved in other criminal incident with primary suspect?
SF193	If yes, describe incident	SNF_otherinc2	String	If yes, describe incident
SF194	Political extremist?	SNF_polex	(0)No; (1)Yes; (-99)Missing	Is related person a political extremist?

Q#	Variable Name	Variable ID	Values	Description
SF195	If political extremist, specify	SNF_polex2	(1)Far-rightist; (2)ALF-ELF; (3)Global Jihadi; (4)Local Jihadi; (5)Non-religious/secular Arab nationalist; (6)Other international terrorist	If political extremist, specify
SF196	If not an extremist, specify	SNF_polex3	(1)White-collar offender; (2)Blue-collar offender; (3)Organized crime; (4)Other criminal status; (5)Non-criminal status	If not a political extremist, specify
SF197	Immediate family?	SNF_familytie1	(0)No; (1)Yes; (-99)Missing	Is related person immediate family (e.g. spouse, siblings)?
SF198	Non-immediate family?	SNF_familytie2	(0)No; (1)Yes; (-99)Missing	Is related person non-immediate family (e.g. cousins)?
SF199	Co-defendant?	SNF_crimetie1	(0)No; (1)Yes; (-99)Missing	Is related person a co-defendant (i.e. prosecuted in the same judicial case as suspect)?
SF200	Co-suspect?	SNF_crimetie2	(0)No; (1)Yes; (-99)Missing	Is person a co-suspect (i.e. involved in same scheme but prosecuted in separate case or not prosecuted)?

Q#	Variable Name	Variable ID	Values	Description
SF201	Business at time of scheme?	SNF_businesstie1	(0)No; (1)Yes; (-99)Missing	Did person engage in legitimate business activities with suspect at time of scheme (e.g. business partners, service provider, etc.)?
SF202	Business in the past?	SNF_businesstie2	(0)No; (1)Yes; (-99)Missing	Did related person engage in legitimate business activities with suspect before scheme (e.g. former business associates)?
SF203	Additional information	SNF_othertie2	String	Provide any additional information on this relationship
SF204	Primary source	SNF_dsor2	(1)Police (2)Court (3)Other Government Doc (4)Militia Watchdog (5)ADL (6)SPLC (7)Other Watch Pub (8)News-Journalist (9)Scholarly Work (10)Scholarly Database (11)Nonscholarly Work (12)Website (13)Key Informant (14)Other Source	Primary source of relational ties data?

Q#	Variable Name	Variable ID	Values	Description
SF205	Secondary source	SNF_dsor3	(1)Police (2)Court (3)Other Government Doc (4)Militia Watchdog (5)ADL (6)SPLC (7)Other Watch Pub (8)News-Journalist (9)Scholarly Work (10)Scholarly Database (11)Nonscholarly Work (12)Website (13)Key Informant (14)Other Source	Secondary source of relational ties data?
SF206	Suspect name	SF_NameB	String	Suspect name
SF207	Suspect ID#	SF_id3B	Numeric	Suspect ID#
SF208	Prior arrests	SF_prior	(0)No; (1)Yes; (-99)Missing	Prior arrest history
SF209	# of priors	SF_prior2	(0)0; (1)1-5; (2)6-20; (3)more than 20	Total # of prior arrests

Q#	Variable Name	Variable ID	Values	Description
SF210	Arrested ideological	SF_arideo	(0)No; (1)Yes; (-99)Missing	Ever arrested for ideological crimes?
SF211	Ideological violent	SF_arvio1a	(0)No; (1)Yes; (-99)Missing	Ever arrested for ideological violent crimes?
SF212	# of ideological violent	SF_arvio1b	Numeric	# of ideological violent crime arrests if known
SF213	Non-ideological violent	SF_arvio2a	(0)No; (1)Yes; (-99)Missing	Ever arrested for non-ideological violent crimes?
SF214	# non-ideological violent	SF_arvio2b	Numeric	# of non-ideological violent crime arrests if known
SF215	Ideological property	SF_arpro1a	(0)No; (1)Yes; (-99)Missing	Ever arrested for ideological property crimes?
SF216	# ideological property	SF_arpro1b	Numeric	# of ideological property crime arrests if known
SF217	Non-ideological property	SF_arpro2a	(0)No; (1)Yes; (-99)Missing	Ever arrested for non-ideological property crimes?
SF218	# non-ideological property	SF_arpro2b	Numeric	# of non-ideological property crime arrests if known

Q#	Variable Name	Variable ID	Values	Description
SF219	Ideological drug	SF_ardru1a	(0)No; (1)Yes; (-99)Missing	Ever arrested for ideological drug-related crimes?
SF220	# ideological drug	SF_ardru1b	Numeric	# of ideological drug-related crime arrests if known
SF221	Non-ideological drug	SF_ardru2a	(0)No; (1)Yes; (-99)Missing	Ever arrested for non-ideological drug-related crimes?
SF222	# non-ideological drug	SF_ardru2b	Numeric	# of non-ideological drug-related crime arrests if known
SF223	Ideological gun	SF_argun1a	(0)No; (1)Yes; (-99)Missing	Ever arrested for ideological gun-related crimes?
SF224	# ideological gun	SF_argun1b	Numeric	# of ideological gun-related crime arrests if known
SF225	Non-ideological gun	SF_argun2a	(0)No; (1)Yes; (-99)Missing	Ever arrested for non-ideological gun-related crimes?
SF226	# non-ideological gun	SF_argun2b	Numeric	# of non-ideological gun-related crime arrests if known
SF227	Ideological white collar	SF_arwc1a	(0)No; (1)Yes; (-99)Missing	Ever arrested for ideological white-collar crimes?

Q#	Variable Name	Variable ID	Values	Description
SF228	# ideological white collar	SF_arwc1b	Numeric	# of ideological white-collar crime arrests if known
SF229	Non-ideological white collar	SF_arwc2a	(0)No; (1)Yes; (-99)Missing	Ever arrested for non-ideological white-collar crimes?
SF230	# non-ideological white collar	SF_arwc2b	Numeric	# of non-ideological white-collar crime arrests if known
SF231	Ideological alcohol	SF_aral1a	(0)No; (1)Yes; (-99)Missing	Ever arrested for ideological alcohol-related crimes?
SF232	# ideological alcohol	SF_aral1b	Numeric	# of ideological alcohol-related arrests if known
SF233	Non-ideological alcohol	SF_aral2a	(0)No; (1)Yes; (-99)Missing	Ever arrested for non-ideological alcohol-related crimes?
SF234	# non-ideological alcohol	SF_aral2b	Numeric	# of non-ideological alcohol-related arrests if known
SF235	Ideological traffic	SF_artraf1a	(0)No; (1)Yes; (-99)Missing	Ever arrested for ideological traffic offenses?
SF236	# ideological traffic	SF_artraf1b	Numeric	# of ideological traffic arrests if known

Q#	Variable Name	Variable ID	Values	Description
SF237	Non-ideological traffic	SF_artraf2a	(0)No; (1)Yes; (-99)Missing	Ever arrested for non-ideological traffic offenses?
SF238	# non-ideological traffic	SF_artraf2b	Numeric	# of non-ideological traffic arrests if known
SF239	Ideological civil disobedience	SF_arnvcd1a	(0)No; (1)Yes; (-99)Missing	Ever arrested for ideological civil disobedience?
SF240	# ideological civil disobedience	SF_arnvcd1b	Numeric	# of ideological civil disobedience arrests if known
SF241	Non-ideological civil disobedience	SF_arnvcd2a	(0)No; (1)Yes; (-99)Missing	Ever arrested for non-ideological disobedience?
SF242	# non-ideological civil disobedience	SF_arnvcd2b	Numeric	# of non-ideological civil disobedience arrests if known
SF243	Ideological tax refusal	SF_artro1a	(0)No; (1)Yes; (-99)Missing	Ever arrested for ideological failure to file a tax return, i.e. tax refusal (omission)?
SF244	# ideological tax refusal	SF_artro1b	Numeric	# of ideological tax refusal arrests (omission) if known
SF245	Non-ideological tax refusal	SF_artro2a	(0)No; (1)Yes; (-99)Missing	Ever arrested for non-ideological failure to file a tax return (omission)?

Q#	Variable Name	Variable ID	Values	Description
SF246	# non-ideological tax refusal	SF_artro2b	Numeric	# of non-ideological arrests for failure to file a tax return (omission) if known
SF247	Ideological tax-related	SF_artra1a	(0)No; (1)Yes; (-99)Missing	Ever arrested for ideological tax-related crime (affirmative)?
SF248	# ideological tax-related	SF_artra1b	Numeric	# of ideological tax-related arrests (affirmative) if known
SF249	Non-ideological tax-related	SF_artra2a	(0)No; (1)Yes; (-99)Missing	Ever arrested for non-ideological tax-related crime (affirmative)?
SF250	# non-ideological tax-related	SF_artra2b	Numeric	# of non-ideological tax-related arrests (affirmative) if known
SF251	Ideological tax-refusal civil actions	SF_catro1a	(0)No; (1)Yes; (-99)Missing	Ever arrested for ideological failure to file a tax return, i.e. tax refusal (omission), in the context of a civil action?
SF252	# ideological tax-refusal civil action	SF_catro1b	Numeric	# of ideological tax refusal arrests in the context of a civil action if known
SF253	Non-ideological tax-refusal civil action	SF_catro2a	(0)No; (1)Yes; (-99)Missing	Ever arrested for non-ideological failure to file a tax return (omission) in the context of a civil action?
SF254	# non-ideo tax-refusal civil	SF_catro2b	Numeric	# of non-ideological arrests for

Q#	Variable Name	Variable ID	Values	Description
	action			failure to file a tax return (omission) in the context of a civil action if known
SF255	Ideological tax-related civil action	SF_catri1a	(0)No; (1)Yes; (-99)Missing	Ever arrested for ideological tax-related violation (affirmative) in the context of a civil action?
SF256	# ideological tax-related civil action	SF_catri1b	Numeric	# of arrests for ideological tax-related violation (affirmative) in the context of a civil action if known
SF257	Non-ideological tax-related civil action	SF_catri2a	(0)No; (1)Yes; (-99)Missing	Ever arrested for non-ideological tax-related violation (affirmative) in the context of a civil action?
SF258	# non-ideological tax-related civil action	SF_catri2b	Numeric	# of arrests for non-ideological tax-related violation (affirmative) in the context of a civil action if known
SF259	Ideological land use/environmental	SF_arlue1a	(0)No; (1)Yes; (-99)Missing	Ever arrested for ideological violation of land use or other environmental-related crime?
SF260	# ideological land use/environment	SF_arlue1b	Numeric	# of arrests for ideological violation of land use or other environmental-related crime if known

Q#	Variable Name	Variable ID	Values	Description
SF261	Non-ideological land use/environmental	SF_arlue2a	(0)No; (1)Yes; (-99)Missing	Ever arrested for non-ideological violation of land use or other environmental-related crime?
SF262	# non-ideological land use/environmental	SF_arlue2b	Numeric	# of arrests for non-ideological violation of land use or other environmental-related crime if known
SF263	Ideological land use/enviro civil action	SF_calue1a	(0)No; (1)Yes; (-99)Missing	Ever arrested for ideological violation of land use or other environmental-related crime in the context of a civil action?
SF264	# ideological land use/environmental civil action	SF_calue1b	Numeric	# of arrests for ideological violation of land use or other environmental-related crime in the context of a civil action if known
SF265	Non-ideological land use/environmental civil action	SF_calue2a	(0)No; (1)Yes; (-99)Missing	Ever arrested for non-ideological violation of land use or other environmental-related crime in the context of a civil action?
SF266	# non-ideological land use/environmental civil action	SF_calue2b	Numeric	# of arrests for non-ideological violation of land use or other environmental-related crime in the context of a civil action if known

Q#	Variable Name	Variable ID	Values	Description
SF267	Other ideological	SF_aroth1a	(0)No; (1)Yes; (-99)Missing	Ever arrested for other ideological crimes?
SF268	# other ideological	SF_aroth1b	Numeric	# of arrests for other ideological crimes
SF269	If other, specify	SF_aroth1c	String	If arrested for other ideological crimes, specify
SF270	Other non-ideological	SF_aroth2a	(0)No; (1)Yes; (-99)Missing	Ever arrested for other non-ideological crimes?
SF271	# other non-ideological	SF_aroth2b	Numeric	# of arrests for other non-ideological crimes
SF272	If other, specify	SF_aroth2c	String	If arrested for other non-ideological crimes, specify
SF273	Ideological foreign arrests	SF_arfor1a	(0)No; (1)Yes; (-99)Missing	Ever arrested for ideological crimes in foreign countries?
SF274	# ideological foreign arrests	SF_arfor1b	Numeric	# ideological foreign arrests
SF275	If yes, where and what	SF_arfor1c	String	If yes, specify where suspect was arrested and for what ideological crime

Q#	Variable Name	Variable ID	Values	Description
SF276	Non-ideological foreign arrests	SF_arfor2a	(0)No; (1)Yes; (-99)Missing	Ever arrested for non-ideological crimes in foreign countries?
SF277	# non-ideological foreign arrests	SF_arfor2b	Numeric	# non-ideological foreign arrests
SF278	If yes, where and what	SF_arfor2c	String	If yes, specify where suspect was arrested and for what non-ideological crime
SF279	Prior convictions	SF_convc	(0)No; (1)Yes; (-99)Missing	Prior convictions, if applicable
SF280	# prior convictions	SF_convc2	Numeric	Total number of prior convictions
SF281	Prior ideological convictions	SF_idcon	(0)No; (1)Yes; (-99)Missing	Ever convicted for ideological crimes?
SF282	# prior ideological convictions	SF_idcon2	Numeric	# of prior ideological convictions
SF283	Foreign ideological conviction	SF_idconfor	(0)No; (1)Yes; (-99)Missing	Ever convicted for ideological crimes in foreign countries?
SF284	# foreign ideological convictions	SF_idconfor2	Numeric	# of prior foreign ideological convictions
SF285	If yes, where and what	SF_idconfor3	String	If yes, specify where suspect was

Q#	Variable Name	Variable ID	Values	Description
				arrested and for what ideological crime
SF286	Foreign non-ideological conviction	SF_xidconfor	(0)No; (1)Yes; (-99)Missing	Ever convicted abroad for non-ideological crimes?
SF287	# foreign non-ideological convictions	SF_xidconfor2	Numeric	# of prior foreign non-ideological convictions
SF288	If yes, where and what	SF_xidconfor3	String	If yes, specify where suspect was arrested and for what non-ideological crime
SF289	Prior non-arrests	SF_prnoarr	(0)No; (1)Yes; (-99)Missing	Did the suspect commit any crime for which he/she was not arrested?
SF290	If yes, specify	SF_prnoarr2	String	If yes, specify
SF291	Ever in prison	SF_prison	(0)No; (1)Yes; (-99)Missing	Was suspect ever in prison to serve sentence?
SF292	# of terms	SF_priso2	Numeric	Number of terms if multiple incarcerations
SF293	Length of terms in months	SF_priso3	Numeric	Length of prison terms in months
SF294	Ever in prison (2)	SF_priso4	(0)No; (1)Yes; (-99)Missing	Was suspect ever in prison for reasons other than serving sentence (e.g. pre-trial detention)?

Q#	Variable Name	Variable ID	Values	Description
SF295	If yes, explain why	SF_priso5	String	If yes, explain why
SF296	Federal prison	SF_prifed	(0)No; (1)Yes; (-99)Missing	Served time in federal prison?
SF297	State prison	SF_prista	(0)No; (1)Yes; (-99)Missing	Served time in state prison?
SF298	Local prison	SF_priloc	(0)No; (1)Yes; (-99)Missing	Served time in local prison?
SF299	Served time in foreign prison	SF_prifor	(0)No; (1)Yes; (-99)Missing	Served time in foreign prison?
SF300	If yes, where	SF_prifor2	String	If yes, specify where
SF301	Gang in prison	SF_ganpri	(1)never joined gang; (2)joined a white supremacist/separatist gang in prison; (3)joined other type of gang in prison	Did suspect join a gang while in prison?
SF302	Investigated	SF_invst	(0)No; (1)Yes; (-99)Missing	Was suspect investigated for participation in scheme?

Q#	Variable Name	Variable ID	Values	Description
SF303	Arrested ideological	SF_arinc	(0)No; (1)Yes; (-99)Missing	Day of arrest
SF304	Day of arrest	SF_arrstdy	Numeric	Month of arrest
SF304	Month of arrest	SF_arrstmnth	Numeric	Year of arrest
SF304	Year of arrest	SF_arrstyr	Numeric	Year of arrest
SF305	Indicted	SF_indicted	(0)No; (1)Yes; (-99)Missing	Was suspect indicted for involvement in scheme?
SF306	Indictment ID	SF_indictID	String	Indictment ID
SF307	Day of indictment	SF_indctdy	Numeric	Day of indictment
SF307	Month of indictment	SF_indctmnth	Numeric	Month of indictment
SF307	Year of indictment	SF_indctyr	Numeric	Year of indictment
SF308	Day of superseding indictment (1)	SF_superdy1	Numeric	Day of superseding indictment (1)
SF308	Month of superseding indictment (1)	SF_supermth1	Numeric	Month of superseding indictment (1)
SF308	Year of superseding indictment (1)	SF_superyr1	Numeric	Year of superseding indictment (1)
SF309	Day of superseding indictment (2)	SF_superdy2	Numeric	Day of superseding indictment (2)

Q#	Variable Name	Variable ID	Values	Description
SF309	Month of superseding indictment (2)	SF_supermth2	Numeric	Month of superseding indictment (2)
SF309	Year of superseding indictment (2)	SF_superyr2	Numeric	Year of superseding indictment (2)
SF310	Day of judgment	SF_jdgmntdy	Numeric	Day of judgment
SF310	Month of judgment	SF_jdgmntmnth	Numeric	Month of judgment
SF310	Year of judgment	SF_jdgmntyr	Numeric	Year of judgment
SF311	Day of sentence	SF_sentdy	Numeric	Day of sentence
SF311	Month of sentence	SF_sentmnth	Numeric	Month of sentence
SF311	Year of sentence	SF_sentyr	Numeric	Year of sentence
SF312	Charges indicted	SF_charged1	String	List all charges suspect was indicted with (e.g. mail fraud, money laundering, etc)
SF313	USC provisions (1)	SF_charged2	String	List USC provisions in indictment, if known (e.g. USC 18:345)
SF314	# of charges	SF_numch	Numeric	Number of charges against suspect, if known
SF315	# of counts	SF_cnts	Numeric	Number of counts against suspect, if known
SF316	Charges convicted	SF_convicted1	String	List all charges suspect was convicted for (e.g. mail fraud, money laundering, etc)

Q#	Variable Name	Variable ID	Values	Description
SF317	USC provisions (2)	SF_convicted2	String	List USC provisions for which convicted, if known (e.g. USC 18:345)
SF318	# charges convicted	SF_charcv	Numeric	Number of charges convicted for, if applicable
SF319	# counts convicted	SF_cntcv	Numeric	Number of counts convicted of, if applicable
SF320	Resisted arrest?	SF_resist	(0)No; (1)Yes; (-99)Missing	Did the suspect resist arrest?
SF321	Bail granted	SF_bail	(1)No; (2)Yes; (3)yes but later revoked	Was bail granted by court?
SF322	If yes, amount	SF_balam	Numeric	Specify bail amount, if applicable
SF323	Permanent injuction	SF_injunction	(0)No; (1)Yes; (-99)Missing	Did suspect receive a permanent injunction order to refrain from certain activities (e.g. prepare tax returns, provide financial advice, etc.)?
SF324	Month of injunction	SF_monthinj	Numeric	Month of injunction
SF324	Day of injunction	SF_dayinj	Numeric	Day of injunction
SF324	Year of injunction	SF_yearinj	Numeric	Year of injunction

Q#	Variable Name	Variable ID	Values	Description
SF325	Contempt of court?	SF_contempt	(0)No; (1)Yes; (-99)Missing	Was suspect hold in contempt of court?
SF326	Month of court order	SF_contemptmth	Numeric	Month of court order
SF326	Day of court order	SF_contemptdy	Numeric	Day of court order
SF326	Year of court order	SF_contemptyr	Numeric	Year of court order
SF327	Juridiction of trial	SF_jur	(1)federal; (2)state; (3)both	Jurisdiction of trial
SF328	Jurisdiction, specified	SF_jur2	String	Specify state or federal circuit or county
SF329	# of co-defendants	SF_coefd	Numeric	Specify number of co-defendants on trial, if applicable
SF330	Representation	SF_represn	(1)private attorney; (2)attorney for cause-Kirk Lyons etc.; (3)public defense-assigned; (4)represented himself-herself	Legal representation in court

Q#	Variable Name	Variable ID	Values	Description
SF331	Trial result	SF_trslt	(1)Incompetent to stand trial; (2)pled guilty; (3)tried alone and found guilty by jury; (4)tried with co-defendants and found guilty by jury; (5)dismissed due to mistrial or government motion; (6)acquitted; (7)not guilty by reason of insanity; (8)guilty but mentally ill; (9)charges dropped before trial; (10)selected bench trial and convicted; (11)selected bench trial and acquitted	Trial result
SF332	Appeal	SF_apeal	(1)no appeal; (2)appeal pending; (3)appealed and lost; (4)appealed and won; (5)appealed and retried	Did suspect appeal sentence?
SF333	Informant	SF_inform	(0)No; (1)Yes; (-99)Missing	Suspect government informant, if known
SF334	Confession	SF_snitch	(0)No; (1)Yes; (-99)Missing	Did suspect confess?

Q#	Variable Name	Variable ID	Values	Description
SF334	Testified against co-defendant	SF_confes	(0)No; (1)Yes; (-99)Missing	Did suspect testify in court against confederates?
SF336	Court sentence	SF_ctsnt	(0)No; (1)Yes; (-99)Missing	Was suspect given prison sentence by court?
SF337	Minimum	SF_ctsnt2	Numeric	Minimum sentence in months
SF338	Maximum	SF_ctsnt3	Numeric	Maximum sentence in months
SF339	Court fine	SF_fine	(0)No; (1)Yes; (-99)Missing	Was suspect given a monetary fine by court?
SF340	Amount	SF_fine2	Numeric	If yes, specify amount
SF341	Other sentence, specify	SF_otsent	String	If suspect received another type of court sentence, specify
SF342	Probation at offense	SF_prob	(0)No; (1)Yes; (-99)Missing	Was suspect on probation at time of offense?

Q#	Variable Name	Variable ID	Values	Description
SF343	Current status	SF_stats	(1)paroled in community; (2)in custody serving sentence; (3)in pre-trial custody; (4)deported/repatriated; (5)executed; (6)at large/fugitive; (7)on death row; (8)free/served time; (9)free/never served time	Current status
SF344	Civil action	SF_civli	(1)no civil action; (2)civil action by government (injunction-civil suits-etc); (3)civil action by watch-group; (4)civil action by victim; (5)civil action by private party	Was civil action taken against suspect?
SF345	Found liable	SF_civli1	(0)No; (1)Yes; (-99)Missing	Was suspect found liable?
SF346	If yes, amount	SF_civli2	Numeric	If suspect was found civilly liable, specify for what amount in dollars
SF347	Month of judgment	SF_civlimnth	Numeric	Month of civil judgment
SF347	Day of judgment	SF_civllidy	Numeric	Day of civil judgment
SF347	Year of judgment	SF_civliyr	Numeric	Year of civil judgment

Q#	Variable Name	Variable ID	Values	Description
SF347-1	Additional Information	SF_memo	String	Any additional information related to the suspect
SF342	RT:Month of judgment	SF_rtjdgmntmnth	Numeric	Retrial: Month of judgment
SF342	RT:Day of judgment	SF_rtjdgmntdy	Numeric	Retrial: Day of judgment
SF342	RT:Year of judgment	SF_rtjdgmntyr	Numeric	Retrial: Year of judgment
SF343	RT:Bail	SF_rtbail	(1)No; (2)Yes; (3)yes but later revoked	Retrial: Was bail granted by court?
SF344	RT:Amount	SF_rtbalam	Numeric	Retrial: Specify bail amount, if applicable
SF345	RT:Representation	SF_rtrepresn	(1)private attorney; (2)attorney for cause-Kirk Lyons etc.; (3)public defense-assigned; (4)represented himself-herself	Retrial: Legal representation in court
SF346	RT:All charges indicted	SF_rtcharged1	String	Retrial: List all charges (e.g. mail fraud, money laundering, etc)
SF347	RT:USC provisions charged	SF_rtcharged2	String	Retrial: List USC provisions (e.g. USC 18:345)
SF348	RT:# charges	SF_rtnumch	Numeric	Retrial: Number of charges against suspect, if applicable
SF349	RT:# counts	SF_rtcnts	Numeric	Retrial: Number of counts against suspect, if applicable

Q#	Variable Name	Variable ID	Values	Description
SF350	RT:All charges convicted	SF_rtconvicted1	String	Retrial: List all charges convicted (e.g. mail fraud, money laundering, etc)
SF351	RT:USC provisions convicted	SF_rtconvicted2	String	Retrial: List USC provisions convicted (e.g. USC 18:345)
SF352	RT:# charges convicted	SF_rtcharcv	Numeric	Retrial: Number of charges convicted of, if applicable
SF353	RT:# counts convicted	SF_rtcntcv	Numeric	Retrial: Number of counts convicted of, if applicable
SF354	RT:Jurisdiction	SF_rtjur	(1)federal; (2)state; (3)both	Retrial: Jurisdiction of trial
SF355	RT:Jurisdiction, specified	SF_rtjur2	String	Retrial: Specify state or federal circuit or county
SF356	RT:# co-defendants	SF_rtcoefd	Numeric	Retrial: Specify number of co-defendants on trial, if applicable

Q#	Variable Name	Variable ID	Values	Description
SF357	RT:Trial result	SF_rttrslt	(1)Incompetent to stand trial; (2)pled guilty; (3)tried alone and found guilty by jury; (4)tried with co-defendants and found guilty by jury; (5)dismissed due to mistrial or government motion; (6)acquitted; (7)not guilty by reason of insanity; (8)guilty but mentally ill; (9)charges dropped before trial; (10)selected bench trial and convicted; (11)selected bench trial and acquitted	Retrial: Trial Result
SF358	RT:Appeal	SF_rtapeal	(1)no appeal; (2)appeal pending; (3)appealed and lost; (4)appealed and won; (5)appealed and retried	Retrial: Did suspect appeal?
SF359	RT:Informant	SF_rtinform	(0)No; (1)Yes; (-99)Missing	Retrial: Suspect government informant, if known
SF360	RT:Testified against	SF_rtsnitch	(0)No; (1)Yes; (-99)Missing	Retrial: Did suspect testify against codefendants?

Q#	Variable Name	Variable ID	Values	Description
SF361	RT:Sentence	SF_rtctsnt	(0)No; (1)Yes; (-99)Missing	Retrial: Was suspect given prison sentence by court?
SF362	RT:Minimum	SF_rtctsnt2	Numeric	Retrial: Minimum sentence length in months
SF363	RT:Maximum	SF_rtctsnt3	Numeric	Retrial: Maximum sentence length in months
SF364	RT:Fine	SF_rtfine	Numeric	Retrial: Was suspect given a monetary fine by court?
SF365	RT:Amount	SF_rtfine2	Numeric	Retrial: If yes, specify amount
SF366	RT:Other sentence	SF_rtotsent	String	Retrial: If suspect received another type of court sentence, specify

Financial - Business Entity Codebook: Coding Issues

NOTE: This document should be in front of the coder as they code. If a business entity mentioned in the open sources does not meet the inclusion criteria it is NOT to be coded.
(1) INCLUSION CRITERIA – WHAT IS A BUSINESS ENTITY?

A business entity is a legally recognized organization which the open source information indicates:

(i) Was designed to provide financial goods and/or services to customers;

(ii) Was owned, presided, or directed by at least one of the coded suspects;

(iii) Had some role (even if marginal) in the preparation or execution of the scheme.

By business entity, we do not mean groups or organizations where the suspect engages in political activism or terrorist activities (e.g. "We The People", an anti-tax organization; Al-Qaeda, a terrorist organization, etc.). We will code, however, this type of data in the Group section of Suspect 1 Codebook.

Q#	Variable Name	Variable ID	Values	Description
BF1	Relational ID	BF_ID	Numeric	Relational ID (Scheme ID + Masterfile ID)
BF2	Business ID	BF_ID2	Numeric	Business ID
BF3	Business victim?	BF_victim	(0)No; (1)Yes; (-99)Missing	Business victimized or related to victim?
BF4	Business name	BF_name	String	Name of business entity
BF5	Location	BF_location	String	Primary location of business entity
BF6	Additional locations	BF_location2	String	Additional locations
BF7	Month founded	BF_foundmnth	Numeric	Month business entity was founded
BF7	Day founded	BF_founddy	Numeric	Day business entity was founded
BF7	Year founded	BF_foundyr	Numeric	Year business entity was founded
BF8	Business type	BF_type	(1)Sole proprietorship; (2)General partnership; (3)Limited partnership; (4)LLC; (5)Corporation	Type of business entity

BF9	Business services	BF_services	(1)Legal services; (2)Tax preparation; (3)Tax advice; (4)Financial analysis/consultancy; (5)Banking/loans; (6)Investment; (7)Other	Services provided
BF10	If other, specify	BF_services2	String	If other service type, specify
BF11	Shell company	BF_legitimate	(0)No; (1)Yes; (-99)Missing	Is business entity a "shell" company (i.e. a company that exists on paper but transact either no business or minimal business)
BF12	Non-profit	BF_nonprofit	(0)No; (1)Yes; (-99)Missing	Is business entity a non-profit organization?
BF13	Charitable	BF_charitable	(0)No; (1)Yes; (-99)Missing	Is business entity a charitable organization?
BF14	Founder name	BF_founder1	String	Founder's name
BF15	Founder suspect ID	BF_founder2	String	Founder's Suspect ID, if applicable
BF16	Co-founder name	BF_founder3	String	Co-founder's name
BF17	Co-founder suspect ID	BF_founder4	String	Co-founder's Suspect ID, if applicable
BF18	Owner name	BF_owner1	String	Owner's name
BF19	Owner suspect ID	BF_owner2	String	Owner's Suspect ID, if applicable

BF20	Co-owner name	BF_owner3	String	Co-owner's name
BF21	Co-owner suspect ID	BF_owner4	String	Co-owner's Suspect ID, if applicable
BF22	President 1 name	BF_president1	String	President 1 name
BF23	President 1 suspect ID	BF_president2	String	President 1 ID, if applicable
BF24	President 2 name	BF_president3	String	President 2 name
BF25	President 2 suspect ID	BF_president4	String	President 2 ID, if applicable
BF26	Director name	BF_director1	String	Director's name
BF27	Director suspect ID	BF_director2	String	Director's Suspect ID, if applicable
BF28	Co-director name	BF_director3	String	Co-director's name
BF29	Co-direction suspect ID	BF_director4	String	Co-director's Suspect ID, if applicable
BF30	Additional information	BF_addinfo	String	Additional information on business entity, if applicable
BF31	Investigated	BF_invst	(0)No; (1)Yes; (-99)Missing	Was business entity investigated for involvement in scheme?
BF32	Indicted	BF_indicted	(0)No; (1)Yes; (-99)Missing	Was business entity indicted for involvement in scheme?
BF33	Indictment ID	BF_indictID	String	Indictment ID
BF34	Month of indictment	BF_indctdy	Numeric	Month of indictment

BF34	Day of indictment	BF_indctmnth	Numeric	Day of indictment
BF34	Year of indictment	BF_indctyr	Numeric	Year of indictment
BF35	Month of judgment	BF_jdgmntdy	Numeric	Month of judgment
BF35	Day of judgment	BF_jdgmntmnth	Numeric	Day of judgment
BF35	Year of judgment	BF_jdgmntyr	Numeric	Year of judgment
BF36	Month of sentence	BF_sentdy	Numeric	Month of sentence
BF36	Day of sentence	BF_sentmnth	Numeric	Day of sentence
BF36	Year of sentence	BF_sentyr	Numeric	Year of sentence
BF37	Charges indicted	BF_jur	String	List all charges business entity was indicted with (e.g. mail fraud, money laundering, etc)
BF38	USC provisions (1)	BF_jur2	String	List USC provisions in indictment, if known (e.g. USC 18:345)
BF39	# of charges	BF_trslt	Numeric	Number of charges against business entity, if applicable
BF40	# of counts	BF_apeal	Numeric	Number of counts against business entity, if applicable
BF41	Charges convicted	BF_fine	String	List all charges business entity was convicted for (e.g. mail fraud, money laundering, etc)
BF42	USC provisions (2)	BF_fine2	String	List USC provisions for which convicted, if known (e.g. USC 18:345)
BF43	# charges convicted	BF_otsent	Numeric	Number of charges convicted for, if

				applicable
BF44	# counts convicted	BF_charged1	Numeric	Number of counts convicted of, if applicable
BF45	Jurisdiction of trial	BF_charged2	(1)federal; (2)state; (3)both	Jurisdiction of trial
BF46	Jurisdiction, specified	BF_numch	String	Specify state or federal circuit or county
BF47	Trial result	BF_cnts	(1)Incompetent to stand trial; (2)pled guilty; (3)tried alone and found guilty by jury; (4)tried with co-defendants and found guilty by jury; (5)dismissed due to mistrial or government motion; (6)acquitted; (7)not guilty by reason of insanity; (8)guilty but mentally ill; (9)charges dropped before trial; (10)selected bench trial and convicted; (11)selected bench trial and acquitted	Trial result
BF48	Appeal	BF_convicted1	(1)no appeal; (2)appeal pending; (3)appealed and lost; (4)appealed and won; (5)appealed and retried	Did business entity appeal sentence?

BF49	Court fine	BF_convicted2	(0)No; (1)Yes; (-99)Missing	Did business entity receive a monetary fine as sentence?
BF50	Amount	BF_charcv	Numeric	If yes, specify amount
BF51	Other sentence, specify	BF_cntcv	String	If other sentence type, specify
BF52	Extremist link	BF_polex	(0)No; (1)Yes; (-99)Missing	Does business entity have political extremist links?
BF53	If yes, specify	BF_polex2	(1)Far-rightist; (2)ALF-ELF; (3)Global Jihadi; (4);Local Jihadi; (5);Non-religious/secular Arab nationalist; (6)FARC; (7)Other international terrorist	If political extremist link, specify
BF54	Strength of assocation	BF_bond	(0)0; (1)1: (2)2; (3)3; (4)4;	What is business entity's strength of association to the movement?
BF55	Pro-evidence 1	BF_proevid1	String	Evidence supporting extremist link
BF56	Pro-source 1	BF_prosrc1	String	Source of evidence supporting extremist link

BF57	Pro-evidence 2	BF_proevid2	String	Evidence supporting extremist link
BF58	Pro-source 2	BF_prosrc2	String	Source of evidence supporting extremist link
BF59	Pro-evidence 3	BF_proevid3	String	Evidence supporting extremist link
BF60	Pro-source 3	BF_prosrc3	String	Source of evidence supporting extremist link
BF61	Pro-evidence 4	BF_proevid4	String	Evidence supporting extremist link
BF62	Pro-source 4	BF_prosrc4	String	Source of evidence supporting extremist link
BF63	Pro-evidence 5	BF_proevid5	String	Evidence supporting extremist link
BF64	Pro-source 5	BF_prosrc5	String	Source of evidence supporting extremist link
BF65	Con-evidence 1	BF_conevid1	String	Evidence contrary to extremist link
BF66	Con-source 1	BF_consrc1	String	Source of evidence contrary to extremist link
BF67	Con-evidence 2	BF_conevid2	String	Evidence contrary to extremist link
BF68	Con-source 2	BF_consrc2	String	Source of evidence contrary to extremist link
BF69	Con-evidence 3	BF_conevid3	String	Evidence contrary to extremist link
BF70	Con-source 3	BF_consrc3	String	Source of evidence contrary to extremist link
BF71	Con-evidence 4	BF_conevid4	String	Evidence contrary to extremist link

BF72	Con-source 4	BF_consrc4	String	Source of evidence contrary to extremist link
BF73	Con-evidence 5	BF_conevid5	String	Evidence contrary to extremist link
BF74	Con-source 5	BF_consrc5	Numeric	Source of evidence contrary to extremist link

Assessment Codebook: Coding Issues

(1) Do we count the number of sources that we received from the searcher or the number of sources we actually use? In some cases different sources give the same information.

Answer: Coders should count the total number of sources that were found re the case in the searched materials even if they are duplicates. This is because sometimes it might be difficult to establish specifically which type of source provided the information coded. For example if you have a watch-group publication and a news article that state the same thing, which one do you count/include in the assessment CB? Thus, the answer is to count both.

(2) Please keep in mind the project's protocol to resolve discrepancies and conflicting information regarding open sources (See section on Coding Cases):

(3) Obviously, this codebook MUST be coded LAST- after the other codebooks have been coded.

(4) Coders should also keep in mind the "open ended issues" variable in the assessment codebook, which can be extremely useful to note unsolved issues/problems with the case for future update.

Q#	Variable Name	Variable ID	Values	Description
AF1	ID Number	AF_ID	Numeric	Relational ID (Scheme ID + Masterfile ID)
AF2	# Police documents	AF_police	Numeric	Total number police documents
AF3	# court documents	AF_court	Numeric	Total number court documents
AF4	# other government documents	AF_ogovt	Numeric	Total number other government documents
AF5	# militia watchdog documents	AF_Milwd	Numeric	Total number of Militia Watchdog documents
AF6	# ADL documents	AF_adl	Numeric	Total number of ADL documents
AF7	# SPLC documents	AF_splc	Numeric	Total number of SPLC documents
AF8	# other watch-group documents	AF_opub	Numeric	Total number of other watch-group documents
AF9	# news documents	AF_news	Numeric	Total number of news/journalistic documents
AF10	# scholarly documents	AF_schol	Numeric	Total number of scholarly articles
AF11	# scholarly database documents	AF_#cdb	Numeric	Total number of scholarly database documents
AF12	# non-scholarly database documents	AF_nschl	Numeric	Total number of non-scholarly database documents
AF13	# websites	AF_web	Numeric	Total number of Internet websites
AF14	# key informants	AF_keyinf	Numeric	Total number of key informants
AF15	# other sources	AF_osour	Numeric	Total number of other sources

Q#	Variable Name	Variable ID	Values	Description
AF16	Total # documents/sources	AF_source	Numeric	Total number of documents/sources
AF17	Reliability	AF_reliab	(1)Complete reliability; (2)Usually reliable; (3)Fairly reliable; (4)Not usually reliable; (5)Unreliable; (6)Can't judge; (-99)Missing	Reliability Assessment
AF18	Evaluation	AF_eval	(1)Outstanding; (2)Very good; (3)Good; (4)Fair; (5)Poor;	Evaluation of open sources
AF19	Quality: Scale 1-50	AF_rate	Numeric	Scale quality
AF20	Open ended issues	AF_ issues	String	Open ended issues
AF21	Date of last search	AF_searchdate	MM/DD/YY	Date of last open-source search
AF22	News-library articles	AF_newslib	(1)Articles DO NOT need purchased (2)Articles need purchased (3)Articles have been purchased	News-library articles to be purchased

BIBLIOGRAPHY

Abadinsky, H. (2006). *Organized Crime*. Belmont, CA: Wadsworth Publishing.

Abrams, R. (2005). The Material Support Terrorism Offenses: Perspectives Derived from the (Early) Model Penal Code. *Journal of National Security Law & Policy, 1*(5), 5-35.

Adamoli, S., Di Nicola, A., Savona, E. U., & Zoffi, P. (1998). *Organized crime around the world.* Helsinki, Finland: European Institute for Crime Prevention and Control.

Akers, R. L. (1998). *Social Learning and Social Structure: A General Theory of Crime and Deviance*. Boston, MA: Northeastern University Press.

Albanese, J. (1995). Where organized and white-collar crime meet: Predicting the infiltration of legitimate businesses. In J. Albanese (Ed.), *Contemporary issues in organized crime*. New York, NY: Criminal Justice Press.

Albanese, J. (2005). Fraud: The characteristic crime of the twenty-first century. *Trends in Organized Crime, 8*(4), 6-14.

Albert, R., & Barabasi, A.L. (2002). Statistical mechanics of complex networks. *Reviews of Modern Physics, 74*(1), 47-97.

Alexander, M.C., & Danowski, J. A. (1990). Analysis of an ancient network: personal communication and the study of social structure in a past society. *Social Networks, 12*, 313-335.

Anti-Defamation League (2003, May 13). The Tax Protest Movement Since 9/11. *ADL Report*. Retrieved from: http://www.adl.org/learn/extremism_in_america_updates/movements/tax_protest_movement/tax_protest_update_030513.htm

Anti-Defamation League (2005). *Extremism in America: Tax Protest Movement*. Retrieved from: http://www.adl.org/learn/ext_us/TPM.asp?xpicked=4&item=21

Antonopoulos, G. A. (2008), 'The Greek Connection(s): The Social Organisation of the Cigarette Smuggling Business in Greece', *European Journal of Criminology, 5,* 263–88.

Ashcroft, J. (2004, June 8). *Statement of John Ashcroft, Attorney General, before the Committee on the Judiciary*. United States Senate Oversight of the Department of Justice: Terrorism and Other Topics. Retrieved from http://www.fas.org/irp/congress/2004_hr/060804ashcroft.html.

Atran, S. (2003). Genesis of Suicide Terrorism. *Science, 299* (5612), 1534 – 1539.

Baker W. E., & Faulkner, R. R. (1993). The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment Industry. *American Sociological Review, volume 58*(6), 837-860.

Bandura, A. (1977). *Social Learning Theory*. Englewood Cliffs, NJ: Prentice Hall.

Barkun, M. (1996). Religion, militias and Oklahoma City: The mind of conspiratorialists. *Terrorism and Political Violence, 8*(1), 50- 64.

Barnes, R. (2010, June 22). Supreme Court upholds ban on 'material support' to foreign terrorist groups. *The Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2010/06/21/AR2010062101811.html

Beare M. E., (2003) (Ed.). *Critical reflections on transnational organized crime, money laundering, and corruption*. Toronto, CA: University of Toronto Press.

Bearman, P. S., Moody, J., & Stovel, K. (2004). Chains of Affection: The Structure of Adolescent Romantic and Sexual Networks. *American Journal of Sociology, 110*(1), 44-91.

Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy, 76*, 169-217.

Beirich, H. (2004). Talking Tough: One of the largest "Patriot" conferences in years is marked by heated calls for revolution and violent resistance. *Southern Poverty Law Center, SPLC Intelligence Report*, Spring 2004. Retrieved from: www.splcenter.org/intel/intelreport/article.jsp?aid=380&printable=1

Belli, R., & Freilich, J. D. (2009). Situational Crime Prevention and Non-Violent Terrorism: A "Soft" Approach against Ideologically Motivated Tax Refusal. In J. D. Freilich & G. R. Newman. *Reducing Terrorism Through Situational Crime Prevention. Crime Prevention Studies, 25*, 173-206.

Benson, M.L. & Moore, E. (1992). Are white-collar offenders and common criminals the same? An empirical and theoretical critique of a recently proposed general theory of crime. *Journal of Research in Crime and Delinquency, 29*, 251-272.

Bequai, A. (2002). White collar crime: A handmaiden of international tech terrorism. *Computers & Security, 21*(6), 514-519.

Berdal M., & Serrano M. (2002). *Transnational Organized Crime & International Security. Business as usual?* Boulder, CO: Lynne Rienner Publishers.

Biagioli, A. (2008). Financial crime as a threat to the wealth of nations: A cost-effectiveness approach. *Journal of Money Laundering Control, 11*(1), 88-95.

Biersteker, T. J., & Eckert, S. E. (2008a). Introduction: the challenge of terrorist financing. In T. J. Biersteker, & S. E. Eckert (Eds.). *Countering the financing of terrorism* (pp. 1-16). New York, NY: Routledge.

Biersteker, T. J., & Eckert, S. E. (2008b). Conclusion: taking stock of efforts to counter the financing of terrorism and recommendations for the way forward. In T. J. Biersteker,

& S. E. Eckert (Eds.). *Countering the financing of terrorism* (pp. 289-304). New York, NY: Routledge.

Biersteker, T.J., Eckert, S.E., & Romaniuk, P. (2008). International initiatives to combat the financing of terrorism. In T. J. Biersteker, & S. E. Eckert (Eds.). *Countering the financing of terrorism* (pp. 234-259). New York, NY: Routledge.

Block, A. A., & Griffin, P. A. (2002). Transnational financial crime: Crooked lawyers, tax evasion, and securities fraud. *Journal of Contemporary Criminal Justice, 18*(4), 381-393.

Boissevan, J. (1974), *Friends of friends: Networks, Manipulators and Coalitions*. Oxford, UK: Blackwell.

Borgatti, S. P., Everett, M. G., & Freeman, L. C. (2002). *UCINET for Windows: Software for Social network Analysis.* Harvard, MA: Analytic Technologies.

Borgatti, S.P., & Everett, M.G. (1999). Models of Core/Periphery Structures. *Social Networks, 21*, 375-395.

Bovenkerk, F., & Chakra, B. A. (2007). Terrorism and organised crime. In L. Holmes (Ed.), *Terrorism, organised crime and corruption: networks and linkages,* (pp. 29-41). Northampton, MA: Edward Elgar Publishing.

Breinholt, J. (2005). *Taxing terrorism from Al Capone to Al Qaida: Fighting violence through financial regulation*. [PDF Document]. Retrieved from http://www.strategycenter.net/docLib/20061007_TaxingTerrorismVol1.pdf.

Browning, L. (2008, April 9). US says it will increase efforts against 'tax defiers'. *The New York Times.* Retrieved from http://www.nytimes.com/2008/04/09/business/09tax.html?_r=1&fta=y.

Bruinsma, G., & Bernasco, W. (2004). Criminal groups and transnational illegal markets. *Crime, Law, and Social Change*, *41*, 79-94.

Burrows, J., & Hopkins, M. (2005). Business and crime. In Tilley, N. (Ed.) (2005). *Handbook of Crime Prevention and Community Safety,* (pp. 486-515). Devon, UK: Willan Publishing.

Burt, R. S. (1984). Network items and the general social survey. *Social Networks, 6,* 293-340.

Burt, R. S. (2001). Structural Holes Versus Network Closure as Social Capital. In N. Lin, K. Cook, & R. S. Burt (Eds.). *Social Capital: Theory and Research,* (pp. 31-56). Hawthorn, NY: Aldine de Gruyter.

Burt, R. S. (2005). *Brokerage and closure: An introduction to social capital.* Oxford, UK: Oxford University Press.

Carrington, P. J., Scott, J., & Wasserman, S. (2005). *Models and Methods in Social Network Analysis*. New York, NY: Cambridge University Press.

Chermak, S.M. (2002). *Searching for a Demon: The Media Construction of the Militia Movement.* Boston, MA: Northeastern University Press.

Chermak, S.M., Freilich, J.D., Parkin, W.S., & Lynch. J.P. (1). Comparing data sources of American terrorism and extremist crime: Investigating selectivity bias. *Journal of Quantitative Criminology.* Forthcoming.

Chermak, S. M., Freilich, J. D., & Shemtob, Z. (2009). Law enforcement training and the domestic far right. *Criminal Justice and Behavior, 36*(12), 1305-1322.

Chesney R. (2005). The Sleeper Scenario: Terrorism-Support Laws and the Demands of Prevention. *Harvard Journal on Legislation, 42*(1), 1-89.

Clarke, R. V. G. (1980). 'Situational' crime prevention: Theory and practice. *British Journal of Criminology, 20*(2), 136-147.

Clarke, R. V. G. (1997). *Situational crime prevention: Successful case studies*. Guilderland, NY: Harrow and Heston.

Clarke, R. V. G. (1999). *Hot products: Understanding, anticipating and reducing demand for stolen goods*. London, UK: Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate.

Clarke, R. V. G., & Felson, M. (1993). *Routine activity and rational choice*. New Brunswick, NJ: Transaction Publishers.

Clarke, R. V.G., & Homel, R.. (1997). A revised classification of situational crime prevention techniques. In S. P. Lab. (Ed). *Crime prevention at a crossroads*. Highland Heights, KY: Anderson Publishing.

Clarke, R. V. G., & Newman, G. R. (2006). *Outsmarting terrorists*. Westport, CT: Praegers Security International.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review, 44*, 588-605.

Coles, N. (2001). It's not what you know – it's who you know that counts: Analysing serious crime groups as social networks. *British Journal of Criminology, 41*(4), 580-594.

Collins, R. (1988). *Theoretical Sociology*. New York, NY: Harcourt Brace Jovanovich.

Compin, F. (2008). The role of accounting in money laundering and money dirtying. *Critical Perspectives on Accounting, 19*(5), 591-602.

Corcoran, J. (1990). *Bitter harvest, Gordon Kahl and the Posse Comitatus: Murder in the Heartland*. New York: Penguin Books.

Cords, D. (2005). Tax Protestors and Penalties: Ensuring Perceived Fairness and Mitigating Systemic Costs. *Brigham Young University Law Review, 6*, 1515-1571.

Cornish, D. (1994). The Procedural Analysis of Offending and its Relevance for Situational Prevention. *Crime Prevention Studies 3,* 151-196.

Cornish, D. B., & Clarke, R.V.G. (1986). Situational prevention, displacement of crime and rational choice theory. In K. Heal, & G. Laycock, (Eds.), *Situational crime prevention: From theory into practice* (pp. 1-16). London: Her Majesty's Stationery Office.

Cornish, D. B., & Clarke, R.V.G. (2002). Analyzing organized crimes. In A. R. Piquero, & S. G. Tibbetts (Eds.), *Rational Choice and Criminal Behavior: Recent Research and Future Challenges* (pp. 41-64). New York, NY: Routledge.

Cornish, D. B., & Clarke, R.V.G. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. In M. Smith, & D. B. Cornish (Eds.), *Crime Prevention Studies: Theory for situational crime prevention, 16*, 41-96.

Cornish, D. B., & Clarke, R.V.G. (2008). The rational choice perspective. In Wortley, R. & Mazerolle, L. (Eds.). *Environmental Criminology and Crime Analysis*, (pp. 21-47). Collumpton, UK: Willan Publishing.

Croall, H. (2001). *Understanding white collar crime*. Buckingham, UK: Open University Press.

Curtis, R.,& Wendel, T. (2000). Toward the development of a typology of illegal drug markets. In Natarajan, M., & Hough, M. (Guest Eds.). *Illegal drug markets: from research to policy. Crime Prevention Studies, 11,* 121-152.

de Armond P. (1996). *Christian Patriots At War with the State.* Retrieved from http://www.publicgood.org/reports/belief/

de Nooy, W., Mrvar, A., & Batagelj, V. (2005). *Exploratory Social Network Analysis with Pajek*. New York, NY: Cambridge University Press.

Dean, H., & Melrose M., (1996). Unravelling citizenship: The significance of social security benefit fraud. *Critical Social Policy, 16*(48), 3-31.

deKieffer, D. E. (2008). Trade diversion as a fund raising and money laundering technique of terrorist organizations. In T. J. Biersteker, & S. E. Eckert (Eds.). *Countering the financing of terrorism* (pp. 150-173). New York, NY: Routledge.

Di Nicola, A., & Zoffi, P. (2005). Italian lawyers and criminal clients. Risks and countermeasures. *Crime, Law, & Social Change, 42*: 201-225.

Dishman, C. (2005). The leaderless nexus: When crime and terror converge. S*tudies in Conflict & Terrorism, 28*(3), 237-252.

Doig, A. (2006). *Fraud*. Collumpton, UK: Willan Publishing.

Doreian, P., Batafelj, V., Freligoj, A. (2005). *Generalized blockmodeling.* Cambridge, UK: Cambridge University Press.

Dugan, L., LaFree, G., & Fogg, H. (2006). A First Look at Domestic and International Global Terrorism Events, 1970-1997. In S. Mehrotra, D.D. Zeng, H. Chen, B. Thuraisingham, and F. Wang (Eds.) *Intelligence and Security Informatics, IEEE International Conference on Intelligence and Security Informatics, ISI 2006 San Diego, CA, USA May 2006 Proceedings*. Berlin, Germany: Springer-Verlag.

Eaton, L. (2007, October 22). Judge declares mistrial in Muslim charity case, *The New York Times*. Retrieved from http://www.nytimes.com/2007/10/22/world/americas/22iht-22holy.8005339.html

Eckert, S. (2008). The US regulatory approach to terrorist financing. In In T. J. Biersteker, & S. E. Eckert (Eds.). *Countering the financing of terrorism* (pp. 209-233). New York, NY: Routledge.

Ehrenfeld, R. (2003). *Funding Evil: How Terrorism is Financed – and How to Stop it*. Chicago, IL: Bonus Books.

Ekblom, P. (2007). Making offenders richer. *Imagination for crime prevention: Essays in honour of Ken Pease. Crime Prevention Studies, 21*, 41-57.

Ekblom, P., & Tilley, N. (2000). Going equipped: Criminology, situational crime prevention and the resourceful offender. *British Journal of Criminology, 40*(3), 376-398.

Erickson, B. H. (1981). Secret Societies and Social Structure. *Social Forces, 60*(1), 188-210.

Felson, M. (1998). *Opportunity makes the thief: Practical theory of crime prevention*. London, UK: Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate.

Felson, M. (2002). *Crime and Everyday Life*. Thousand Oaks, CA: Sage Publications.

Felson, M. (2003). The Process of Co-offending, *Crime Prevention Studies: Theory for Practice in Situational Crime Prevention*, 149-168.

Fijnaut, C., & Paoli, L. (Eds.)(2004). *Organised Crime in Europe. Concepts, Patterns, and Control Policies in the European Union and Beyond*. Dordrecht, NL: Springer.

Flynn, K. & Gerhardt, G. (1995). *The silent brotherhood: The chilling inside story of America's violent anti-government militia movement*. New York, NY: Signet Penguin.

Frank, O., & Strauss, D. (1986). Markov graphs. *Journal of the American Statistical Association, 81*, 832-842.

Freeman, L. C. (1979). Centrality in Social Networks: Conceptual Clarification. *Social Networks, 1*, 215-239.

Freeman, L. C. (2004). *The development of social network analysis: A study in the sociology of science*. Vancouver, CA: Empirical Press.

Freeman, L.C. (2005). Graphic techniques for exploring social network data. In In P.J. Carrington, J. Scott, & S. Wasserman (eds.), *Models and Methods in Social Network Analysis* (pp. 248-269). New York, NY: Cambridge University Press.

Freilich, J.D., & Chermak, S. (2009). Preventing Deadly Encounters between Law Enforcement and American Far-Rightists. In J. D. Freilich & G. R. Newman. *Reducing Terrorism Through Situational Crime Prevention. Crime Prevention Studies, 25*, pp. 141-172.

Freilich, J.D., Chermak, S., & Caspi, D. (2009a). Critical events in the life trajectories of domestic extremist white supremacist groups: A case study analysis of four violent organizations. *Criminology and Public Policy, 8*(3), 497-530.

Freilich, J.D., Chermak, S., & Simone, J. (2009b). Surveying American State Police Agencies about Terrorism Threats, Terrorism Sources, and Terrorism Definitions. *Terrorism and Political Violence, 21*(3), 450-475.

Freilich, J.D. & Pridemore, W.A. (2006). Mismeasuring militias: Limitations of advocacy group data and of state-level studies of paramilitary groups. *Justice Quarterly, 23*(1): 147-162.

Friedrichs, D. (2004). Enron Et Al.: Paradigmatic White Collar Crime Cases for the New Century. *Critical Criminology, 12*(2), 113-132.

Gallant, M. M. (2007). Tax and terrorism: A new partnership? *Journal of Financial Crime, 14*(4), 453-459.

Garton, L., Haythornthwaite, C., & Wellman, B. (1997). Studying online social networks. *Journal of Computer Mediated Communications, 3* (1), Retrieved from http://jcmc.indiana.edu/vol3/issue1/garton.html.

Gershman, B. L. (1999). *Prosecutorial misconduct*. Belmont, CA: West Publishing Company.

Gill, M. (2005). Reducing the capacity to offend: restricting resources for offending. In Tilley, N. (Ed). *Handbook of Crime Prevention and Community Safety,* (pp. 306-328). Devon, UK: Willan Publishing.

Gill, M. (Ed.) (1994). *Crime at Work: Studies in Security and Crime Prevention.* Leicester, UK: Perpetuity Press.

Giraldo, J. K., & Trinkunas, H. A. (2007). The political economy of terrorism financing. In J. K. Giraldo, & H. A. Trinkunas, (Eds.). *Terrorism financing and state responses: A comparative perspective*, (pp. 7-20). Stanford, CA: Stanford University Press.

Glueck, S., & Glueck, E. (1950). *Unraveling Juvenile Delinquency*. New York, NY: The Commonwealth Fund.

Goodreau, S. M., (2007). Advances in exponential random graph (p *) models applied to a large social network, *Social Networks*, 29, 2-231.

Goodreau, S. M., Kitts, J. A., & Morris, M., (2009). Birds of a Feather, Or Friend of a Friend? Using Exponential Random Graph Models to Investigate Adolescent Social Networks, *Demography*, *46* (1), 103-125.

Gottfredson, M.R., & Hirschi, T. (1990). A general theory of crime. Stanford, CA: Stanford University Press.

Grabbe, J. O. (2002, May 13). In Praise of Hawala. *The Laissez Faire Electronic Times*. Retrieved from http://freedom.orlingrabbe.com/lfetimes/hawala.htm.

Granovetter, M. (1973). The strength of weak ties. *American Journal of Sociology, 78*, 1360-1380.

Gregory, F. (2003). Classify, Report and Measure: the UK Organised Crime Notification Scheme. In A. Edwards and P. Gill (Eds). *Transnational Organised Crime: Perspectives on Global Security,* (pp. 78–96). London. UK: Routledge.

Gruenewald, J., Freilich, J. D., & Chermak, S. (2008). An overview of the domestic far-right and its criminal activities. In B. Perry, & R. Blazak. (Eds). *Hate crime: Issues and perspectives*. New York, NY: Praeger.

Gunaratna, R. (2002). *Inside Al Qaeda: Global Network of Terror*. New York, NY: Columbia University Press.

Gunaratna, R. (2008). The evolution of Al Qaeda. In T. J. Biersteker, & S. E. Eckert (Eds.). *Countering the financing of terrorism* (pp. 47-62). New York, NY: Routledge.

Gunning, J. (2008). Terrorism, charities and diasporas: Contrasting the fundraising practices of Hamas and al Qaeda among Muslims in Europe. In T. J. Biersteker, & S. E. Eckert (Eds.). *Countering the financing of terrorism* (pp. 93-125). New York, NY: Routledge.

Haller, M. H. (1990). Illegal enterprise: A theoretical and historical interpretation, *Criminology, 28*, 207-235.

Hamilton-Smith, N. & Kent, A. (2005). The prevention of domestic burglary. In Tilley, N. (Ed.) *Handbook of Crime Prevention and Community Safety*, (pp. 417-457). Devon, UK: Willan Publishing.

Hamm, M. S. (2007). *Terrorism as crime: from Oklahoma City to Al-Qaeda and beyond*. New York, NY: New York University Press.

Hamm, M. S., & Van de Voorde, C. (2005). Crimes committed by terrorist groups: Theory, research, and prevention. *Trends in Organized Crime, 9*(2), 18-51.

Handcock, M.S. (2003) Assessing degeneracy in statistical models of social networks. *Center for statistics and the social sciences working paper No. 39.*

Hanneman, R. A., & Riddle, M. (2005). *Introduction to social network methods*. Retrieved from http://faculty.ucr.edu/~Hanneman and Riddle/.

Hardister, A. (2003).Can we buy peace on earth? The price of freezing terrorist assets in a Post-September 11 World, *North Carolina Journal of International Law and Commercial Regulation, 28,* 605-661.

Hargens, L.L. (2000). Using the literature: reference networks, reference contexts, and the social structure of scholarship. *American Sociological Review, 65*, 846-865.

Harrigan, N. (2008). *PNet for dummies: An introduction to estimating exponential random graph (p*) models with PNet. Version 1.04.* [PDF document]. Published on the PNet website at the University of Melbourne. Retrieved from http://www.sna.unimelb.edu.au/pnet/pnet.html#download

Heller, R. (1997). Selective prosecution and the federalization of criminal law: the need for meaningful judicial review of prosecutorial discretion. *University of Pennsylvania Law Review, 145*, 1039-1358.

Hewitt, C. (2003). *Understanding terrorism in America: From the Klan to Al Qaeda*. New York, NY: Routledge.

Hirschi, T. (1969). *Causes of delinquency*. Berkeley, CA: University of California Press.

Hobbs, D. (1994). Professional and organised crime in Britain. In M. Maguire, R. Morgan, & R. Reiner (Eds.). *The Oxford Handbook of Criminology,* (pp. 441-468). Oxford, UK: Clarendon Press.

Hoffman, B. (2006). *Inside Terrorism (2nd Ed.)*. New York, NY: Columbia University Press.

Horgan, J. (2008). Interviewing Terrorists: A Case for Primary Research. In Chen, H., Reid, E. Sinai, J., Silke, A., Ganor, B. (Eds.). *Terrorism Informatics: Knowledge Management and Data Mining for Homeland Security*, (pp. 27-50), New York, NY: Springer.

Horgan, J., & Taylor, M. (1999). Playing the 'Green card'--financing the provisional IRA: Part 1. *Terrorism & Political Violence, 11*(2), 1-38.

Horgan, J., & Taylor, M. (2003). Playing the 'green card'-- financing the provisional IRA: Part 2. *Terrorism & Political Violence, 15*(2), 1-60.

Huisman, M. & Van Duijn, M.A.J. (2005). Software for social network analysis. In P.J. Carrington, J. Scott, & S. Wasserman (eds.), *Models and Methods in Social Network Analysis* (pp. 270-316). New York, NY: Cambridge University Press.

Hutchinson, S., & O'malley, P. (2007). A crime-terror nexus? Thinking on some of the links between terrorism and criminality. *Studies in Conflict & Terrorism, 30*(12), 1095-1107.

Internal Revenue Service (IRS) (2006). *IRS Announces "Dirty Dozen" Tax Scams for 2006.* Retrieved from: http://www.irs.gov/newsroom/article/0,,id=154293,00.html.

Internal Revenue Service (IRS) (2008). *Phishing Scams, Frivolous Arguments Top the 2008 "Dirty Dozen" Tax Scams.* Retrieved from: http://www.irs.gov/newsroom/article/0,,id=180075,00.html.

Jacobs, J. (2007, June 17). Follow the money. Paul Wolfowitz was right: To stop terrorists, cut off their money supply. *MSNBC News*. Retrieved from http://www.msnbc.msn.com/.

Johnston, D. & Risen, J. (2003, February 23). Lone Terrorists May Strike in the U.S., Agencies Warn, *New York Times*, p. 15.

Juergensmeyer, M. (2001). *Terror in the Mind of God: the Global Rise of Religious Violence*. Berkeley, CA: University of California Press.

Kane, J., & Wall, A. (2005). *Identifying the links between white-collar crime and terrorism.* NIJ-Sponsored Study Final Grant Report, Grant No.2003-IJ-CX-1018, National Institute of Justice, Office of Justice Programs, US Department of Justice.

Kelly, R. J. (1999). *The upperworld and the underworld: Case studies of racketeering and business infiltrations in the United States*. New York, NY: Kluwer Academic.

Kenney, M. (2007). *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation*. University Park, PA: The Pennsylvania State University.

Kim, Y. (2007). Using Spatial Analysis for Monitoring Fraud in a Public Delivery Program. *Social Science Computer Review, 25*(3), 287-301.

Kleemans, E. R. (2007). Organized crime, transit crime, and racketeering, *Crime and Justice: A Review of Research, 35,* 163-215.

Klerks, P. (2003). The network paradigm applied to criminal organisations: theoretical nitpicking or a relevant doctrine for investigators? Recent developments in the Netherlands. *Connections 24*(3), 53–65.

Knoke, D. (1990). Networks of political action: toward theory construction. *Social Forces, 68*, 1041–63.

Knoke, D., & Yang, S. (2008). Social network analysis, 2nd ed. *Series: Quantitative Applications in the Social Sciences*. Thousand Oaks, CA: Sage.

Koehly, L. M., & Pattison, P. (2005). Random graph models for social networks: multiple relations or multiple raters. In Carrington, P. J., Scott, J., & Wasserman, S. (Eds.). *Models and Methods in Social Network Analysis*, (pp. 162-189). New York, NY: Cambridge University Press.

Kossinets, G. (2008). Effects of missing data in social networks. *Social Networks, 28*, 247-268.

Krackhardt, D. (1987). Cognitive social structures. *Social Networks, 9*, -109-134.

Krebs, V. E. (2002a). Mapping networks of terrorist cells. *Connections, 24*(3), 43.

Krebs, V. E. (2002b). Uncloaking terrorist networks. *First Monday, 7*(4). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/941/863

Lacoste, J. & Tremblay, P. (2003). Exploring Target Attractiveness in Vandalism. In M. J. Smith, & D. B. Cornish. (Eds). *Theory for Practice in Situational Crime Prevention*, 197-236.

LaFree, G. & Dugan, L. (2004). How Does Studying Terrorism Compare to Studying Crime? *Sociology of Crime, Law and Deviance, 5*, 53-74.

LaFree, G., & Dugan, L. (2007). Introducing the Global Terrorism Database. *Terrorism and Political Violence, 19,* 181-204.

Laumann, E.O., Marsden, P.V., & Prensky, D. (1992). The boundary specification problem in network analysis. In Freeman, L.C., White, D. R., & Romney, A.K. (Eds.). *Research methods in social network analysis,* (pp. 61-87). New Brunswick, NJ: Transaction Publishers.

Lavoie, D. (2001, November 07). Boston man arrested in terror money network. *The Associated Press*. Retrieved from http://www.boston.com/news/daily/07/attacks_boston_money.htm.

Leenders, R.T. (1997). Longitudinal behavior of network structure and actor attributes: Modeling interdependence of contagion and selection. In E. Doreian, & E.N. Stokman (Eds.). *Evolution of social networks*, (pp. 165-184). Amsterdam, NL: Gordon and Breach, Amsterdam.

Levi, M. (1994). Masculinities and *white-collar crime*. In T. Newburn & B. Stanko (Eds.), *Just boys doing business* ,(pp. 234-252). London, UK: Routledge.

Levi, M. (2003). Organised and financial crime. In T. Newburn (Ed.) *Handbook of Policing,* (pp. 443-466). Collumpton. UK: Willan Publishing.

Levi, M. (2008a). Lessons for countering terrorist financing from the war on serious and organized crime. In In T. J. Biersteker, & S. E. Eckert (Eds.). *Countering the financing of terrorism* (pp. 260-288). New York, NY: Routledge.

Levi, M., (2008b). Organised Fraud: Unpacking Research on Networks and Organisation. *Criminology and Criminal Justice, 8*(4): 389-420.

Levi, M., Nelen, M. & Lankhorst, F. (2005). Lawyers as crime facilitators in Europe: An introduction and overview. *Crime, Law & Social Change, 42*(2-3), 117-121.

Levi, M., & Reuter, P. (2006). Money laundering. *Crime and Justice, 34,* 289-376.

Levitas, D. (2002). *The Terrorist Next Door: The Militia Movement and the Radical Right.* New York, NY: St. Martin's Press.

Lin, N. (2008). Building a network theory of social capital. In Lin, N., Cook, K., Burt, & R.S. (Eds.). *Social Capital: Theory and Research,* (pp. 3-30). New Brunswick, NJ: Transaction Publishers.

Makarenko, T. (2004). The Crime–Terror Continuum: Tracing the Interplay between Transnational Organised Crime and Terrorism. *Global Crime, 6*(1), 129-145.

Malm, A. (2007). Marijuana cultivation in British Columbia: Using spatial and social network analysis techniques to inform evidence-based policy and planning. (ProQuest Information & Learning). *Dissertation Abstracts International. Section A: Humanities and Social Sciences, 68* (3), 1170-1170.

Malm, A., Bichler, G., & Van De Walle, S. (2010). Comparing the ties that bind criminal networks: Is blood thicker than water? *Security Journal, 23*(1): 52-74.

Manning, G. (2005). *Financial investigation and forensic accounting*. Boca Raton, FL: CRC Press.

Marsden, P. (2005). Recent developments in network measurement. In Carrington, P. J., Scott, J., & Wasserman, S. (Eds). *Models and Methods in Social Network Analysis,* (pp. 8-30). New York, NY: Cambridge University Press.

Masciandaro, D., Takats, E., Unger, B. (2007). *Black Finance: the Economics of Money Laundering*. Cheltenham, UK: Edward Elgar Publishing Limited.

McCulloch, J., & Pickering, S., (2005). Suppressing the Financing of Terrorism: Proliferating State Crime, Eroding Censure and Extending Neo-Colonialism. *British Journal of Criminology*, *45*, 470-486.

McGarrell, E.F., Freilich, J. D. & Chermak, S. M. (2007). Intelligence-led policing as a framework for responding to terrorism. *Journal of Contemporary Criminal Justice 23*(2),142-158.

McGloin, J.M. (2004). Associations among criminal gang members as a defining factor of organization and as a predictor of criminal behavior: The gang landscape of Newark, New Jersey. Ph.D. dissertation, Rutgers The State University of New Jersey - Newark, United States -- New Jersey. Retrieved February 6, 2011, from Dissertations & Theses: Full Text. (Publication No. AAT 3131756).

McGloin, J.M. (2005). Policy and Intervention Considerations of a Network Analysis of Street Gangs, *Criminology and Public Policy, 4* (3), 607-636.

McGloin, J.M., Sullivan, C., Piquero, A., & Bacon, S. (2008). Investigating the stability of co-offending and co-offenders among a sample of youthful offenders. *Criminology, 46*, 155-188.

McNab, J.J. (2006). Schemes, Scams, and Cons, Updated [PDF Document]. *Supplemental Report to the 2001 Committee Testimony, United States Senate Committee on Finance*. Retrieved from http://deathandtaxes.com/.

McNab, J.J. (2010). 'Sovereign' Citizen Kane: the conspiratorial ideology behind a double cop-killer is spreading rapidly. *Intelligence Report, 139.* Southern Poverty Law Center (SPLC).

McPherson, M., Smith-Lovin, M., & Cook, J. (2001). Birds of a feather: Homophily in Social Networks. *Annual Review of Sociology, 27*, 415-444.

Merari, A. (1991). Academic research and government policy on terrorism. *Terrorism and Political Violence, 3*(1), 88-102.

Middleton, D., & Levi, M. (2005). The role of solicitors in facilitating 'Organized Crime': Situational crime opportunities and their regulation. *Crime, Law & Social Change, 42*(2-3), 123-161.

Mishal, S., & Sela, A. (2000). *The Palestinian Hamas*. New York, NY: Columbia University Press.

Morselli, C. (2009). *Inside Criminal Networks*. New York, NY: Springer.

Morselli, C., & Giguere, C. (2006). Legitimate strengths in criminal networks. *Crime, Law, & Social Change, 45*, 185-200.

Morselli, C., Giguere, C., & Petit, K. (2007). The efficiency/security trade-off in criminal networks. *Social Networks, 29,* 143-153.

Morselli, C., & Kazemian, L. (2004). Scrutinizing RICO. *Critical Criminology, 12*, 351-369.

Morselli, C., & Roy, J. (2008). Brokerage qualifications in ringing operations. *Criminology, 46*(1), 71-98.

Napoleoni, L. (2005). *Terror incorporated: tracing the dollars behind the terror networks.* New York, NY: Seven Stories Press.

Nardo, M. (2004). Mapping the trails of financial crime. *Journal of Financial Crime, 12*(2), 139-143.

Natarajan, M. (2006). Understanding the structure of a large heroin distribution network: A quantitative analysis of qualitative data. *Journal of Quantitative Criminology, 22*(2), 171-192.

National Commission on Terrorist Attacks Upon the United States (2004). *The 9/11 Commission Report.* [PDF Document]. Retrieved from http://govinfo.library.unt.edu/911/report/index.htm.

Naylor, R.T. (1997). Mafia, markets, and myths: On the theory and practice of enterprise crime. *Transnational Organized Crime, 3*, 1–45.

Naylor, R. T. (2000). Economic and organized crime: Challenges for criminal justice. *Strategic Issues Series*. Department of Justice, Canada: Research and Statistics Division. Retrieved from dsp-psd.pwgsc.gc.ca/Collection/J3-4-02-12E.pdf.

Nelken, D. (2002). White Collar Crime. In M. Maguire, R. Morgan & R. Reiner (Eds.), *The Oxford Handbook of Criminology, 3rd ed.,* (pp. 844-877). New York, NY: Oxford University Press.

Newman, G. R., Clarke, R.V.G., & Shoham, S. G., (Eds.) (1997). *Rational Choice and Situational Crime Prevention: Theoretical Foundations*. Aldershot, UK: Ashgate.

Newman, G.R., & Clarke, R.V.G.. (2003). *Superhighway robbery: Preventing E-commerce crime*. Portland, OR: Willan Publishing.

Niggli, M.A. (2007). Rational Choice and the Legal model of the Criminal. In G. R. Newman, R.V. G. Clarke, and S.G. Shoam (Eds). *Rational Choice and Situational Crime Prevention: Theoretical Foundations.* Aldershot, UK: Ashgate.

Norton, A.R. (2009). *Hezbollah: A short history*. Princeton, NJ: Princeton University Pres.

Öhlén, M. (2009, October 26). Al-Barakaat has been removed from terror list. *Stockholm News*. Retrieved from http://www.stockholmnews.com/more.aspx?NID=4209.

Passas, N. (2003). *Informal Value Transfer Systems, Money Laundering and Terrorism.* Washington, DC: Report to the National Institute of Justice (NIJ) and the Financial Crimes Enforcement Network (FINCEN).

Passas, N. (2007).Terrorism financing mechanisms and policy dilemmas. In J. K. Giraldo, & H. A. Trinkunas, (Eds.). *Terrorism financing and state responses: A comparative perspective,* (pp. 21-38). Stanford, CA: Stanford University Press.

Pattison, P., & Wasserman, S. (1999). Logit models and logistic regressions for social networks: II. Multivariate relations. *British Journal of Mathematical and Statistical Psychology, 52,* 169-193.

Picarelli, J. T., & Shelley, L. I. (2007). Organized crime and terrorism. In J. K. Giraldo, & H. A. Trinkunas, (Eds.). *Terrorism financing and state responses: A comparative perspective*, (pp. 39-55). Stanford, CA: Stanford University Press.

Pitcavage, M. (1996). "*Patriot" Profiles #1: Joe Holland, Calvin Greenup, and the Anti-Tax Militia*. Anti-Defamation League, The Militia Watchdog. Retrieved from http://www.adl.org/mwd/holland.asp.

Pitcavage, M. (1999). *Old Wine, New Bottles: Paper Terrorism, Paper Scams and Paper "Redemption."* Militia Watchdog Publications. Retrieved from: http://www.adl.org/mwd/redemption.asp.

Pitcavage, M. (2001). Camouflage and Conspiracy: the Militia Movement from Ruby Ridge to Y2K. *American Behavioral Scientist, 44*(6), 957-981.

Podolny, J.M. (1993). A status-based model of market competition. *American Journal of Sociology, 98*, 829-872.

Podolny, J.M., & Stuart, T.E. (1995). A role-based ecology of technological change. *American Journal of Sociology, 100,* 1224-1260.

Raphaeli, N. (2003). Financing of terrorism: Sources, methods, and channels. *Terrorism & Political Violence, 15*(4), 59-82.

Reed, G. E., & Yeager, P. C. (1996). Organizational offending and neoclassical criminology: Challenging the reach of a general theory of crime. *Criminology, 34,* 357-382.

Reiss, A. J. (1986). Co-offender influences on criminal careers. In A. Blumstein, J. Cohen, J. A. Roth, & C.A. Visher (Eds.). *Criminal Careers and Career Criminals, Vol. 2*. Washington, DC: National Academy Press.

Reiss, A. J., & Farrington, D.F. (1991). Advancing knowledge about co-offending: Results from a prospective longitudinal survey of London males, *Journal of Criminal Law and Criminology, 82:* 360-395.

Reuter, P., & Truman, E. M. (2004). *Chasing Dirty Money: the Fight Against Money Laundering*. Washington, DC: Institute for International Economics.

Robins, G., Pattison, P., Kalish, Y., & Lusher, D. (2007a). An introduction to Exponential Random Graph (p*) Models for social networks. *Social Networks, 29*, 173–191.

Robins, G., Snijders, T., Wang, P., Handcock, M., & Pattison, P. (2007b). Recent developments in Exponential Random Graph (p*) Models for social networks. *Social Networks, 29*, 192–215.

Robins, G.L, & Pattison, P.E. (2005). Interdependencies and social processes: dependence graphs and generalized dependence structures. In P.J. Carrington, J. Scott, & S. Wasserman (eds.), *Models and Methods in Social Network Analysis* (pp. 192-214). New York, NY: Cambridge University Press.

Robins, G.L., Elliott, P., & Pattison, P.E. (2001). Network models for social selection processes. *Social Networks, 23*, 1-30.

Rogers, E. M. (1962). *Diffusion of Innovations*. Glencoe: Free Press.

Rollins, J., & Wyler, L. S. (2010). *International Terrorism and Transnational Crime: Security Threats, U.S. Policy, and Considerations for Congress.* Washington, DC: Congressional Research Service.

Rowlingson, K., Whyley, C., Newburn, T. and Berthoud, R. (1997). *Social Security Fraud: The role of penalties,* London, UK: Her Majesty's Stationery Office.

Ruggiero, V. (1997). Criminals and service providers: Cross-national dirty economies. *Crime, Law & Social Change, 32*, 203-233.

Ruggiero, V. (2003). Global markets and crime. In M. E. Beare, (Ed.), *Critical reflections on transnational organized crime, money laundering, and corruption*, (pp. 171-182). Toronto, CA: University of Toronto Press.

Sageman, M. (2004). *Understanding terror networks*. Philadelphia, PA: University of Pennsylvania Press.

Sanchez, C. (2009). *Return of the Sovereigns: Resurgence of Far-Right Movement Reported. SPLC Intelligence Report, Issue Number 133, Spring 2009.* Retrieved from http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2009/spring/return-of-the-sovereigns.

Sanger-Katz, M. (2006, June 11). Protesters see income tax as a scam. *Concord Monitor*, Retrieved from: http//:www.concordmonitor.com/apps/pbcs.dll/article?AID=/20060611/REPOSITORY/606110338

Sarnecki, J. (2001). *Delinquent networks: Youth co-offending in Stockholm*. Cambridge, UK: Cambridge University Press.

Schmid, A. P. (2004). Frameworks for conceptualizing terrorism. *Terrorism and Political Violence, 16*(2), 197-221.

Scott, J. (2000). *Social Network Analysis*. Newbury Park, CA: Sage Publications.

Shapiro, N. J. (2007). Terrorists' organizations' vulnerabilities and inefficiencies: a rational choice perspective. In J. K. Giraldo, & H. A. Trinkunas, (Eds.). *Terrorism financing and state responses: A comparative perspective*, (pp. 56-71). Stanford, CA: Stanford University Press.

Shelley, L. & Melzer, S. (2008). The Nexus of Organized Crime and Terrorism: Two Case-Studies in Cigarette Smuggling. *The International Journal of Comparative and Applied Criminal Justice, 32* (1), 43-63.

Shelley, L. I., & Picarelli, J. T. (2005). Methods and motives: Exploring links between transnational organized crime and international terrorism. *Trends in Organized Crime, 9*(2), 52-67.

Sherman, L..Gartin, P., & Buerger, M. (1989). Hot spots of predatory crime: Routine activities and the criminology of place. *Criminology, 27*, 27-55.

Shumate, M., & Palazzolo, E.T. (2010). Exponential random graph (p*) models as a method for social network analysis in communication research. In press. *Communication Methods and Measures.*

Silke, A. (2001). The devil you know: Continuing problems with research on terrorism. *Terrorism and political violence, 13*(4), 1-14.

Silke, A. (2008). Research on Terrorism: A Review of the Impact of 9/11 and the Global War on Terrorism. In Chen, H., Reid, E. Sinai, J., Silke, A., Ganor, B. (Eds.). *Terrorism Informatics: Knowledge Management and Data Mining for Homeland Security*, (pp. 27-50), New York, NY: Springer.

Smith, B. L. (1994). *Terrorism in America: Pipe Bombs and Pipe Dreams*. Albany, NY: State University of New York Press.

Smith, B.L., Cothren J., Roberts, P., & Damphousse, K. R. (2008). *Geospatial Analysis of Terrorist Activities: The Identification of Spatial and Temporal Patterns of Preparatory Behavior of International and Environmental Terrorists.* NIJ Final Report, Grant 2005-IJ-CX-0200.

Smith, B. L., & Damphousse, K. R. (1998). Terrorism, politics, and punishment: A test of structural-contextual theory and the "liberation hypothesis". *Criminology, 36*, 67-92.

Smith, B. L., & Damphousse, K. R. (2003). *The American Terrorism Study*. Oklahoma City: Memorial Institute for the Prevention of Terrorism.

Smith, B. L., Damphousse, K. R., Jackson, F., & Sellers, A. (2002). The prosecution and punishment of international terrorism in federal courts: 1980-1998. *Criminology & Public Policy, 1*(3), 311-338.

Smith, B.L., Damphousse, K.R., & Roberts, P. (2006). *Final Technical Report: Pre-Incident Indicators of Terrorist Incident: The Identification of Behavioral, Geographic, and Temporal Patterns of Preparatory Conduct* (pp. 1-100). National Institute of Justice. Washington, DC: Office of Justice Programs.

Smith, M.J. (1998). Regulating opportunities: multiple roles for civil remedies in situational crime prevention. *Crime Prevention Studies, 9*, 67-88.

Snijders, T.A.B. (2005). Models for Longitudinal Network Data. In P. J. Carrington, J. Scott, & S. Wasserman. *Models and Methods in Social Network Analysis*, (pp. 215-247). New York, NY: Cambridge University Press.

Snijders, T.A.B. (2009). *Specification and estimation of exponential random graph models for social (and other) networks.* [PDF Document]. Presentation at University of Oxford, March 24, 2009. Retrieved from www.stats.ox.ac.uk/~snijders/p12_ergm.pdf.

Snijders, T.A.B., Pattison, P.E., Robins, G. & Handcock, M. S. (2006). New specifications for exponential random graph models. *Sociological Methodology*, 99–153.

Snijders, T.A.B., Steglich, C.E.G., & Schweinberger, M. (2007). Modeling the co-evolution of networks and behavior. In K. van Montfort, H. Oud, & A. Satorra (Eds.). *Longitudinal models in the behavioral and related sciences*, (pp. 41-71). Mahwah, NJ: Lawrence Erlbaum.

Southern Poverty Law Center (2001). Don Quixote of Queensbury: Bob Schulz's We The People may be tilting at windmills, but its efforts reflect a re-energized tax protest movement. SPLC Intelligence Report,Winter 2001. Retrieved from: www.splcenter.org/intel/intelreport/article.jsp?aid=115&printable=1

Southern Poverty Law Center (2007). Tax Protesters: Crackdown Hits Tax Protesters, Celebrities Included. SPLC Intelligence Report, Spring 2007. Retrieved from: www.splcenter.org/intel/intelreport/article.jsp?aid=744&printable=1

Spaaij, R. (2010). The Enigma of Lone Wolf Terrorism: An Assessment. *Studies in Conflict & Terrorism, 33*(9), 854-870.

Sparrow, M. K., (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks, 13*, 251–274.

Steglich, C.E.G., Snijders, T.A.B. & Pearson, M. (2010). Dynamic Networks and Behavior: Separating Selection from Influence, *Sociological Methodology*. In press.

Stern, J., & Modi, A. (2008). Producing terror: organizational dynamics of survival. In T. J. Biersteker, & S. E. Eckert (Eds.). *Countering the financing of terrorism,* (pp. 17-46). New York, NY: Routledge.

Stohl, M. (2008). Networks, terrorists and criminals: the implications for community policing. *Crime, Law and Social Change, 50,* 59-72.

Sutherland, E.H., & Cressey, D.R. (1960). A theory of differential association. In Cressey, E.S. (Ed.). *Principles of Criminology (6th ed.).* Chicago, IL: J.B. Lippincott Company.

Sykes, G., & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review, 22*(6), 664-670.

Taylor, I. (1999). *Crime in Context: A Critical Criminology of Market Societies*. Boulder, CO: Westview.

Thony, J. (2002). *Money laundering and terrorism financing: an overview*. [PDF Document]. Retrieved from www.imf.org/external/np/leg/sem/2002/cdmfl/eng/thony.pdf

Tilley, N. (Ed.) (2005). *Handbook of Crime Prevention and Community Safety*. Devon, UK: Willan Publishing.

Trasler, G. (1986). Situational crime control and rational choice: A critique. In K. Heal, & G. Laycock, (Eds.). *Situational crime prevention: From theory into practice,* (pp. 17-24). London, UK: Her Majesty's Stationery Office.

Tremblay, P. (1993). Searching for suitable co-offenders. In R.V.G. Clarke & M. Felson. *Routine activity and rational choice,* (pp. 17-37). New Brunswick, NJ: Transaction Publishers.

Turk, A.T. (2004). Sociology of terrorism. *Annual Review of Sociology, 30*, 271-286.

United Nations General Assembly (1999*). International Convention for the Suppression of the Financing of Terrorism*. Retrieved from: treaties.un.org/doc/db/Terrorism/summary-18-11.pdf.

US Code Title 18.

US Department of State (2003). *International Narcotics Control Strategy Report 2003.*Bureau for International Narcotics and Law Enforcement Affairs, March 2004. Retrieved from: http://www.state.gov/p/inl/rls/nrcrpt/2003/.

Valente, T. (1995). *Network models of the diffusion of innovations*. Cresskill, NJ: Hampton Press.

Van der Hulst, R. C. (2009). Introduction to Social Network Analysis (SNA) as an investigative tool. *Trends in Organized Crime, 12*, 101-121.

Van Duijn, M.A.J., & Vermunt, J. (2006). What is special about social network analysis? *Methodology, 2*(1), 2-6.

Van Duyne P., & Levi M. (1999). Criminal financial investigations: a strategic and tactical approach in the European dimension. In Viano E. C. (Ed.), *Global Organized Crime and International Security*. Aldershot, UK: Ashgate.

Van Duyne P., & Von Lampe K. (Eds.) (2002). *Upperworld and underworld in cross-border crime*. Nijmegen, NL: Wolf Legal Publishers.

Van Meter, K. M. (2002). Terrorists/liberators: Researching and dealing with adversary social networks. *Connections, 24*(3), 66-78.

Vander Beken, T. (2004). Risky business: A risk-based methodology to measure organized crime. *Crime, Law, and Social Change, 41*(5), 471-516.

Veness, D. (1999). Low intensity and high impact conflict*. Terrorism & Political Violence, 11*(4), 8.

Viano E.C. (1999) (Ed.), *Global Organized Crime and International Security*, Aldershot, UK: Ashgate.

Viano, E. C., Magallanes, J. & Bridel, L. (2003) (Eds.), *Transnational Organized Crime. Myth, power and profit*. Durham, CL: Carolina Academic Press.

Wang, P., Robins, G., & Pattison, P. (2004). *PNet, Version 1.0*. University of Melbourne, Australia.

Wang, P., Robins, G., Pattison, P. (2009). *PNet. Program for the Simulation and Estimation of Exponential Random Graph (p*) Models. User Manual.* [PDF Document]. University of Melbourne, Australia. Retrieved from http://www.sna.unimelb.edu.au/pnet/pnet.html.

Warde, I. (2007). *The price of fear: the truth behind the financial war on terror*. Berkeley, CA: University of California Press.

Waring, E. (2002). Co-offending as a network form of social organization. In E. Waring, & D. Weisburd (Eds.). *Crime and Social Organization, Advances in Criminological Theory,* Vol. 10, p. 15-29. New Brunswick, NJ: Transaction Publishers.

Warr, M. (2002). *Companions in crime*. Cambridge, UK: Cambridge University Press.

Wasserman, S. & Faust, K. (1994). *Social Network Analysis*. Cambridge, UK: Cambridge University Press.

Wasserman, S., & Pattison, P. (1996). Logit models and logistic regressions for social networks: I. An introduction to Markov graphs and p. *Psychometrika, 61*(3), 401-425.

Wasserman, S., & Robins, G. (2005). An introduction to random graphs, dependence graphs, and p*. In: P.J. Carrington, J. Scott, & S. Wasserman (eds.), *Models and Methods in Social Network Analysis* (pp. 148-161). New York, NY: Cambridge University Press.

Webb, B. (2005). Preventing vehicle crime. In Tilley, N. (Ed.) *Handbook of Crime Prevention and Community Safety* (pp. 458-485). Devon, UK: Willan Publishing.

Weerman, F.M.. (2003). Co-offending as Social Exchange. Explaining Characteristics of Co-offending. *British Journal of Criminology, 43*(2), 398-416.

Weinberg, L., Pedahzur, A., Hirsch-Hoefler, S. (2004). The challenges of conceptualizing terrorism. *Terrorism and Political Violence, 16*(4), 777-794.

Weisburd, D., Wheeler, S., Waring, E., and Bode, N. (1991). *Crimes of the Middle Classes: White Collar Offenders in Federal Courts*. New Haven, CT: Yale University Press.

Wilkinson, D.L., McBryde, M.S., Williams, B., Bloom, S., & Bell, K. (2009). Peers and gun use among urban adolescent males: An examination of social embeddedness. *Journal of Contemporary Criminal Justice*, *25*(1), 20-44.

Williams, P. (1999). Transnational criminal networks. In J. Arquilla, & D. Ronfeldt (Eds.) *Networks and Netwars,* (pp. 61–97). Santa Monica, CA: Rand.

Williams, P. (2007). Warning indicators and terrorist finances. In J. K. Giraldo, & H. A. Trinkunas (Eds.). *Terrorism financing and state responses: A comparative perspective,* (pp. 72-92). Stanford, CA: Stanford University Press.

Williams, P. (2008). Terrorist financing and organized crime: nexus, appropriation or transformation? In T. J. Biersteker, & S. E. Eckert (Eds.). *Countering the financing of terrorism* (pp. 126-149). New York, NY: Routledge.

Williams, P., & Godson, R. (2002). Anticipating organized and transnational crime. *Crime, Law & Social Change, 37*, 311-355.

Wimmer A., & Lewis, K. (2010). Beyond and below racial homophily: ERG Models of a friendship network documented on Facebook. *American Journal of Sociology, 116*(2), 583-642.

Wortley, R. (1998). A two-stage model of situational crime prevention. *Studies on Crime and Crime Prevention, 7*(2), 173-188.

Wortley, R. (2001). A classification of techniques for controlling situational precipitators of crime. *Security Journal, 14*(4), 63- 82.

Wortley, R. (2002). *Situational prison control: Crime prevention in correctional institutions.* Cambridge, UK: Cambridge University Press.

Wright, A. (2006). *Organised Crime*. Collumpton, UK: Willan Publishing.

Xu, J., & Chen, H. (2008). The Topology of Dark Networks. *Communications of the ACM, 51*(10), 58-65.

Xu, J., Byron, M., Siddhart, K., Chen, H. (2004). Analyzing and visualizing criminal network dynamics: A case study. *Intelligence and Security Informatics, Proceedings 3073*, 359-377.

Young, J. T.N. (2010). How Do They 'End Up Together'? A Social Network Analysis of Self-Control, Homophily, and Peer Relationships. *Journal of Quantitative Criminology*. In press.

Zhang, S.X., Chin, K., & Miller, J. (2007). Women's participation in Chinese transnational smuggling: A gendered market perspective. *Criminology, 45*(3), 699-733