CASE STUDIES OF U.S. LAW ENFORCEMENT TECHNIQUES AGAINST ORGANIZED CRIME GROUPS

*Joseph K. Wheatley**

I. INTRODUCTION

U.S. law enforcement authorities face a variety of domestic and transnational organized crime groups. Those groups run the gamut in the types of crimes committed; structure and unifying purposes; from small to large in size; and from local to regional to national and transnational in scope. While not statutorily binding, there are several major definitions of organized crime in the United States, including the following two definitions, which may aid decision-makers in setting priorities and focusing resources as new criminal threats are identified and prosecuted.

In 1986, the President's Commission on Organized Crime released a report, which listed six characteristics of organized crime groups:

> The criminal group is a continuing, structured collectivity of persons who utilize criminality, violence, and a willingness to corrupt in order to gain and maintain power and profit. The characteristics of the criminal group, which must be evidenced concurrently, are: [1] continuity, [2] structure, [3] criminality, [4] violence, [5] membership based on a common denominator, [6] a willingness to corrupt and a power/profit goal.[1]

In 2008, *the Law Enforcement Strategy to Combat International Organized Crime* defined international organized crime groups as:

> [T]hose self-perpetuating associations of individuals who operate internationally for the purpose of obtaining power, influence, monetary and/or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/or violence. There is no single structure under which international organized criminals operate; they vary from hierarchies to clans, networks and cells, and may evolve to other structures. The crimes they commit also vary.[2]

The 2008 *Strategy's* definition shares terms in common with the 1986 President's Commission on Organized Crime's six characteristics, such as continuity, structure, and pursuit of power as a goal; and shares terms in common with the *United Nations Convention Against Transnational Organized Crime*. These definitions are not limited to a particular organization, such as the Mafia, leaving room for various types of organizations to qualify as an organized crime group, such as gangs and cybercrime groups.

This article examines three different forms of organized crime groups in the United States, which also operate transnationally in some cases—the Mafia, gangs, and cybercrime groups. In doing so, this article offers case studies of how various types of law enforcement tools have been used successfully against those three forms of organized crime groups. By no means are those three organized crime groups an exhaustive list of the groups which operate in the United States or elsewhere. However, as they are each distinctive forms of organized crime groups, with varying predicate offences, structures, modes of operations, and unifying purposes, they serve as helpful examples about law enforcement tools which may be successful

* Trial Attorney, Organized Crime and Gang Section, Criminal Division, United States Department of Justice, United States of America.

[1] President's Commission on Organized Crime, *Report to the President and the Attorney General, The Impact: Organized Crime Today* (1986), pp. 25–29 [hereinafter *President's Commission Report*].

[2] United States Department of Justice, *The Law Enforcement Strategy to Combat International Organized Crime* (23 April 2008), p. 2.

against different types of organized crime groups.

II. THE AMERICAN MAFIA

The Mafia holds a prominent place in American popular conceptions of organized crime. The terms of "Mafia" and "organized crime" even tend to be treated as one and the same. Congressional investigations in the 1950's and 1960's increased the government's knowledge about the Mafia, also known as "La Cosa Nostra," commonly translated into English as "Our Thing".[3] Until that time, the Mafia as an institution was largely unknown to the U.S. Congress. Investigations by the U.S. Congress' Kefauver and McClellan Committees helped reveal, to the public and legislators, the Mafia's infrastructure, rules, and leadership.[4]

The Mafia is a hierarchical organization, composed of career criminals, that requires its members to show loyalty and obedience.[5] Mafia groups, also known as "families," operate in a given city or region.[6] A "boss" serves as the leader of a Mafia family and receives a large fraction of the family's earnings.[7] An "underboss" manages the daily operations of a Mafia family and represents the boss when necessary.[8] "Captains" manage the "soldiers," the low-level members who carry out most of the Mafia family's activities, at times using uninitiated associates of the family.[9]

The Mafia earns money from various crimes. In the 1950's, the Mafia derived most of its revenue from loan-sharking and gambling.[10] The Mafia has also earned money from prostitution, labor racketeering, and sales of black market goods.[11] Starting in the 1980's, narcotics trafficking became the most significant source of revenue for the Mafia.[12] Using legitimate businesses as money laundering fronts, the Mafia hides the sources of its finances.[13]

The Mafia is just one example of the large, hierarchical organized crime groups that operate in the United States. For instance, U.S. law enforcement agencies face Russian organized crime groups and gangs, such as MS-13 and others described below, that are also large and hierarchical.

A. Successful Methods against the Mafia

Various methods have been used successfully against the Mafia, including electronic surveillance and informants. While various methods have been used successfully, this section offers examples of the use of the Racketeer Influenced and Corrupt Organizations statute and undercover operations against the Mafia.

1. Racketeer Influenced and Corrupt Organizations Statute ("RICO")

In 1970, the U. S. Congress enacted the Organized Crime Control Act, which included Racketeer Influenced and Corrupt Organizations, a landmark law commonly known as "RICO". RICO represented a new approach by the United States for conceptualizing and targeting organized crime.[14] RICO treats organized crime groups as they really are, criminal enterprises to be dismantled, whether they are traditional groups that prey upon their victims face-or-face, or cybercrime groups that prey upon their victims from thousands of miles away. To paraphrase, RICO criminalizes a pattern of conduct performed as part of a criminal enterprise, such as owning, participating in, or funding such enterprises, or conspiracies to commit such

---

[3] *See* United States Congress, *Senate Report No. 617* (1969), pp. 36–43.
[4] *See generally* United States Congress, *Organized Crime and Illicit Traffic in Narcotics: Hearings Before the Permanent Subcommittee on Investigations of the Senate Committee on Government Operations* (1963), p. 80 [hereinafter *McClellan Committee Hearings*]; United States Congress, *Report of the Senate Special Committee to Investigate Organized Crime in Interstate Commerce*, S. Rep. No. 307 (1951) [hereinafter *Kefauver Committee Report*].
[5] *McClellan Committee Hearings*, p. 2 (remarks of Senator John McClellan).
[6] President's Commission on Law Enforcement and Administration of Justice, *Task Force Report: Organized Crime* (1967), p. 7 [hereinafter *Task Force Report*].
[7] *President's Commission Report*, p. 39.
[8] *Id.*; *Task Force Report*, p. 7.
[9] *President's Commission Report*, p. 39; *Task Force Report*, pp. 7–8.
[10] *Task Force Report*, pp. 2, 4; *Kefauver Committee Report*, p. 2.
[11] *Kefauver Committee Report*, p. 1.
[12] *President's Commission Report*, p. 11.
[13] *Task Force Report*, p. 4.
[14] 18 U.S.C.A. § § 1961–1968 (West).

conduct.[15] In its focus on criminal enterprises, RICO distinguishes itself from the various laws targeting organized crime that preceded it. RICO possesses considerable flexibility to target new criminal groups that arise, since it names no particular criminal group as liable for prosecution.

In 1980, ten years after enacting RICO, the federal government used the statute to prosecute a leader of the Mafia. On November 21, 1980, Frank "Funzi" Tieri, the head of the Genovese organized crime family, one of the Mafia's five families in New York City, became the first Mafia boss convicted under RICO. He was sentenced to ten years' imprisonment on January 23, 1981.[16]

By the mid-1980's, the federal government's RICO prosecutions of organized crime figures had expanded considerably. On February 25, 1985, in the "Commission Case," a federal grand jury in New York City indicted the bosses, and some major subordinates, of the city's five Mafia organized crime families, for various racketeering offences, including murder.[17] The Commission Case targeted not only the five Mafia families in New York, but also the "Commission", the governing board created by the families to oversee Mafia operations in the United States.[18] The trial made extensive use of electronic surveillance, including recordings of Mafia headquarters, phones, and vehicles. On November 19, 1986, a jury convicted the eight defendants of nearly all the charges against them.[19] On January 13, 1987, a federal judge sentenced each defendant to one-hundred years' imprisonment, except for one defendant, who received a forty-year prison sentence.[20]

In the years following the Commission Case, Mafia leaders, members, and associates around the country were convicted, including the heads of the New York, Boston, and Philadelphia Mafia families, which further weakened the Mafia families. In another blow to the Mafia, on January 20, 2011, the U.S. Department of Justice announced charges in three cities against more than 100 alleged Mafia leaders, members, and associates, including RICO and related crimes, such as murder and extortion. This was the largest day of Mafia arrests in U.S. history.[21]

Cases such as the Commission Case and the indictments in 2011 are merely a few examples of the large RICO prosecutions of Mafia families. Around the United States, law enforcement authorities continue to undermine the Mafia crime families using RICO and other methods. Such prosecutions attack the structure and the chains of command of the Mafia families by impeding the recruitment and retention of their leaders and members. In turn, these prosecutions diminish the Mafia families as institutions and limit their capacity to commit crimes.

2. Undercover Operations

One prominent example of the effectiveness of undercover operations against the Mafia is Joseph Pistone, a Special Agent of the Federal Bureau of Investigation ("FBI"), who infiltrated the Bonanno and Colombo Mafia crime families.[22] From 1976 through 1981, Pistone worked undercover as Mafia associate "Donnie Brasco." By using an undercover agent, the FBI did not have to rely for evidence on informants inside of the crime families.

Posing as a jewel thief providing his skills to the Mafia, Pistone earned the trust of leading members of the crime families, who discussed various crimes in his presence, including murders of rival Mafia members, hijackings of delivery trucks, and the sale of stolen property. Some of those conversations were recorded by Pistone, which further corroborated the events that Pistone observed. Because those conversations were recorded, prosecutors could rely on both Pistone's testimony and the voices of the Mafia members themselves as evidence.

---

[15] 18 U.S.C.A. § 1962 (West).
[16] Les Ledbetter, "Frank Tieri, 77, Convicted New York Crime Leader", *New York Times*, 31 March 1981.
[17] Michael Arena, et al., "Raising the Curtain on Organized Crime", *Newsday*, 9 July 1986.
[18] Ed Magnuson, "A jury convicts eight Mobsters", *Time*, 1 December 1986.
[19] Arnold H. Lubasch, "Judge Sentences 8 Mafia Leaders to Prison Terms", *New York Times*, 14 January 1987, p. A1.
[20] *Id*.
[21] William K. Rashbaum, "Nearly 125 Arrested in Sweeping Mob Roundup", *New York Times*, 20 January 2011, p. A21.
[22] Federal Bureau of Investigation, "Joe Pistone, Undercover Agent". Available from https://www.fbi.gov/history/famous-cases/joe-pistone-undercover-agent (accessed 25 April 2017).

Pistone became such a trusted associate of the Mafia that the Bonanno crime family considered making him a full member of the organization. However, the FBI decided to conclude the undercover operation before Pistone became a member, because of the risk of violence. After the Pistone's true identity was revealed, chaos erupted within the Mafia world, with leaders and members concerned about future infiltration by government investigators and informants. Evidence collected by Pistone contributed to the convictions of more than 100 Mafia members and associates. The prosecutions particularly depleted the leadership and membership of the Bonanno crime family and damaged the crime family as an institution, which was shunned for a period of time by the Mafia's ruling Commission.

III. GANGS

In recent years, the federal government has engaged in a crackdown on gangs, many of which are large organizations that operate internationally, nationally, or regionally. While gangs commit a variety of crimes, including white-collar offences such as fraud and identity theft, they tend to focus on drug crimes and violent crimes, such as murder, shootings, and robberies. Certain gangs may resemble or eventually resemble a traditional organized crime group, such as the Mafia. The primary author of the RICO statute, G. Robert Blakey, has remarked that the Mafia was once less sophisticated and gradually morphed over time into an organized crime group: "[Gangs are] in the process of growing into Mafias … The Mafia started out as a gang."[23]

While there is a no single definition for gangs, a report by the U.S. Department of Justice's Bureau of Justice Assistance remarked that most of the gang definitions include a portion, or all, of the following factors:

> [1] Three or more individuals associate periodically as an ongoing criminal group or organization, whether loosely or tightly structured.
>
> [2] The group or organization has identifiable leaders, although the leader for one type of criminal activity may be different than the leader for another.
>
> [3] The group has a name or identifying symbol
>
> [4] The organization's members, individually or collectively, currently engage in, or have engaged in, violent or other criminal activity[.]
>
> [5] The group frequently identifies itself with or claims control over specific territory (turf) in the community, wears distinctive dress and colors, and communicates through graffiti and handsigns among other means.[24]

One example of a prominent gang in the United States is Mara Salvatrucha 13, commonly known as MS-13. U.S. Attorney General Jeff Sessions has named MS-13 and other violent groups as major threats, and committed significant federal resources to prosecuting them.[25] MS-13, which is composed primarily of Salvadorans and other Central Americans, has thousands of members in various states around the United States, and reputedly tens of thousands of members in Central America.[26] Prosecutions in cities across the country, such as Atlanta, Dallas, Los Angeles, New York, and Washington, D.C., have shown coordination between MS-13 chapters domestically and internationally, including coordination of violent crime between Central American MS-13 leaders and MS-13 chapters operating in U.S. cities. Among the gang's crimes are murder, armed assaults, robbery, transportation and distribution of drugs, and alien smuggling.

Another prominent gang in the United States is the Vice Lords, which has thousands of members nationwide. As shown in court, the gang engages in a variety of crimes, including murder, shootings, robbery,

---

[23] John Gibeaut, "Gang Busters", *ABA Journal*, January 1998, p. 65.
[24] United States Department of Justice, Bureau of Justice Assistance, *Urban Street Gang Enforcement* (January 1997), p. 30.
[25] Jake Pearson, "Trump, top officials take aim at brutal MS-13 street gang", *New York Daily News*, 19 April 2017. Available from http: //www. nydailynews. com/newswires/new-york/trump-top-officials-aim-brutal-ms-13-street-gang-article-1.3069112 (accessed on 27 April 2017).
[26] *Id*.

narcotics trafficking and witness intimidation. The Vice Lords' leaders are located in Chicago and Detroit and the gang is broken down into various "branches," with names such as the "Traveling Vice Lords" and "Insane Vice Lords." Members who seek to leave the gang oftentimes endure a physical beating by multiple Vice Lord members or are targeted for killing. The Vice Lords also has a biker gang affiliate known as the Phantom Outlaw Motorcycle Club ("Phantoms"), which emerged from the Vice Lords and was led in part by Vice Lords. The Phantoms are headquartered in Detroit and have sub-groups, known as "chapters" in at least ten states, as well as a chapter of "Nomads" that travel at will. As shown in court, the Phantoms and its members were involved in a range of criminal activity, including conspiracy to commit murder, shootings, robbery, extortion, and the possession and sale of stolen vehicles and motorcycles.

A. Successful Methods against Gangs

Various methods have been used successfully against gangs across the country, including RICO. For instance, the U.S. Department of Justice's Organized Crime and Gang Section ("OCGS") and U.S. Attorney's Offices have prosecuted the MS-13 gang using RICO in various U.S. states, including Maryland, Georgia, Virginia, New Jersey, North Carolina, and California.[27] In another example, OCGS and the Detroit U.S. Attorney's Office have pursued RICO and other charges against the Vice Lords and Phantoms over several years, resulting in seven indictments and the convictions of 27 leaders, members, and associates. RICO indictments, such as these and others, have aided the government in undermining gangs as organizations and preventing further violence.

While various methods have been used successfully against gangs, such as the RICO prosecutions described above, this section offers specific examples of the use of informants, electronic surveillance, and testimony under cooperation agreements.

1. Informants and Electronic Surveillance

In Detroit in 2013, the government's use of an informant and electronic surveillance helped prevent large-scale violence, and assisted in the prosecution of the Vice Lords and Phantoms. As shown in court, a member of the Phantoms agreed to become an informant for the government, following his arrest on a firearms charge in 2013. Once he agreed to cooperate with the government, the informant began providing information to investigators about the historical and ongoing activities of Vice Lords and Phantoms. Further, the informant began recording his in-person conversations with other Vice Lords and Phantoms members, as well as his phone calls with members. In total, the informant recorded dozens of conversations, with some lasting more than an hour. Given the informant's former role as National President of the Phantoms and his long association with its members, he was well-placed within the organization to gather information, including recorded conversations with Antonio Johnson, the "Three-Star General" over all Vice Lords in Michigan and the National President of the Phantoms.

The informant made recordings and told law enforcement investigators about various crimes by the Vice Lords and Phantoms, including shootings, extortion of rival groups, robberies, assaults, and motorcycle thefts. For instance, recordings entered into evidence showed Vice Lords and Phantoms talking about shooting a member of a rival group in September 2013, including the identity of the Phantom/Vice Lord who fired the gun. Other recordings show Antonio Johnson telling the informant before the shooting took place, "I don't burn buildings. At all. I burn bodies", and after the shooting, "I think they gonna want to talk with once we kill like ten of them".

However, there was one particular crime to which the informant alerted law enforcement, which helped the government prevent large-scale violence by the Vice Lords and Phantoms in 2013. Recordings made by the informant and other evidence showed that the Vice Lords and Phantoms developed a three-phase mass murder plot against a rival group that was interrupted by law enforcement as phase one was just about to begin. In the first phase, the Vice Lords and Phantoms were to murder at least three members of a rival group in Detroit, in order to lure additional victims to Michigan for the funeral. In the second phase, the Vice Lords and Phantoms were to murder all members of the rival group who would be at the rival's Detroit headquarters following the funeral of the three victims murdered in the first phase. In the third phase, the Vice Lords and Phantoms were to kill rivals in other cities throughout the country where the Phantoms had

[27] *Id.*

chapters.

Acting on the recordings from the informant and other evidence, law enforcement officers from the Bureau of Alcohol, Tobacco, Firearms, and Explosives, FBI, and Detroit Police Department were able to interrupt the mass murder plot before it could happen by executing search warrants and arresting Vice Lords and Phantoms members in October 2013. During the execution of one of the search warrants, a Phantoms leader shot at federal agents. The informant's recordings and other evidence showed at trial that, at the time of the search warrants and arrests, the Vice Lords and Phantoms were preparing for the first phase of the murder plot, including stockpiling firearms, hiring a thief to steal a van to be used in the murders, conducting research and surveillance of their intended victims, and assigning Phantom members and Vice Lords members to stalk and murder the intended victims.

Using these recordings and the informant, the government was able to avert the mass murder plot, and build a prosecution of the Phantoms and Vice Lords. In a series of indictments in 2013 and 2014, fourteen alleged leaders and members of the Vice Lords and Phantoms were charged with RICO, the mass murder plot, several shootings, and other offences. Among the defendants was Antonio Johnson, the "Three-Star General" over all Vice Lords in Michigan and the National President of the Phantoms.

2. Testimony under Cooperation Agreements

Another example of an effective method against gangs is the use of witness testimony under cooperation agreements. Following the indictment of Vice Lords and Phantoms members, the government continued to build its prosecution of the criminal groups. As was shown in court, several Vice Lords and Phantoms agreed to cooperate with the government's prosecution after being charged for their offences. Testimony by these cooperating witnesses contributed significantly to the prosecution of the criminal groups.

Such agreements are commonly known as "cooperation agreements." They require some liability for a defendant's criminal conduct; in which a defendant agrees to fully and truthfully cooperate, testify in any court proceeding concerning matters asked of him or her, and enter a guilty plea on other charges. In exchange for this cooperation, the government files a motion giving the judge special discretion in determining the defendant's sentence. Often the sentencing judge will reduce the defendant's sentence. This opportunity for a sentence reduction creates an incentive to cooperate.

Testimony by witnesses under cooperation agreements is effective against organized crime groups, and defendants in general, for a variety of reasons. First, insider witness testimony can be more effective at explaining the internal operations of a criminal organization than undercover operations or electronic surveillance. Second, insiders are already well placed within the criminal groups, compared to undercover officers. If undercover officers are able to penetrate a criminal organization, it is very difficult and they are rarely able to penetrate deep within the organization. Third, insider witnesses are able to interpret coded or confusing language that is recorded on electronic surveillance, and explain those conversations in court.

In court during two trials, several cooperating witnesses testified against the Vice Lords and Phantoms, and demonstrated the effectiveness of insider testimony. Witnesses explained to the jury how the criminal groups worked from the inside, such as the groups' leadership, membership, chain of command, rules, history, and rivals. Further, they described crimes involving the two groups, and identified who committed each of those crimes. This testimony included details and context about the Vice Lords and Phantoms organizations and their crimes that other methods would not necessarily have uncovered. For instance, insider witnesses testified about private conversations with other members of the organizations, the organizations' private meetings, and crimes that were not observed by the police, such as shootings, assaults, robberies, and motorcycle theft.

This testimony by witnesses using cooperation agreements was powerful evidence against the Vice Lords and Phantoms, especially when combined with other evidence, such as audio recordings made by the informant. Through guilty pleas and two trials, thirteen of the fourteen alleged Vice Lords and Phantoms described above were convicted for various crimes connected to the groups, including RICO, the mass murder plot, shootings, and robberies. The highest prison sentence was for 40 years, imposed on Marvin Nicholson, a Vice Lord and the National Enforcer of the Phantoms; followed by 35 years in prison for Antonio Johnson, the "Three-Star General" over all Vice Lords in Michigan and the National President of the

Phantoms.

In total, the methods described above, such as RICO, electronic surveillance, informants, and cooperating witness testimony, contributed to seven indictments and the convictions of 27 leaders, members, and associates of the Vice Lords and Phantoms. The convictions were for a variety of additional crimes, including armed home invasions, the disclosure of private medical information that was taken from a hospital database, and the shooting of a family of four with a machine gun, after two of the family members had left or attempted to leave the gang.

Various methods, such as RICO, informants, electronic surveillance, and witness testimony under cooperation agreements, continue to be used effectively against gangs. The methods are effective against large gangs, such as MS-13 and the Vice Lords, but also smaller gangs that commit violence and other crimes in communities around the country.

IV. CYBERCRIME GROUPS

The traditional conception of organized crime, typified by the Mafia and gangs, has been upended, in part, by the Internet and other communications technologies that cybercrime groups use. Compared to the Mafia and gangs, cybercrime groups may have opaque and fluid command structures, and they appear to avoid using violence as a means of asserting control and discipline. Their offences are magnified by, or almost entirely dependent upon, the use of the Internet and other communications technologies, such as identity theft, online banking theft, and fraud schemes.

On April 23, 2008, in a speech before the Center for Strategic and International Studies in Washington, DC, then-U.S. Attorney General Michael Mukasey announced the release of *The Law Enforcement Strategy to Combat International Organized Crime* (the "*Strategy*"),[28] which identified cybercrime groups, among other international groups, as an organized crime threat.

Cybercrime, perpetrated by organized crime groups and others, presents a major threat to the United States and other countries. In addition to human suffering and other harms of such crime, cybercrime imposes significant costs upon people around the world. Estimates vary of the annual costs imposed by cybercrime, but they number in the hundreds of billions of dollars. For instance, the Center for Strategic and International Studies has estimated, in 2014, that the "likely annual cost to the global economy is more than $400 billion",[29] and that the costs account for about 0.8% of global GDP and about 0.64% of the United States' GDP.[30] Further, PwC's 2014 survey of organizations indicated that, in 2014, 19% of U.S. organizations each lost between $50,000 and $1 million, and 7% of U.S. organizations each lost more than $1 million.[31]

Although cybercrime has been a matter of concern for decades, sophisticated cyberattacks have occurred in recent years, and been committed on a far grander scale than before. For instance, in January 2014, Target, a large U.S. retailer, announced that cybercriminals had stolen the credit card information of 40 million shoppers, and the personal information of 70 million shoppers. Between 1 and 3 million of those credit cards were reportedly sold, yielding an estimated $53.7 million for the perpetrators. The cyberattack cost Target an estimated $148 million, and cost financial institutions an estimated $200 million.

While there are ways for U.S. law enforcement authorities to respond to such threats, the 2008 *Strategy* recognized the challenges facing them by cybercrime groups and other international organized crime groups. As then-Attorney General Michael Mukasey stated upon the release of the *Strategy*: "International organized crime poses a greater challenge to law enforcement than did the traditional mafia, in many respects. And the geographical source of the threat is not the only difference. The degree of sophistication is almost markedly different".[32] By their nature, organized crime groups may cross various jurisdictions, which complicates national law enforcement authorities' efforts to obtain evidence and prosecute members and associates of

[28] The *Strategy* drew upon a threat assessment of international organized crime to which various agencies contributed.
[29] Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime* (June 2014), p. 1.
[30] *Id.* at 9, 11. *See also generally*, KPMG International, *Issues Monitor: Cyber Crime—A Growing Challenge for Governments* (July 2011).
[31] PricewaterhouseCoopers, *Global Economic Crime Survey—US Supplement*, 2014, p. 14.

groups. Groups move across national borders with less difficulty, in comparison to law enforcement authorities, which are confined to their domestic jurisdictions and which must cooperate with foreign authorities to investigate crimes occurring beyond their borders. Additionally, international groups' elaborate financial and personnel structures, and prosecuting such groups, is time-consuming and expensive.

A. Successful Methods against Cybercrime Groups

The *Strategy* identifies four priority areas for the federal government to address against cybercrime groups and other international organized crime groups: 1) gathering and making use of information and intelligence; 2) setting priorities and targeting the most significant threats; 3) using the resources of the government in partnership with foreign authorities; and 4) using the enterprise model in investigating and prosecuting criminal enterprises to dismantle them.[33]

While various methods have been used successfully, this section offers examples of the use of an undercover operation, an informant, and RICO against cybercrime groups.

1. Undercover Operations

One prominent example of the effectiveness of undercover operations against cybercrime groups is the FBI's and U.S. Secret Service's investigation from 2006 through 2008 of DarkMarket, an Internet forum for buying and selling personal data used in perpetrating fraud. The forum, which *The Guardian* newspaper called the "top English language cybercrime site in the world", cost the banking industry tens of millions of dollars.[34] As news articles reflect, FBI Special Agent J. Keith Mularski spent roughly two years undercover on DarkMarket, posing as a cybercriminal, and infiltrating the forum. Mularksi, operating under the nickname "Master Splynter", inserted himself into DarkMarket's shadowy world of cybercrime, and gradually gathered information about the organization and the individuals buying and selling personal data over it. Eventually, Mularski earned the trust of DarkMarket's founder, later revealed to be Renukanth Subramaniam, nickname "JiLsi," who was then living in London. In an interview with *CNet News*, Mularski explained how he capitalized on that relationship to obtain greater access to the forum and its participants:

> I had good relations with the administrator whose alias was "Jilsi." He wasn't a very technical guy and was having problems running the site because it was getting attacked by a rival group. So I told him about my background as a spammer and told him how good I was at setting up sites. I did some demonstrations and set up some test sites to show him I had the skills. Then there was just a lot of talk and rapport building. One night when DarkMarket was getting attacked by a rival group I said I was ready and that I could secure the server for him and he said "let's move." That gave me full access to everyone using it and what they were doing.[35]

Thanks to Mularski's penetration of the criminal organization, he was ultimately able to control and monitor the forum from an FBI computer in Pittsburgh, Pennsylvania. In 2008, law enforcement authorities dismantled DarkMarket and began arresting alleged members of the forum around the world. Eventually, 60 alleged members were arrested in the United States, the United Kingdom, Germany, and Turkey, including DarkMarket founder Subramaniam, who pleaded guilty to charges in January 2010 in London.

2. Informants

The government's prosecution of Shadowcrew shows both the advantages and risks of using an informant. With the help of an informant, identified in court documents and media reports as Albert Gonzalez, the government investigated and prosecuted Shadowcrew, an Internet forum that allegedly facilitated computer hacking and the distribution of stolen credit card, debit card, and bank account numbers, as well as counterfeit identification documents. Gonzalez, who had been working as a "moderator" on Shadowcrew,

---

[32] United States Attorney General Michael Mukasey, *Remarks Prepared for Delivery by Attorney General Michael B. Mukasey on International Organized Crime at the Center for Strategic and International Studies* (23 April 2008). Available at https://www.justice.gov/archive/criminal/icitap/2008/04-23-08-mukasey-speech.pdf (accessed on 1 May 2017).

[33] United States Department of Justice, *The Law Enforcement Strategy to Combat International Organized Crime*, p. 1.

[34] Caroline Davies, "Welcome to DarkMarket – global one-stop shop for cybercrime and banking fraud", *The Guardian*, 14 January 2010.

[35] Elinor Mills, "Q&A: FBI agent looks back on time posing as a cybercriminal", CNet, 29 June 2009. Available from https://www.cnet.com/news/q-a-fbi-agent-looks-back-on-time-posing-as-a-cybercriminal/ (accessed on 25 April 2017).

agreed to become an informant for the government after his arrest in July 2003, and provided assistance to the investigation. *The New York Times* described his work as an informant:

> After he agreed in 2003 to become an informant, Gonzalez helped the Justice Department and the Secret Service build, over the course of a year, an ingenious trap for Shadowcrew. Called Operation Firewall, it was run out of a makeshift office in an Army repair garage in Jersey City. Gonzalez was its linchpin. Through him, the government came to, in hacker lingo, own Shadowcrew, as undercover buyers infiltrated the network and traced its users around the world; eventually, officials even managed to transfer the site onto a server controlled by the Secret Service. Meanwhile, Gonzalez patiently worked his way up the Shadowcrew ranks. He persuaded its users to communicate through a virtual private network, or VPN, a secure channel that sends encrypted messages between computers, that he introduced onto the site. This VPN, designed by the Secret Service, came with a special feature: a court-ordered wiretap.[36]

In October 2004, 19 of Shadowcrew's alleged members and associates were charged federally in New Jersey for various cybercrimes stretching from 2002 to 2004.

The indictment alleged that Shadowcrew crossed the United States and at least six other countries, and involved approximately 4,000 people.[37] Further, the indictment held the defendants responsible for trafficking in at least 1.5 million stolen credit and bank card numbers, and losses in excess of $4 million.[38] Law enforcement authorities estimate that, if Shadowcrew had not been stopped, the credit card industry may have faced losses totaling hundreds of millions of dollars.[39] To date, except for two fugitives, all of the Shadowcrew defendants located in the United States have pleaded guilty and received sentences, ranging from probation up to 90 months in prison.[40]

However, the government's successful use of Gonzalez as an informant demonstrates the risks of using informants. As news reports show, the government later learned that Gonzalez committed crimes behind the government's back while he worked as an informant. At the time Gonzalez was aiding the government's investigation of Shadowcrew, and after he ceased working as an informant, Gonzalez worked with other cybercriminals to obtain access to payment card accounts in the computer databases of large corporations. In total, Gonzalez and others gained access to roughly 180 million accounts, including accounts in the databases of large U.S. companies, such as OfficeMax and the T.J. Maxx and Marshalls clothing chains. According to the government, the loss exposure for the victim companies for the data breaches was more than $400 million in reimbursements and forensic and legal fees. In March 2010, Gonzalez was sentenced to two concurrent 20-year prison terms, which he is currently serving. At one of his sentencing hearings, the judge stated: "What I found most devastating was the fact that you two-timed the government agency that you were cooperating with, and you were essentially like a double agent."[41]

3. RICO

While the use of RICO is new in cybercrime cases, it has also proven to be an effective method. On December 6, 2013, a federal trial jury in Las Vegas, Nevada reached the first RICO conviction of a defendant for cybercrime offences. At trial, the government presented evidence that the defendant, David Ray Camez, and others participated in an organization known as "Carder.su", an alleged marketplace for the distribution and sale of stolen personal and financial information, that reportedly had an estimated 5,500 members in July 2011. On May 15, 2014, a federal judge sentenced Camez to 20 years in prison for his offences, and ordered him to pay $20 million in restitution.[42] In total, 56 defendants were charged in four indictments, as part of

---

[36] James Verini, "The Great Cyberheist", *The New York Times Magazine*, 10 November 2010. Available from https://mobile.nytimes.com/2010/11/14/magazine/14Hacker-t.html (accessed on 25 April 2017).
[37] United States Department of Justice, *Nineteen Individuals Indicted in 'Carding' Conspiracy* (28 October 2004). Available from https://www.justice.gov/archive/criminal/cybercrime/press-releases/2004/mantovaniIndict.htm (accessed on 26 April 2017).
[38] United States District Court for the District of New Jersey, *United States v. Mantovani, et al.* (28 October 2004).
[39] United States Secret Service, *U.S. Secret Service's Operation Firewall Nets 28 Arrests* (28 October 2004). Available from https://www.scribd.com/document/1220697/US-Treasury-pub2304 (accessed on 26 April 2017).
[40] *See* United States Department of Justice, *Houston Man Sentenced to 90 Months for Identity Theft* (11 July 2006). Available from http://www.usdoj.gov/opa/pr/2006/July/06_crm_424.html (accessed on 26 April 2017); U.S. Attorney's Office, District of New Jersey, *'Shadowcrew' Identity Theft Ringleader Gets 32 Months in Prison* (29 June 2006).
[41] Verini, "The Great Cyberheist".

Operation Open Market, which targeted the Carder.su organization. As of December 2015, 33 individuals have been convicted, with the remaining defendants being either fugitives or awaiting trial.[43]

V. CONCLUSION

This article has examined three forms of organized crime groups—the Mafia, gangs, and cybercrime groups—and offered case studies of effective law enforcement tools against each group. While these three groups and the case studies about them are not an exhaustive survey, they serve as an introduction to helpful law enforcement tools. These tools may be used effectively against various types of organized crime groups, even as groups differ in their predicate offences, structures, modes of operations, and unifying purposes. As organized crime groups constantly evolve, so must the methods used against them. Each organized crime group has a weakness, whether it is a violent gang operating openly on the streets of a city, or a secretive cybercrime group that stretches across the world. Law enforcement agencies, working collaboratively within and across countries, must constantly search for new ways to capitalize on such weaknesses, use investigative and prosecutorial tools that befit each situation, and bring those organized crime groups to justice.

[42] United States Department of Justice, *Member of Organization That Operated Online Marketplace for Stolen Personal Information Sentenced to 20 Years in Prison* (15 May 2014).
[43] United States Department of Justice, *Member of Organized Cybercrime Ring Sentenced to 150 Months in Prison for Selling Stolen and Counterfeit Credit Cards* (9 April 2015).