Chapter Three

TRANSNATIONAL CRIMINAL NETWORKS[1]

Phil Williams

Editors' abstract. Many old-style criminal hierarchies (e.g., the Italian Mafia) are reorganizing into sprawling transnational networks. Williams (University of Pittsburgh) analyzes this trend, with an emphasis on developments unfolding in Russian criminal organizations. He draws on the academic literatures about social and business networks to deepen our understanding of this phenomenon. The chapter builds upon earlier articles in which he pioneered the study of transnational criminal organizations from network perspectives, notably "The Nature of Drug-Trafficking Networks," Current History, *April 1998.*

In a recent analysis of global trends, the U.S. National Intelligence Council included a short section on criminal organizations and networks. It noted that

> criminal organizations and networks based in North America, Western Europe, China, Colombia, Israel, Japan, Mexico, Nigeria, and Russia will expand the scale and scope of their activities. They will form loose alliances with one another, with smaller criminal entrepreneurs, and with insurgent movements for specific operations. They will corrupt leaders of unstable, economically fragile, or failing states, insinuate themselves into troubled banks and businesses,

[1]The author thanks John Picarelli, Bill Koenig, and Paul N. Woessner for a series of helpful discussions on the role of network analysis in intelligence; and Gregory O'Hayon, William Cook, Jeremy Kinsell, and Brian Joyce for their work at the University of Pittsburgh's Ridgway Center in mapping Russian and other criminal networks. He also thanks the I2 Company for providing the software used for these activities.

> and cooperate with insurgent political movements to control substantial geographic areas.[2]

In other words, there is a growing recognition that organized crime is increasingly operating through fluid network structures rather than more-formal hierarchies.

However, the traditional paradigm for studying organized crime emphasized identifying the hierarchical or pyramidal structures of criminal organizations. Finding its fullest expression in the 1967 report on organized crime by the President's Commission on Law Enforcement and Administration of Justice and in Donald Cressey's famous analysis in *Theft of the Nation*, this interpretation of organized crime was based on the example provided by La Cosa Nostra in the United States. It emphasized the existence of a "nationwide illicit cartel and confederation," the governing role of a national commission, hierarchical structure, and the clear division of labor between local branches.[3]

Cressey's analysis, though, provoked several pioneering studies that challenged the mainstream interpretation of organized crime as having a rational corporate structure, arguing not only that organized crime was much more fluid than portrayed by the conventional wisdom, but also that patron-client relations and network structures played a pivotal role. Francis Ianni looked at the role of African American and Puerto Rican criminal networks in New York, while Joseph Albini contended that even Italian organized crime in the United States could best be understood through patron-client relations rather than formal hierarchies.[4] In an important historical study of organized crime in New York, Alan Block discovered that it was not only more fragmented and chaotic than believed, but also that it involved

---

[2]National Intelligence Council, *Global Trends 2015* (Washington: National Intelligence Council, December 2000) p. 41.

[3]For an excellent excerpt summarizing Cressey's views, see Donald R. Cressey, "The Functions and Structure of Criminal Syndicates," in Patrick J. Ryan and George E. Rush, eds., *Understanding Organized Crime in Global Perspective* (London: Sage, 1997) pp. 3–15, especially p. 3.

[4]Francis J. Ianni, *Black Mafia: Ethnic Succession in Organized Crime* (New York: Simon and Schuster, 1974), and Joseph Albini, *The American Mafia: Genesis of a Legend* (New York: Appleton, Crofts, 1971).

"webs of influence" that linked criminals with those in positions of power in the political and economic world. These patterns of affiliation and influence were far more important than any formal structure and allowed criminals to maximize opportunities.[5]

More recently, Gary Potter has suggested that organized crime in the United States can best be understood in network terms, while Finckenauer and Waring, in a study on Russian émigré criminals in the United States, concluded that they operate largely through network structures.[6] Of particular importance is the work of Malcolm Sparrow, who not only applies concepts from social network analysis to the operation of criminal networks, but also offers innovative insights into ways in which the vulnerabilities of these networks might be identified and exploited.[7] My own work has also moved in this direction.[8]

This emphasis on criminal networks reflects a growing acknowledgment, among researchers into crime, that there is no single, dominant organizational structure with universal applicability, and the realization by law enforcement agencies that they are seeing patterns of organized crime that do not fit the traditional hierarchical structure. The German BKA (the equivalent of the American FBI), for example, has observed that most of the criminal organizations it investigates are "loose, temporary networks" and that "lastingly established, hierarchical structures" are rather in the minority. In the BKA's view, the evidence in Germany suggests that even hierarchical organizations

---

[5]Alan Block, *East Side–West Side: Organizing Crime in New York 1939–1959* (Swansea U.K.: Christopher Davis, 1979).

[6]Gary Potter, *Criminal Organizations: Vice Racketeering and Politics in an American City* (Prospect Heights, Ill.: Waveland Press, 1993), and James O. Finckenauer and Elin J. Waring, *Russian Mafia in America* (Boston: Northeastern University Press, 1998).

[7]Malcolm K. Sparrow, "The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects," *Social Networks,* Vol. 13, No. 3, September 1991, and "Network Vulnerabilities and Strategic Intelligence in Law Enforcement," *International Journal of Intelligence and Counterintelligence,* Vol. 5, No. 3, Fall 1991.

[8]See Phil Williams, "Transnational Criminal Organisations and International Security," *Survival,* Vol. 36, No. 1 (Spring 1994), pp. 96–113, and "The Nature of Drug Trafficking Networks," *Current History,* Vol. 97, No. 618 (April 1998) pp. 154–159.

such as the Italian Mafia families allow their local branches considerable discretion.[9]

Perhaps even more significant, a major study of organized crime in Holland noted great variations in collaborative forms and concluded that

> the frameworks need not necessarily exhibit the hierarchic structure or meticulous division of labor often attributed to mafia syndicates. Intersections of social networks with a rudimentary division of labor have also been included as groups in the sub-report on the role of Dutch criminal groups, where they are referred to as cliques. As is demonstrated . . . there can be sizeable differences in the cooperation patterns within these cliques and between the cliques and larger networks of people they work with on an incidental basis.[10]

In other words, there is a growing recognition that organized crime often operates through fluid networks rather than through more formal hierarchies.

Important as they are, none of these studies systematically explores the advantages of network structures as an organizational form for criminal activities. This chapter identifies both the characteristics of networks that make them an ideal form for organizing criminal activities and the specific characteristics of criminal networks themselves. This conceptual analysis of criminal networks also draws insights from social network and business theories and moves beyond theory to draw implications for policymakers concerned with developing strategies to combat criminal networks.

BACKGROUND ON NETWORK ANALYSIS

Networks are one of the most common forms of social organization. They are simultaneously pervasive and intangible, ubiquitous and invisible, everywhere and nowhere. Networks are not an exclusive orga-

---

[9]FBIS, "BKA Registers Less Damage Caused by Gangs," *Frankfurter Rundschau,* July 13, 1998, p. 3.

[10]Cyrille Fijnaut, Frank Bovenkerk, Gerben Bruinsma, and Henk van de Bunt, *Organized Crime in the Netherlands* (The Hague: Kluwer Law International, 1998) p. 27.

nizational form and often exist within more traditional hierarchical structures, cutting through divisions based on specialization or rank. It is also possible to have networks in which hierarchical organizations are key participants. Networks are also an important complement to markets, making them more efficient, reducing transaction costs, and providing increased opportunities for both buyers and sellers.

These characteristics—their pervasiveness, their capacity to coexist both within and outside hierarchies, their ability to make markets more efficient by facilitating directed flows of information and commodities—give networks an elusive quality. In some respects, they appear little more than plastic organizations that can be molded in many different ways.

Networks vary in size, shape, membership, cohesion, and purpose. Networks can be large or small, local or global, domestic or transnational, cohesive or diffuse, centrally directed or highly decentralized, purposeful or directionless. A specific network can be narrowly and tightly focused on one goal or broadly oriented toward many goals, and it can be either exclusive or encompassing in its membership.

Networks facilitate flows of information, knowledge, and communication as well as more-tangible commodities. As communications have become cheaper and easier, networks have expanded enormously. Indeed, technological networks facilitate the operation of larger and more-dispersed social networks and can even act as a critical force multiplier for certain kinds of social networks. Against this background, the analysis here seeks to:

- Delineate very briefly the underlying concepts and ideas that encourage and facilitate analysis of criminal organizations in terms of network structures. These include social network analysis, a growing literature on network business organizations (a concept developed most fully in the idea of the virtual corporation), and previous studies of organized crime that have emphasized the importance of networks rather than the more traditional hierarchical structures.

- Identify the characteristics of networks that make them attractive to criminals and to elucidate further the major characteristics of criminal networks.
- Specify critical roles in criminal networks, bearing in mind that there are network roles that relate to the functioning of the network and substantive roles related specifically to the nature of the criminal enterprise. In some cases, these two roles might overlap; in others, however, they will be quite distinct.
- Highlight and assess the operations of criminal networks. In effect, the analysis will examine a case study of a criminal network that penetrated a legal institution—the Bank of New York.
- Outline ways in which governments and law enforcement agencies can attack networks more effectively. This requires an analysis of network vulnerabilities and how these can be exploited.

Some Underlying Analytic Concepts

The Network. A network can be understood very simply as a series of nodes that are connected. The nodes can be individuals, organizations, firms, or computers, so long as they are connected in significant ways. The focus here, of course, is on networks that originate and operate in order to obtain financial rewards through and from illicit activities. As such, this analysis draws on three separate strands of research: social network analysis, discussions of network business organizations, and previous work on criminal organizations (work that departs significantly from the emphasis on formal hierarchies that was long part of the dominant paradigm in the study of organized crime).

Social Network Analysis. Social network analysis originated in several fields, including anthropology, sociology, and social psychology. Perhaps the most important of the early pioneers was J. L. Moreno, who, in the 1930s, developed the notion of a "sociogram." This was

> a picture in which people (or more generally any social units) are represented as points in two-dimensional space, and relationships

among pairs of people are represented by lines linking the corresponding points.[11]

The essence of this type of approach is its focus on "the relationships or ties between the nodes or units in the network." These ties can be based on a variety of underpinning factors, such as "kinship, material transactions, flow of resources or support, behavioral interaction, group co-memberships, or the affective evaluation of one person by another."[12] In many cases there will be some kind of exchange between the nodes, whether of commodities or services (broadly defined to include information and favors). Whatever the basis for the relationship, however, the network concept emphasizes the linkages among actors.

Accordingly, social network analysis examines such issues as the importance or prominence of particular individuals in the network; the concept of centrality, i.e., the individual in the network with the most—or most important—ties to other actors; the notions of closeness and distance based on communication paths among the actors in the network; the notion of cohesive subgroups, that is, subsets of actors among whom there are relatively strong, direct, intense, frequent, or positive ties; the extent to which the relationships and transactions within it are regulated by explicit or tacit rules; and the number and diversity of actors within the network. Whatever the focus, however, there is a recognition of the flexibility and dynamism of social networks, qualities that stem from the ways in which ties are constantly formed and strengthened or weakened and broken.

Partly because of this dynamism, some sociologists conclude that network-based organizations are capable of superior performance than are more traditionally structured hierarchical organizations, especially in terms of adaptability to changes in their environment. This conclusion is reinforced by a growing literature on business networks—literature that has particular relevance to the discussion here since organized crime is perhaps best understood in quasi-

[11]Stanley Wasserman and Katherine Faust, *Social Network Analysis: Methods and Applications* (Cambridge: Cambridge University Press, 1994) pp. 11–12.

[12]Ibid. p. 8.

Clausewitzian terms as the continuation of business by criminal means.

Business Networks. The focus on networks in business has emerged in response to the limitations, rigidities, and inefficiencies associated with strict hierarchical structures, the need to exploit globalization through partnerships and strategic alliances, and a desire to emulate the Japanese success with the *keiretsu* (regularized networks of suppliers that enhance the efficiency of the production process). It has also emerged out of a recognition that understanding the opportunities provided by "structural holes" (see below) can be critically important for the success of a business in a competitive environment.[13]

The notion of business networks has been developed most explicitly, however, in the concept of the virtual corporation and its dependence on what are sometimes termed "agile networks."[14] Such notions place considerable emphasis on flexible internal communication networks; connections to other organizations; shared interests in obtaining certain outcomes; the need to respond rapidly to external opportunities and challenges; the capacity for environmental scanning, rapid information-processing, and quick decisionmaking; and the capacity of the organization to learn and adapt.

It is clear even from this abbreviated discussion of network organizations in business that a rich and varied research agenda has resulted in many important insights, some of which are as relevant to the functioning of criminal networks as they are to any other kind of enterprise network. Indeed, another important strand of research underlying the present analysis is the studies of networks that have been undertaken by analysts focusing directly on organized crime.

---

[13]Ronald S. Burt, *Structural Holes: The Social Structure of Competition* (Cambridge, Mass.: Harvard University Press, 1992).

[14]See Alf Steinar Saetre and David V. Gibson, *The Agile Network: A Model of Organizing for Optimal Responsiveness and Efficiency,* www.utexas.edu/depts/ic2/aamrc/saetrex.html.

Dimensions of Criminal Networks

Although networks are an important, and somewhat neglected, form of criminal organization, they are not the sole or exclusive form. The traditional hierarchical model long associated with Mafia families in the United States, for example, does not need to be jettisoned: After all, it is possible to have networks of hierarchies, hybrid organizational forms with some hierarchical components and a significant network dimension, and even a network of networks. If networks come in a great variety of shapes, however, they vary along several critical dimensions.

First, a network can be created and directed by a core of organizers who want to use it for specific purposes (a "directed network") or it can emerge spontaneously as a mechanism to add efficiency to the functioning of a market (a "transaction network"). The Colombian cocaine trade in the 1980s and early 1990s was very much a directed network—at least at the core—which came into existence to transport cocaine to the United States. The heroin trade from Southeast Asia, in contrast, is far more of a transaction network, in which brokers play a critical role at almost every stage of the process. Producers supply heroin to independent distributors, and it is then passed along a chain of brokers until it reaches the retail market. In practice, of course, a directed network can be part of a larger transaction network, and it appears that with the demise of the large, vertically integrated networks operating out of Medellín and Cali, the Colombian cocaine trade has increasingly taken on this hybrid quality.

Second, networks can range from small, very limited associations at the local level to transnational supplier networks that move a variety of goods, either licit or illicit—or even both—across national borders. Membership can be determined by a particular characteristic, such as ethnicity, or can be relatively open. Supplier networks are likely to be multiethnic when instrumental considerations outweigh the desire or need to maintain a high degree of exclusiveness.

Among the larger criminal networks, it is possible to identify both key individuals and key companies or firms through which they operate. One of the best examples of an extensive transnational criminal network is that revolving around Semeon Mogilevich. Based in Hungary,

Mogilevich is reputed to have close links with the Solntsevo criminal organization in Moscow, with prostitution activities in Frankfurt, with the Genovese family in New York, and with Russian criminals in Israel. For several years, Mogilevich operated in part through a company called Magnex YBM operating in the United States and Canada (where it was engaged in money laundering—the process of turning criminal proceeds into clean money by hiding origin and ownership—and stock fraud) and also had a network of companies in the Bahamas, the British Channel Islands, and the Caymans. Significantly, as a key figure in this transnational network, Mogilevich is far less vulnerable than a traditional Mafia don or family head, and, despite continued allegations about his role, he has never been convicted of any crime.

Third, networks can be highly structured and enduring in nature or they can be loose, fluid, or amorphous in character, with members coming and going according to particular needs, opportunities, and demands. Some individuals or even small organizations will drift in and out of networks when it is convenient for them to do so. Other networks will have a more enduring membership. In yet other cases, there will be some members who provide continuity (and direction) to the network, while others will play an occasional or ephemeral part. There will be both "embedded ties" and enduring relations based on high levels of trust, mutual respect, and mutual concern; but also more fleeting relations based on nothing more than a short-term coincidence of interests. A similar dynamism is evident in the way in which criminals develop and use front companies, creating them wherever opportunities exist and abandoning or closing them whenever they become the targets of law enforcement investigations.

Last, networks can be focused very narrowly on a single purpose or on the supply of a single product, or they can supply a broader range of illegal products or engage in more diverse criminal activities. Colombian and Mexican drug trafficking organizations, for example, engage in a very narrow range of activities. Although there has been a tendency to traffic in more than one kind of drug, essentially they are in the drug trafficking business and little else. Russian and Chinese criminal organizations, in contrast, have a very diverse portfolio of criminal activities, trafficking in drugs, stolen cars, arms, prostitution, antiqui-

ties, and endangered species, yet also engaging in various forms of extortion and financial fraud.

Whatever their precise characteristics, networks provide criminals with diversity, flexibility, low visibility, durability, and the like. Indeed, their attractions are very considerable:

- Networks can often operate clandestinely. The more visible a criminal enterprise the more likely it is to be attacked by law enforcement. One of the most significant points about networks, however, is that they are not immediately and obviously visible. Criminal networks can hide behind various licit activities, can operate with a lower degree of formality than other types of organization, and can maintain a profile that does not bring them to the attention of law enforcement. In some cases, of course, the network will be exposed. Significantly, though, when the FBI began to investigate the Mogilevich criminal network, there was considerable surprise at its extensiveness.
- Even when they are targeted by law enforcement, many criminal networks are inherently dispersed, with the result that they do not provide obvious centers of gravity or loci for law enforcement attacks. Lacking a physical infrastructure or a large investment of sunk costs that would add significantly to their vulnerability, networks can also migrate easily from areas where risks from law enforcement are high to areas where the risks are much lower.
- Criminal networks, especially when they are transnational in character, can exploit differences in national laws and regulations (Israel, for example, only criminalized money laundering in 2000) by engaging in what might be termed jurisdictional arbitrage. Throughout the 1990s, for example, criminals from the former Soviet Union flooded into Israel, exploiting both the law of return and the lack of anti–money laundering measures. In some cases, money from Russia was used in Israel to buy up virtually bankrupt businesses that would then start to make "profits" that flowed back to Russia. In some instances transnational criminal organizations also create jurisdictional confusion, making it difficult for any single nation's law enforcement agencies to act effectively against them. Laundering money through a series of firms and banks in multiple jurisdictions, for example, makes it arduous and costly for law enforcement to follow the money trail.

- Networks also offer opportunities for both redundancy and resilience. In network structures, it is easier to create redundancies than it is in more formal and rigid organizations—so that even if part of the network is destroyed it can still operate. Furthermore, degradation of a network does not necessarily lead to its demise: Networks are very resilient and can easily be rebuilt.

In view of these advantages, it is not surprising that network structures have become particularly prevalent in contemporary organized crime, whether in the United States, Europe, or states in transition such as Russia, Ukraine, other newly independent states of the former Soviet Union, South Africa, and Cambodia, or even China and Cuba. Accordingly, the analysis now looks at the main characteristics of criminal networks, characteristics that help make them extremely difficult to combat.

TYPICAL CHARACTERISTICS OF CRIMINAL NETWORKS

Network Cores

Networks of any substantial size will generally have both a core and a periphery, reflecting asymmetries of power, influence, and status within the network. The core is characterized by dense connections among individuals who, in the case of a directed network, provide the steering mechanism for the network as a whole. Usually the originators of the criminal enterprise, the core members initiate specific criminal activities, arbitrate disputes, and provide direction. Their relationship is often underpinned by bonding mechanisms that help to create high degrees of trust and cohesion.

In many cases, bonding will be directly related to family or kinship: Many Italian Mafia groups are still organized along family lines, while Turkish drug trafficking and criminal organizations are often clan based. Other bonding mechanisms include ethnicity and common experience in which the participants develop a strong sense of trust and mutual reliance.

Membership in youth gangs or time spent together in prison can also provide critical bonding mechanisms. In the United States, the Mexican Mafia (which is not actually Mexican) started as a prison gang in

Southern California but has developed much more extensively. Yet, it is the common experience that continues to give the core of the network a capacity to operate with confidence that disloyalty or defection are unlikely.[15]

If network cores exhibit strong collective identities, cohesion does not necessarily enhance—and can actually reduce—the capacity to obtain information and "mobilize resources from the environment." Indeed,

> recent trends in network analysis posit an inverse relationship, in general, between the density/intensity of the coupling of network ties on the one hand and their openness to the outside environment on the other.[16]

This explains the attraction of a two-tier structure in which the weaknesses of the core in carrying out the functions of information acquisition are more than offset by the periphery.

Network Peripheries

This zone features less dense patterns of interaction and looser relationships than the core. Yet, these characteristics play a critical role in networks, exhibiting and exploiting "the strength of weak ties."[17] In effect, the periphery allows the network to operate at a far greater distance—both geographically and socially—than would otherwise be the case, facilitating more-extensive operations, more-diverse activities, and the capacity to carry out effective intelligence collection.[18]

---

[15]The analysis here and the discussion of bonding mechanisms rests heavily on Ianni, 1974, pp. 282–293.

[16]See David Stark and Gernot Grabher, "Organizing Diversity: Evolutionary Theory, Network Analysis, and Postsocialist Transformations," in Stark and Grabher, eds., *Restructuring Networks: Legacies, Linkages, and Localities in Postsocialism* (New York and London: Oxford University Press, in press).

[17]Mark Granovetter, "The Strength of Weak Ties," *American Journal of Sociology*, Vol. 78 (1973) pp. 1360–1380.

[18]Ibid. and Burt, 1992.

The Cali cartel, for example, was generally thought of as a highly centralized and structured organization. In fact, it was a networked structure with a set of key figures at the core and a periphery that included not only those directly involved in the processing and transportation of cocaine, but also taxi drivers and street vendors who were an invaluable source of information at the grass-roots level.

For criminal networks, this capacity is critical, because it allows them to anticipate and thereby to neutralize many law enforcement initiatives. Indeed, sensitivity to both threats and opportunities is vital to the continued functioning of criminal networks, making them highly adaptable. In this sense, criminal networks resemble agile corporations: The ability to obtain advance warning is complemented by a capacity for rapid reconfiguration of internal structures and operational activities. Because they have limited fixed assets, networks not only have limited exposure to risks but also adapt in ways that further reduce this exposure and exploit the paths of least resistance.

Criminal Networks As Defensive Structures

If criminal networks usually have early warning mechanisms that provide the first line of defense against law enforcement, there are also additional defensive mechanisms that can be integrated very effectively into their network structures. As I have noted elsewhere:

> Two-tiered networks . . . with both core and periphery have formidable internal defense mechanisms. While it is possible for law enforcement to infiltrate the periphery of the network, getting in to the core is much more difficult partly because entry is dependent on a high level of trust that is based on bonding mechanisms rather than functional utility. Moreover, there will usually be several nodes in the network which act as built-in insulators between core and periphery, distance the core leaders from operations, and make it very difficult for law enforcement to strike at the center of gravity as opposed to nibbling around the edges. The concomitant of this, of course, is that the periphery is where the risks from law enforcement are greatest. Ultimately, however, this is not too serious a problem . . . if parts of the periphery are seriously infiltrated or compromised, they can

> simply be discarded and new members recruited for the outer reaches of the network.[19]

Compartmented networks are good at protecting not only the core membership but also information (while also having effective information flows from periphery to core) that could compromise criminal operations or the integrity of the network. Criminal networks compartmentalize knowledge and information, making it difficult for law enforcement to have more than localized effects on their operations. This is not to deny that, on occasion, there will be defectors or informants whose testimony enables law enforcement to inflict considerable damage, as happened to the Sicilian Mafia in the 1980s.

For the most part, however, networks are very good at self-protection. This is even true when they operate outside the home state—where ethnicity and language become additional defensive mechanisms. U.S. law enforcement agencies, for example, find it difficult to infiltrate Nigerian and Chinese networks in the way they did La Cosa Nostra. Electronic surveillance is also highly problematic since many of the networks use unfamiliar languages or dialects. An additional problem is that criminal networks based on ethnicity are generally located in ethnic communities that offer cover, concealment, and a constant supply of recruits. This is an important factor, for example, in explaining the success of Turkish drug trafficking organizations, and more recently Albanian criminal networks in Western Europe.

Criminal Networks As Facilitators of Cooperation

Even distinctively ethnic networks are not exclusive in their collaboration. Part of the reason for this is that although such networks do not lack organizational identities, they are not overly preoccupied with organizational form. Criminal networks come together with one another when it is convenient or beneficial for them to do so without this being a threat to their identity or *raison d'etre*.

Connections among different criminal networks became a major feature of the organized crime world during the 1990s. Colombian-

[19]Phil Williams, "Drug Trafficking Networks," *Current History* (April 1998) pp. 154–159.

Sicilian networks brought together Colombian cocaine suppliers with Sicilian groups possessing local knowledge, well-established heroin distribution networks, extensive bribery and corruption networks, and a full-fledged capability for money laundering. Italian and Russian criminal networks have also forged cooperative relationships, while Colombian and Russian criminals have been meeting in various Caribbean islands to engage in guns-for-drugs deals. The importance of these network connections has been evident in increased seizures of cocaine imported to, or transshipped through, Russia. There have also been reports of Colombian money laundering activities taking place in Russia and Ukraine, something that would not be possible without some kind of network collaboration. The result of such collaboration, of course, is the creation of a network of networks. These super-networks or pan-networks come into existence for various reasons and operate at a variety of levels, varying in scope, duration, and intensity. As Clawson and Lee put it:

> At the lowest level are simple buyer-seller deals involving relatively small investments, little advance planning, and relatively little interaction between the parties. At the highest level is what might be called strategic cooperation, which encompasses the principles of long-term agreements, large volume shipments of both drugs and money, and the creation of specialized infrastructure to facilitate these flows.[20]

The latter can appropriately be characterized as strategic alliances.

Some criminal networks develop steady supplier relationships with one another along the model of the Japanese *keiretsu,* while others develop contract relationships for the provision of certain kinds of services, such as transportation, security, contract killing, and money laundering. Turkish drug traffickers in Belgium, for example, can buy services from Georgian car thieves to meet their transportation needs.

Even some of the more traditional criminal organizations, such as the Sicilians, are also reliant on networks of cooperation to ply their crim-

[20]Patrick L. Clawson and Rensselaer Lee III, *The Andean Cocaine Industry* (New York: St Martins, 1996) p. 84.

inal trade. Indeed, Turkish drug traffickers in Italy have links with the Sicilian Mafia, the Sacra Corona Unita, and the Calabrian 'Ndrangheta. In 1993, a narcotics trafficking network in Turin involved Calabrians, Turks, Pakistanis, and members of the Cali drug trafficking organization, forming what was clearly a highly cosmopolitan criminal network. In short, the internal flexibility of network organizations is mirrored in the capacity of criminals to form and operate flexible alliances and other cooperative ventures. Indeed, network structures facilitate cooperation among criminal enterprises in the same way they facilitate cooperation in the licit business world.

Criminal networks are also able to draw on a whole set of support structures, whether through acts of paternalism in the community or through more strictly financial considerations. Among the support structures are groups that provide false documentation, front companies, transportation, and a financial infrastructure that can be used to move the proceeds of crime. The creation of false documents facilitates the movement of various kinds of contraband and people and offers an extra layer of protection for those involved in criminal activities. A hint of the scale of the support structure was revealed in May 1998 when agents from the Los Angeles branch of the Immigration and Naturalization Service (INS) disrupted a counterfeit document operation and seized more than 24,000 counterfeit documents, sophisticated printing equipment, and 50,000 blank social security cards.[21]

Criminal Networks As Boundary Spanners[22]

Another closely related advantage of criminal networks is their capacity to flow around physical barriers and across legal or geographical boundaries. Networks transcend borders and are well-suited for business operations in a world where responding to the opportunities and challenges posed by globalization has become an imperative. It is no exaggeration to suggest a natural congruence between transnational

[21]INS, "INS Busts Major Counterfeit Document Ring," Press Release, May 21, 1998.

[22]I am grateful to my colleague Professor Kevin Kearns of the Graduate School of Public and International Affairs, University of Pittsburgh, for bringing this term to my attention.

or cross-border activities and network structures, irrespective of whether the networks operate exclusively in the legitimate sector or in supplying illicit (prohibited or stolen) goods and services.

The capacity to cross national borders creates several advantages for criminal networks. It enables them to supply markets where the profit margins are largest, operate from and in countries where risks are the least, complicate the tasks of law enforcement agencies that are trying to combat them, commit crimes that cross jurisdictions and therefore increase complexity, and adapt their behavior to counter or neutralize law enforcement initiatives. One important boundary crossing, of course, is that between the criminal world and the "upperworld." Criminal networks extend across this boundary in ways that are sufficiently important to require discussion in a separate category, which follows below.

Criminal Networks As Creators and Exploiters of Corruption

In a series of widely cited studies, Ronald Burt has provided considerable insight into the effective functioning of networks by means of his concept of structural holes. Defining structural holes as the separation between nonredundant contacts, Burt contends that the information benefits provided by large diverse networks are greater than those provided by small homogenous networks since size and diversity provide more nonredundant contacts.[23] Consequently, extending networks to cover structural holes provides important competitive advantages.

Closely related to this, he argues, relationships can be understood as social capital that can be exploited to benefit the enterprise. Networks provide access to people with specific resources, which create mutually advantageous information benefits and exchange relationships.[24] This is as relevant to organized crime as to business and helps to explain why criminal organizations extend their networks into the licit world. Further, extending a network into government provides access to both information and power.

[23]Burt, 1992.

[24]Ibid.

For criminal networks, spanning structural holes is particularly beneficial when it also involves crossing from one domain into another. By crossing from the underworld into the worlds of government, business, and finance, criminal networks not only identify and exploit new criminal opportunities, but also enhance their capacity to protect existing activities and opportunities.

The specific connections that facilitate criminal entry into the licit world can be understood as gateways or portals, while the relationships at the boundaries of the criminal network and the world of government and/or licit business can prove vital to a whole series of criminal operations and activities. For criminal organizations involved simply in theft, for example, the critical node is the person who can fence the goods, who in effect transfers them from the criminal network back into the world of legitimate business and commerce.

At a more sophisticated level are found the lawyers, accountants, bankers, and other financial professionals who help criminals both to conceal and to invest their profits. This facilitates the flow of criminal proceeds back into the legitimate financial system, where it rapidly becomes indistinguishable from money that has been obtained by legal means. In New South Wales, for example, lawyers, accountants, and financial managers have been categorized as "gatekeepers" for organized crime and targeted accordingly.

Perhaps most important of all, however, are the members of law enforcement agencies and government officials whose link to criminal networks involves exchange of information or protection for money. In the case of politicians, the exchange can be about personal gain but might also be about assistance in mobilizing the vote, support for electoral campaigns, criminal assistance in providing information about political opponents, or even in intimidating and, in extreme cases, eliminating political enemies. In the case of law enforcement personnel or members of the judiciary, the aim of the criminals is to minimize risks by undermining enforcement efforts, suborning the judicial process, and neutralizing the criminal justice system.

In short, criminal organizations extend their reach by coopting individuals and organizations in ways that facilitate, enhance, or protect

their activities. The corruption networks they create are dynamic rather than static, increasing in significance as corrupted officials become more senior. In these circumstances, the exchange relationship between them becomes much more substantial in terms both of the favors done by the official and the payoffs provided by the criminal. While the official is not part of a criminal enterprise, he has become a vital node in a criminal network, providing important services including timely intelligence about law enforcement initiatives. In countries such as Turkey, Mexico, Colombia, Nigeria, and Russia, criminal networks have extended their reach into the domains of both commerce and government, thereby increasing their capacity to accrue large profits while simultaneously reducing the risks they have to confront.

Criminal Networks As Robust and Resilient Organizations

Networks are highly resilient, partly because of what might be termed loose coupling. Charles Perrow distinguishes between tightly coupled and loosely coupled systems. He contends that tightly coupled systems are the least stable because disturbances involve a chain reaction or, at the very least, serious knock-on effects. In contrast, "loose coupling gives time, resources, and alternative paths to cope with the disturbance and limits its impact."[25] Criminal networks—apart from the core—are based largely on loose coupling. Even if some parts of the network are destroyed, the effects are limited since other parts are left intact. In a loosely coupled network, knock-on or cascading effects are limited and damage to one part of the network does not undermine the network as a whole. Loose coupling also preserves more diversity, in response offering considerable latitude in the decision of which parts of the network should respond, in what manner and in what location.

Resilience, however, stems not only from the capacity to limit the damage that is inflicted but also from the ability to mitigate consequences. Criminal networks often develop certain forms of redundancy that facilitate recovery if part of the network is degraded or damaged. In legitimate business, redundant contacts in networks—

[25]See Charles Perrow, *Normal Accidents* (New York: Basic Books, 1984) for a fuller analysis of tight and loose coupling. The quote is from p. 332.

and indeed redundancy in general—are generally seen as wasteful and inefficient. For criminal networks, such costs are greatly outweighed by the benefits of redundancy in the face of attack and degradation by law enforcement.

The more redundancy in the network, the more options there are to compensate for law enforcement successes whether in finding new ways of moving illicit commodities to the market or alternative routes and methods of repatriating profits. In effect, redundancy enables members of the network to take over tasks and responsibilities from those who have been arrested, incarcerated, or killed by law enforcement. The diversity of different connections allows the network to function even if some connections are broken—not least because the nodes and connections that remain intact can be redirected. In effect, network redundancy makes it possible to maintain organizational integrity even in an extremely inhospitable environment.

Criminal Networks As Synergistic Organizations

Although social networks exist independently of technological networks, there are major synergies among the two distinct network forms. The ability of transnational criminal networks to exploit the information and communication networks that developed during the 1990s provides major multiplier benefits. While exploitation of information technologies is certainly not the sole prerogative of network-based organizations, networks are extremely well placed to exploit new technological opportunities. Indeed, many criminal organizations have been using technology as a force multiplier to carry out their entrepreneurial activities with greater efficiency at lower cost.

There is one set of technologies in particular that could give them an enormous advantage in their continued competition with law enforcement—strong forms of encryption. One of the most potent weapons of law enforcement in its struggle with organized crime has been the capacity to monitor communications among criminals—in effect, to identify and listen in on network connections. Encryption provides opportunities to neutralize this capacity and offers criminal networks a form of strategic superiority—the equivalent of an effec-

tive strategic defense initiative, at very low cost and based on off-the-shelf technologies.

In sum, criminal networks provide moving and elusive targets that operate across enemy lines, infiltrating law enforcement agencies and governments, avoiding confrontation in favor of cooption and corruption. They are resistant—although not impervious—to damage and have qualities that facilitate recuperation and regeneration. Before looking more fully at criminal networks in action, however, it is necessary to identify some of the critical roles that their members must play if the network is to maximize its potential.

ROLES IN CRIMINAL NETWORKS

Networks feature a considerable division of labor among members. Indeed, it is possible to identify a series of critical roles, some of which occur in all networks, and others that are found in specific types of "business" in which criminal networks are involved. In some networks, the tasks will be implicit and intuitive; in others, they are explicit and formal. In most criminal networks, the following roles are likely to be discernible:

Organizers. Those core individuals and groups that provide the steering mechanism for the network. These organizers will generally determine the scale and scope of activities and guidance and impetus for their execution.

Insulators. Individuals or groups whose role is essentially to insulate the core from the danger posed by infiltration and compromise. These individuals transmit directives and guidance from the core to the periphery of the network. They also ensure that communication flows from the periphery do nothing to compromise the core.

Communicators. Individuals who ensure that communication flows effectively from one node to another across the network as a whole. Their responsibility is to transmit directives from the core group and provide feedback. In some cases, insulators and communicators will be at odds because of competing impulses inherent in their differing responsibilities; in other cases the same individuals will combine both roles and make appropriate trade-offs.

Guardians. Enforcers concerned with the security of the network who take measures to minimize vulnerability to external attack or infiltration. Precautions about exactly who is recruited to the network combine with measures to ensure loyalty through a mix of ritual oaths and latent coercion directed against the new members or their families. Guardians act to prevent defections from the network, or in the event that such defections take place to ensure that the damage is minimized.

Extenders. Those whose role is to extend the network by recruiting new members, by negotiating with other networks regarding collaboration, and by encouraging defectors from the world of business, government, and law enforcement. Where the extenders are successful, the network will have access to the portals of the licit world discussed above. Among the tactics that extenders typically use are voluntary recruitment through bribery and corruption and involuntary recruitment through coercion, sometimes leavened by the addition of rewards or inducements. Their targets typically include important and powerful politicians who can provide a high degree of protection, bureaucrats in particularly sensitive or pivotal positions, and financial managers who provide access to legitimate financial institutions.

Monitors. Those who ensure the effectiveness of the network and whose responsibilities include reporting weaknesses and problems to the core organizers, who can then initiate remedial action. These network members are particularly crucial in ensuring implementation and providing guidance on appropriate corrective measures where necessary. They ensure that the network is able to adjust to new circumstances and maintain the high degree of flexibility that is critical to the capacity to circumvent law enforcement.

Crossovers. People who have been recruited into a criminal network but who continue to operate in legal institutions, whether governmental, financial, or commercial. Such people not only meet Burt's test of nonredundant contacts, but by operating in a different sphere from most of the network, they are able to provide invaluable information and protection.

These roles appear widely across criminal networks, regardless of their particular specialties. There are, however, other more specific

roles that also have to be filled. Drug trafficking networks, for example, require chemists to oversee the processing of raw materials into finished products. Although such individuals are critical to the productive capacity of the network, their network role might be very limited. Detailed case studies of networks, of course, require the delineation of both general network roles and specific functional roles. The main purpose of the foregoing analysis here, though, is to illuminate the general functions and structures of networks.

CRIMINAL NETWORKS IN ACTION

Criminal networks are characterized by diversity in composition, density of connections, size, structure, shape, underlying bonding mechanisms, degree of sophistication, and scope of activities. This section briefly examines several criminal networks that were either transnational in scope or were the localized components of a transnational network.

The Spence Money Laundering Network

In one case, a money laundering network in New York that was not very sophisticated succeeded in laundering over $70 million for Colombian drug traffickers. The network was a fascinating mix. It included a taxi driver, an honorary consul-general for Bulgaria, a New York City police officer, two rabbis, a firefighter, and an attorney. The network was very amateurish in its methods, bringing large amounts of cash—which represented the proceeds of drug trafficking—to a Citibank branch on a regular basis and thus triggering a suspicious activity report. The deposits were transferred to a bank in Zurich where two employees forwarded the funds to the Caribbean account of a major Colombian drug trafficker. In spite of the diversity of those involved, the movement of the money across jurisdictions, the involvement of banking officials in Zurich, and the ultimate beneficiary, the network exhibited a surprising lack of sophistication.

The Cuntrera-Caruana Clan

A more sophisticated, network-based criminal group is the Cuntrera-Caruana family, which has played a critical role both as network extenders and as a network core for many other evolving criminal networks. For a long time, however, the family was overlooked, and its role in both drug trafficking and money laundering networks was only barely discerned. One reason is that "although structurally they were at the center of things, geographically they were at the outskirts. They did not come from Palermo, they did not move to New York."[26]

Exiled from Sicily in the 1960s, the Cuntrera-Caruanas initially went to Brazil before establishing themselves in Venezuela and Montreal. The clan has been described as

> a close wicker-work of blood-relations composed of family-nucleuses in different countries all over the world, joined with an equal wicker-work of economical and industrial connections, intended to improve their networks for international traffic in narcotics and money-laundering.[27]

As such, the clan provided important nodes in a whole series of drug trafficking and money laundering networks and was critical in linking Colombian drug suppliers with 'Ndrangheta families that distributed cocaine in Italy. In spite of its relatively low profile, the clan has suffered some setbacks. Three of the Cuntrera brothers—Pasquale, Paolo, and Gaspare—were deported from Venezuela in September 1992 and arrested on their arrival in Rome. In 1996, Pasquale Cuntrera was sentenced to 20 years, while his brothers both received 13 years. Nevertheless, the clan continues to operate and is involved in extensive criminal activities in Canada, partly through links with

[26]See Tom Blickman, "The Rothschilds of the Mafia on Aruba," *Transnational Organized Crime,* Vol. 3, No. 2 (Summer 1997) pp. 50–89. The analysis in this paragraph draws heavily on this article.

[27]Ibid.

outlaw motorcycle gangs, Asian-based criminal organizations, Colombian and South American groups, Eastern European–based organizations and Aboriginal-based organized crime groups.[28]

Outlaw Motorcycle Gangs

Another good example of criminal networks is provided by outlaw motorcycle gangs operating predominantly in the United States and Canada, but also in Britain and Scandinavian countries. The most famous are the Hell's Angels, which gradually evolved into criminal organizations, controlling prostitution and engaging in drug trafficking, often specializing in methamphetamine. Individual chapters of the Hell's Angels are organized along hierarchical lines that one close observer has compared to "little armies" with a president, vice president, secretary treasurer, sergeant at arms, and a road captain.[29] At the same time, these nodes are part of a much larger network that is held together by the same ethos, symbols, and sense of identity that often pits them against other outlaw motorcycle gangs.

Although the Angels have approximately 95 chapters in 16 different countries, their presence does not always go unchallenged. Part of this stems from a natural rivalry among different outlaw motorcycle gangs, and part of it stems from conflicts over drugs markets, something that has become increasingly intense as Mexican organizations have taken over much of the methamphetamine trade. In Canada, for example, there was continuing conflict throughout the 1990s between the Hell's Angels and Rock Machine, a gang based in Quebec and Ontario. Periodic outbreaks of open warfare among these groups resulted in several deaths. Even more intense was the conflict in Denmark between the Angels and the Texas Bandidos, a conflict that, on occasion, involved the use of rocket propelled grenades and antitank weapons.[30]

---

[28]Criminal Intelligence Service Canada, *Annual Report on Organized Crime in Canada*, 1998.

[29]Yves Lavigne, *Hell's Angels* (Secaucus N.J.: Lyle Stuart, 1996) p. 68.

[30]Dean E. Murphy, "Biker War Barrels Across Scandinavia: Swedish Legislator Campaigns to Evict Gangs After Rumbles Kill 6," *Los Angeles Times,* August 1, 1996, p. A19.

Immigrant Smuggling Networks

Criminal networks engage in a variety of enterprises, the most lucrative of which is alien smuggling. In 1998, the U.S. Immigration and Naturalization Service, in Operation Seek and Keep, dismantled a network of alien smugglers who for three years had smuggled up to 300 Indian nationals a month to the United States. Their business grossed an average of $70 to $80 million annually. The network had arranged air travel from India to Moscow to Cuba, boats to the Bahamas, and then either boats or planes to Miami. On occasion some of the illegal immigrants went from Cuba to Ecuador and were either brought into the United States via Miami or through Mexico and the southwest border.

The major investigative instrument used by the INS was wiretapping, which led to over 35,000 calls being intercepted. Most of the arrests were made between November 14 and November 19, 1998, and took place in the Bahamas, New York, New Jersey, Miami, Jacksonville, Tampa, Los Angeles, Fort Worth, Houston, Philadelphia, and San Juan, Puerto Rico—a diversity of locations that highlights the network structure of the people-trafficking organization.[31]

Crossover Figures

Most criminal networks extend into the licit world for support. Some of the larger and more powerful criminal networks, however, take this process to considerable lengths and in effect create crossover figures who have very high-level positions in government. Perhaps the most striking examples of this are Guilio Andreotti in Italy and Raul Salinas in Mexico. In the case of Andreotti, he was at the pinnacle of a pattern of collusive relationships between the Christian Democrats and the Mafia, relationships that until the 1980s offered protection and contract opportunities for the criminals and financial payoffs and political support for the Christian Democrat Party.

In Mexico, Salinas was able to amass a personal fortune as his reward for providing high-level protection and support for drug traffickers.

---

[31]INS Press Release, *U.S. Dismantles Largest Global Alien Smuggling Cartel Encountered to Date,* November 20, 1998.

Over $130 million was deposited in Swiss banks, much of it via Citibank in New York. General Guttierez, who was head of Mexico's antidrug unit yet in the pay of major drug traffickers, provides another example of the capacity of criminal networks to insinuate themselves into licit institutions in ways that are highly corrosive of the power, authority, and purpose of these institutions. It is this capacity that makes criminal networks so difficult to attack. Indeed, the next example highlights how a criminal network can embed or nest itself in a legitimate financial institution.

RUSSIAN INVOLVEMENT IN CRIMINAL NETWORKS

Money Laundering and Capital Flight Through the Bank of New York

In autumn 1999, reports appeared that about $15 billion from Russia had been laundered through the Bank of New York. Several officials at the bank were soon suspended. Further revelations suggested links between the Mabetex construction scandal in the Kremlin (in which a Swiss firm paid bribes for a very lucrative renovation contract), the Berezovsky Aeroflot scandal, an Italian criminal organization's money laundering activities, and the funds laundered through the Bank of New York. There were also allegations that one of the key figures in the money laundering was the aforementioned Semeon Mogilevich, a key organized crime figure based in Budapest.

Over the following 15 months, many aspects of the original story were either denied or qualified. Estimates of the amount of money involved were more than halved, and it was also suggested that most of this was capital flight and tax evasion money rather than the proceeds of crime. There was also a sense of frustration in U.S. law enforcement circles: Without the full cooperation of the Russian authorities, proving that prior crimes had been committed in Russia was virtually impossible.

In spite of all these qualifications, the Bank of New York money-laundering operation reveals very clearly the advantages that accrue through embedding a criminal network in a legitimate institution. In effect, what occurred was that a network of people wanting to move money out of Russia took advantage of a Bank of New York policy that

had aggressively sought correspondent relationships with Russian banks without always exercising due diligence. It was this fundamentally sanguine approach—even though in 1994 there was congressional testimony indicating that 40 percent of Russian banks were controlled by organized crime—that made the bank and its officials vulnerable.

Central figures in the scandal were Lucy Edwards and her husband, Peter Berlin, both of whom pleaded guilty to a series of charges. According to court testimony, Lucy Edwards was approached by some Russians in Moscow she had met in her work at the East European division of the Bank of New York. The Russians controlled a bank called DKB and offered to pay Edwards and Berlin if they would assist in moving money from Russia through the Bank of New York. Berlin opened an account at the Bank of New York so that the Russians could obtain access to electronic banking software called micro/CASH-Register, which enabled them to wire-transfer money out of the account. Berlin created a front company, Benex International Company, Inc., (Benex). Lucy Edwards installed the software in a computer located in an office in Forest Hills, Queens, managed by individuals working for DKB. The Russians transferred funds into the Benex account almost daily, then the micro/CASH-Register software was used to transfer it to other accounts around the world.

In July 1996, Peter Berlin opened a second account at the Bank of New York in the name of BECS. In the fall of 1998, the Russians acquired control of Flamingo Bank and wanted a new bank account through which they could transmit funds on behalf of Flamingo. Berlin opened a third account in the name of Lowland and once again obtained micro/CASH-Register software. The Russians set up an office for Lowland in New Jersey.

In April 1999, Flamingo Bank began transferring large sums of money into the Lowland account using micro/CASH-Register software located in Russia to wire-transfer funds out. This facilitated contravention of Russian currency regulations and avoidance of custom duties and taxes. The scheme was also used to pay $300,000 in ransom on behalf of a Russian businessman who had been kidnapped in Russia. With around $7 billion passing through the accounts, Berlin and Edwards received a total of $1.8 million in commission payments.

In effect, this was a premier example of the way in which a criminal network, by coopting a critical and trusted bank official, is able to circumvent banking supervision and due diligence requirements, and embed or nest its activities within a legal and indeed highly reputable institution. In many ways, this is very typical of the style of Russian organized crime, the only difference being that, in this case, a Western financial institution and not simply a Russian bank was compromised.

Russian Organized Crime

Russian organized crime is a sprawling phenomenon that differs from city to city. It embraces ethnically based, non-Russian groups such as Chechens and Azeris and has developed symbiotic links with state and law enforcement apparatus in Russia. Russian criminal organizations also control a considerable portion of Russia's economic activity and have infiltrated key sectors of the Russian economy, such as banking, the aluminum industry, and the St. Petersburg oil and gas sectors. Although some of the major organizations have hierarchical structures, Russian organized crime can only be fully understood in terms of network connections between the underworld and the upperworld.

There are three manifestations of this phenomenon that are particularly important. First, there is cooperation among criminals, businessmen, and politicians who are part of the new iron triangle of network relationships that dominate Russian life. Using network analysis and software tools such as Analyst's Notebook, discussed more fully below, it is possible to trace some of these linkages. In some cases, the connections are made through common financial interests in one or more companies—interests that often make strange and surprising bedfellows.

Next, there is the use of violence to manage relationships that are anything but cooperative. For example, when criminal networks attempt to extend their influence into legitimate businesses and meet resistance, those resisting are often eliminated. Indeed, contract killings have become an important instrument of organized crime—and

also a very visible indicator of organized crime infiltration of licit businesses or economic sectors.

Finally, there are figures who operate in both domains. One of the most notable of these figures is Yuri Shutov, a St. Petersburg Duma deputy who, until his arrest, ran a much-feared assassination squad. Shutov's team carried out a series of contract killings aimed at eliminating criminal rivals, removing obstacles to criminal takeover of the energy sector, and neutralizing threats from law enforcement authorities and reformist politicians.

CONFRONTING CRIMINAL NETWORKS

It is clear from the foregoing examples of criminal networks in action that they are formidable. This does not mean that they are invulnerable, however. Indeed, there are several ways in which governments and law enforcement agencies can respond more effectively to the challenges posed by criminal networks.

Although criminal networks are resistant to disruption and have high levels of redundancy and resilience, they are not impervious to attack by law enforcement. The nature of these networks, however, suggests that the attacks need to be carefully orchestrated, finely calibrated, and implemented in a comprehensive and systematic fashion. Indeed, there are several important prerequisites for initiating effective attacks on networks, especially clear delineation of objectives and enhanced intelligence assessments.

In attacking networks, it is vitally important to determine the major objectives: Are they to destroy the network, simply to degrade its capacity to carry out criminal actions, or to detach the network from its support apparatus in the licit world? The objectives can range from making operations more difficult for the network through creating instability in the environment to more direct attacks on the network itself that are aimed at disruption of its activities, dislocation or degradation of its capabilities, or even its compete destruction. While all are legitimate objectives, it is essential that there is clarity about precisely which of them is being chosen.

Even clear articulation of objectives is no guarantee that they will be achieved. One of the major problems in dealing with criminal networks is the absence of adequate models about precisely how these networks function. This is paralleled in the business world by a lack of understanding of why business networks succeed or fail. In neither domain has there been sufficient comparative work identifying patterns of success or failure. Specifically in relation to criminal networks, there has been little sustained empirical research on how these networks respond to different law enforcement initiatives. It is clear that networks react quickly and effectively to measures such as interdiction efforts and, for example, move their operations or find new modes of concealment and deception.

What is less clear, however, is the exact nature of their response when damage is inflicted upon them. If part of the network is compromised, for example, is it simply jettisoned or amputated and other components given increased responsibilities in an attempt to compensate, or are efforts made to regenerate the damaged portion of the network? Similarly, it is not always clear where the network starts and ends and whether an apparently successful attack has actually fulfilled its objective of significantly degrading or destroying the network. Damage assessment is always difficult; when it involves networks, it is even more problematic than usual.

To overcome these problems it is essential to develop more effective intelligence about criminal networks. In this connection, various software companies, working closely with the law enforcement community, have developed some important tools to assist with the intelligence analysis task. The three major packages are Analyst's Notebook produced by I2 (see www.i2inc.com), Orion Leads produced by Orion Scientific Systems (www.orionsci.com), and Watson Powercase (formerly owned by Harlequin) available from Xanalys (www.xanalys.com). Although these packages differ slightly in both power and usability (with some trade-offs between these two characteristics), they all have capabilities that assist in the identification of criminal networks. All of them, for example, have a component that facilitates telephone toll analysis of patterns of interaction among key individuals. The results of this analysis can be fed into what is generally referred to as association, network, or link analysis.

Such an approach helps to identify and assess the relationships or connections among people and organizations involved in crime, in effect helping to understand and visualize the network. Although it is often used for tactical purposes and for specific cases, link analysis could also be a valuable tool for strategic purposes. It could help, for example, in identifying some of the more important nodes in the network, in identifying key individuals who carry out the various network functions identified in the previous section, and in locating the portals or gateways through which the criminal network successfully crosses into the licit world. It could also be used strategically as an aid to damage assessment. In effect, the analytic intelligence process facilitates both identification and mapping of criminal networks.

Understanding network structures and operations makes it easier to identify vulnerabilities against which concentrated attacks should be directed. Particularly important in this connection is the identification of critical nodes.[32] A critical node in a network is one that generally has a high level of importance and a low level of redundancy. The importance can reflect the existence of certain specialized skills (which can be substantive in terms of the specifics of the criminal enterprise or related to the operation of the criminal network as a network) or the position of the node within the network. The low level of redundancy stems from the lack of adequate substitutes for those with these skills.

In terms of network functions, a critical node might be a person who is well connected and the focus for dense connections. If this person is removed and there are no readily available communication links, then the network could be severely degraded. On the other hand, even a few alternative communication links can provide the basis for reestablishing enough connectivity for the network to continue to function.

In addition to those nodes that are obviously critical, there are those that can become critical because of more general damage inflicted on

[32]This theme is developed in some very interesting ways by Sparrow, "Network Vulnerabilities and Strategic Intelligence in Law Enforcement," *International Journal of Intelligence and Counterintelligence,* Vol. 5, No. 3, Fall 1991. Sparrow's analysis provided both ideas and inspiration for this section.

the network. These nodes—the ones that are important but highly redundant—can become critical if they are attacked simultaneously or in close succession to one another. While this requires effective coordination, it is certainly an option that needs to be considered.

In attacking networks, it is also critical to target the boundaries, either from one network to another or from the criminal world to the upperworld. Particularly important in this connection are network extenders and crossover figures (defectors from the licit world), individuals who, in effect, straddle the boundary between the licit and illicit sectors and provide an important gateway for the criminals into licit financial, political, administrative, or business institutions.

Indeed, it is essential to disentangle the crime-corruption networks (and the nature of the exchanges between criminals and their clandestine supporters in the licit world) and thereby provide opportunities to detach the network from its various support structures. In part, the struggle between law enforcement and organized crime networks can be understood in terms of a competition in crossovers—informants and defectors from criminal networks on the one side and corrupted politicians, bureaucrats, law enforcement personnel, and members of the judiciary on the other.

Closely related to their ties to the upperworld, criminal networks can become deeply embedded in certain social, political, and economic structures that need to be attacked as a system. Perhaps the best example is the world of offshore financial centers and bank secrecy havens, which can be understood as a set of interlocking services provided to criminal networks that enables these networks to move, hide, and protect the proceeds of their criminal activities. Ironically, the providers of these services enjoy the protection of sovereignty. In effect, this puts the network crossovers out of reach and makes it necessary to attack the support system and not simply the network itself.

The other obvious target for attack is the network core. If the network is functioning effectively, however, and the insulation processes are working as intended, then this will prove extremely difficult. If the core figures are identified and removed, one of two results is possible. The first is that the network is so well-established—with the steering mechanisms so deeply embedded in operational procedures that op-

erations have become more or less independent of the core group—that it can continue to function. A variation on this is that some of the figures who have been close to the core, but not necessarily part of it, can substitute for those removed from the steering group. The second possibility is that attacking the core group will significantly degrade the network and along with other measures, such as an attack on the gateways, will either force it to cease operating or, at the very least, significantly degrade its capacity and reach.

In effect, the options being discussed so far are all part of an external attack on the network. It is also possible to initiate internal attacks on criminal networks, however, where the objective is to create dysfunctional relations that seriously degrade the capacity of the network to function effectively. One option, for example, might be to destroy trust through misinformation and actions designed to create suspicion and acrimony. One way of doing this would be to identify some of the network crossovers and, rather than remove them, use them to feed misinformation into the network. Not only could this have a corrosive internal effect, but also it could encourage the criminals to move in directions that make them increasingly vulnerable to external attack.

One other important component of the response to defeating criminal networks is that governments and law enforcement agencies, in effect, need to mimic network structures. One of the advantages criminal networks enjoy is that they are smart, future-oriented organizations locked in combat with governments that, by contrast, are often hobbled by a variety of constraints. Governments still operate along hierarchical lines and are further hindered by bureaucratic rivalry and competition, interagency antipathies, and a reluctance to share information and coordinate operations. Working from John Arquilla's and David Ronfeldt's proposition that it takes a network to defeat a network, the most successful attacks on criminal networks are likely to be those carried out by innovative law enforcement structures that transcend the normal bureaucratic way of doing business.[33] Joint task forces, in which there are a pooling of resources and

[33]John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, Calif.: RAND, 1997).

information and a concerted attack on a particular criminal network, provide an important value-added approach to attacking criminal networks. They can be particularly useful where they involve transnational cooperation in response to a transnational criminal network.

Joint undercover operations have been particularly successful in this respect, largely because they provide access to crucial parts of the criminal network. Operation Green Ice in the early 1990s, for example, involved law enforcement agencies from eight countries and resulted in around 200 arrests in the United States, Spain, Italy, and Britain. In some cases, cooperation of this kind is even being institutionalized. One of the most forward looking agencies in responding to transnational criminal networks through the creation of its own networks has been the Financial Crimes Enforcement Network at the U.S. Treasury (FINCEN). Although FINCEN has its problems—and has been criticized, among other things, for its lack of performance indicators—its importance reflects the way in which the U.S. government has decided to attack not only criminal kingpins and criminal networks, but also the proceeds of crime. A key part of this has been an effort to combat money laundering by making it more difficult to introduce dirty money into the financial system without triggering either cash transaction reports (CTRs) or suspicious activity reports (SARs). In addition, the United States has developed laws for asset seizure and asset forfeiture that allow the confiscation of criminal profits. FINCEN has played a key role in this strategy and has acted as liaison with the financial community, encouraging banks to take on responsibilities such as "know your customer" requirements and the exercise of due diligence in all transactions. It is also the repository for the information provided by the banks through the CTRs and SARs.

FINCEN is one model of what has become known as a financial intelligence unit (FIU). Many other countries have developed their own variants of these units. Australia, for example, has its Transaction Reports and Analysis Center, known as AUSTRAC, while in Bermuda there is a Financial Investigation Unit. Generally FIUs have reporting and analytic functions; in some countries FIUs also have investigative responsibilities. The challenge, however, is that dirty money has become highly mobile, moving rapidly through multiple jurisdictions before being hidden in safe havens that place a high premium on fi-

nancial anonymity and bank secrecy. The response to this has been to create a network of FIUs known as the Egmont Group. Established in 1997, the Egmont Group FIUs meet regularly for plenary sessions, while also exchanging information through a secure web site. As of May 2000, the Egmont Group had 53 operating units in as many countries. Although the national FIUs vary considerably in terms of skills, resources, and available technology, the network facilitates a multinational effort to combat money laundering. Given the speed, ease, and anonymity with which money can be moved around the global financial system, the Egmont Group, by itself, does not level the playing field, but it does make it less uneven.

Such developments are important, particularly when combined with what is a growing trend toward intelligence-led law enforcement. Yet there is still a gap between the prevalence and sophistication of criminal networks on the one side, and law enforcement networks on the other. Closing this gap and developing more-effective strategies to attack criminal networks has to be one of the priorities in government efforts to combat transnational organized crime in the 21st century. This requires changes in attitudes and ways of thinking, in organizational structures, and in the relationship between intelligence and action. Without these changes, criminal networks will continue to retain important advantages over those who are trying to combat them.