Assessing the Dangers of Illicit Networks

Why al-Qaida May Be Less Threatening Than Many Think

Mette Eilstrup-Sangiovanni and Calvert Jones

The globalization of transportation, communication, and finance has benefited not only licit businesses but also professional criminals and terrorists. Arms dealers, drug traffickers, money launderers, human traffickers, terrorists, and other sundry criminals, enabled by new, affordable technologies, are increasingly organizing into sprawling global networks. As a result, understanding international organized crime and terrorism in terms of networks has become a widely accepted paradigm in the field of international relations. In this article we seek to clarify that paradigm, probe deeper into the consequences of the network structure, and challenge conventional wisdom about network-based threats to states.

A common theme in recent international relations scholarship dealing with organized crime and terrorism is the great difficulty states face in combating network-based threats. According to a growing literature, the primary confrontation in world politics is no longer between states but between states and terrorist networks such as al-Qaida, drug smuggling networks such as those in Colombia and Mexico, nuclear smuggling networks in places such as North Korea and Pakistan, and insurgent networks such as those in Iraq.[1] And states are widely reputed to be losing the battle. The main reason, according to the existing literature, is the organizational advantages enjoyed by networked ac-

Mette Eilstrup-Sangiovanni is Lecturer in International Studies at the Centre of International Studies at the University of Cambridge. She is also Fellow of Sidney Sussex College. Calvert Jones is a doctoral student in the Department of International Relations at Yale University.

1. See, for example, Fiona B. Adamson, "Globalisation, Transnational Political Mobilisation, and Networks of Violence," *Cambridge Review of International Affairs,* Vol. 18, No. 1 (April 2005), pp. 31–49; Jörg Raab and H. Brinton Milward, "Dark Networks as Problems," *Journal of Public Administration Research and Theory,* Vol. 13, No. 4 (October 2003), pp. 413–439; Manuel Castells, *The Rise of the Network Society* (Cambridge, Mass.: Blackwell, 1996); Mark Duffield, "War as a Network Enterprise: The New Security Terrain and Its Implications," *Cultural Values,* Vol. 6, Nos. 1–2 (2002), p. 161; John Arquilla and David Ronfeldt, eds., *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, Calif.: RAND, 2001), especially Phil Williams, "Transnational Criminal Networks," pp. 61–98; Michael Kenney, *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation* (University Park: Penn State University Press, 2007); Audrey Kurth Cronin, "Behind the Curve: Globalization and International Terrorism," *International Security,* Vol. 27, No. 3 (Winter 2002/03), pp. 30–58; Sheena Chestnut, "Illicit Activity and Proliferation: North Korean Smuggling Networks," *International Security,* Vol. 32, No. 1 (Summer 2007), pp. 80–111; and Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004).

International Security, Vol. 33, No. 2 (Fall 2008), pp. 7–44

tors. A fluid structure is said to provide networks with a host of advantages including adaptability, resilience, a capacity for rapid innovation and learning, and wide-scale recruitment. Networked actors are also said to be better at exploiting new modes of collaboration and communication than hierarchically organized state actors. The suggestion that "it takes a network to fight a network" is therefore gaining currency, both among academics[2] and in the wider security community.[3]

We agree that network-based threats pose serious challenges to state security. But, we argue, the prevailing pessimism about the ability of states to combat illicit networks is premature. The advantages claimed for networks vis-à-vis hierarchical organizations in the existing literature are often not well characterized or substantiated. Although they tend to enjoy flexibility and adaptability, networks have important—and often overlooked—structural disadvantages that limit their effectiveness. Given the high premium on battling networked threats, it is surprising that these disadvantages have not received more attention from international relations scholars.

To fill this lacuna, we combine theoretical and empirical evidence to illuminate some important network weaknesses. A caveat is in order. We are neither terrorism experts nor criminologists. Our engagement with the phenomenon of "dark networks" is motivated primarily by dissatisfaction with the growing international relations literature, where the term "network" is often used metaphorically and is not clearly defined or expounded.[4] Little systematic use has been made by this literature of theoretical approaches to networks developed in other social sciences, and too little effort has been made to build on findings from extant studies on terrorism, insurgency, and organized crime. As a result, we argue, strategic thinking about how networks can be combated lacks both imagination and historical grounding.

The article begins with a brief discussion of the term "network" in the social sciences. We first offer a review of the current literature on networks. Next we highlight some limitations that raise doubts about whether networks, in gen-

2. See, for example, Arquilla and Ronfeldt, *Networks and Netwars;* Richard M. Rothenberg, "From Whole Cloth: Making Up the Terrorist Network," *Connections,* Vol. 24, No. 3 (2002), pp. 36–42; and Anne-Marie Slaughter, *A New World Order* (Princeton, N.J.: Princeton University Press, 2004).
3. For an analysis of the influence of this idea on U.S. intelligence reform, see Calvert Jones, "Intelligence Reform: The Logic of Information Sharing," *Intelligence and National Security,* Vol. 22, No. 3 (Summer 2007), pp. 384–401.
4. The term "dark networks" was coined by Arquilla and Ronfelt in *Networks and Netwars.*

eral, and clandestine networks, in particular, are as effective as postulated in their ability to challenge states.[5] In general, we argue, international relations scholars have been too quick to draw parallels to the world of the firm where networked organization has proven well adapted to the fast-moving global marketplace. They have consequently overlooked issues of community and trust, as well as problems of distance, coordination, and security, which may pose serious organizational difficulties for illicit networks.

The second section presents historical evidence on the life cycle and operational effectiveness of networks. Despite a near consensus in the existing literature about the superiority of networks to other forms of social organization, only limited historical and comparative research justifies the claim.[6] To remedy this weakness, we draw from a wider body of research on the dynamics of participation in underground movements, the life cycle of terrorism and insurgency, and vulnerabilities in organized crime to unearth potential sources of network debilitation in greater theoretical and historical depth. In the third section, we use these findings as a springboard for analyzing a contemporary, highly potent networked organization: al-Qaida. Although there is much we do not know about this network, the evidence in the public domain suggests al-Qaida is subject to many of the same weaknesses that have beset clandestine networks in the past. We conclude by exploring the theoretical and practical implications of our findings.

Understanding Networks

The term "network" has been among the most widely used by social scientists in the last four decades. Economists, organizational theorists, sociologists, and anthropologists have long applied the concept to analyze social and economic systems in which actors are linked through enduring formal and informal rela-

5. We are interested only in the organizational advantages that may or may not flow from the network form. We do not address potential advantages stemming from the psychological profiles, belief systems, or other attributes of illicit actors.

6. In international relations, sophisticated single case studies of networks abound, but broad comparative work is rare and often exploratory. See, for example, Arquilla and Ronfelt, *Networks and Netwars*. Exceptions are Michael Kenney, *From Pablo to Osama*, who explores the comparative adaptive abilities of drug trafficking and terrorist networks against centralized law enforcement, and Audrey Kurth Cronin, who compares al-Qaida to earlier terrorist networks. See Cronin, "How al-Qaida Ends: The Decline and Demise of Terrorist Groups," *International Security*, Vol. 31, No. 1 (Summer 2006), pp. 7–48.

tions. More recently, political scientists have adopted the network concept to analyze the organization of nonstate actors at both the domestic and transnational level,[7] to study new forms of public administration linking governments and nongovernmental actors,[8] or to map the international structure.[9] In security studies, scholars increasingly emphasize the role of networks in insurgency, terrorism, and organized crime.[10]

Much research on networks originates in sociology and organizational theory, and its genesis in these fields is central to understanding why networks, in international relations, are thought to be so effective. Economic sociologists have typically invoked the network concept to analyze the shift away from the classical model of a vertically integrated firm, which relies on top-down management, set bureaucratic routines, and centralized investment to minimize transaction costs.[11] This model has been challenged by new forms of horizontal coordination. Many firms now collaborate with competitors, subcontractors, and research institutions through formal and informal networks.

Broadly speaking, the literature finds that a networked structure enables flexible, on-demand production models that are far better adapted to the shortened product life cycles and accelerating technological changes that typify today's globalized economy than hierarchically organized production.[12] As we show below, international relations scholarship has largely imported this logic, without significant revision, in its conception of transnational networks as effective actors. Yet, this logic may be misleading, at least with regard to illi-

7. Margaret E. Keck and Kathryn Sikkink, *Activists beyond Borders: Advocacy Networks in International Politics* (Ithaca, N.Y.: Cornell University Press, 1998).
8. Bernd Marin and Renate Mayntz, eds., *Policy Networks: Empirical Evidence and Theoretical Considerations* (Boulder, Colo.: Westview, 1991); James N. Rosenau and Ernst-Otto Czempiel, eds., *Governance without Government: Order and Change in World Politics* (Cambridge: Cambridge University Press, 1992); and Fritz W. Scharpf, "Coordination in Hierarchies and Networks," in Scharpf, ed., *Games in Hierarchies and Networks: Analytical and Empirical Approaches to the Study of Governance Institutions* (Boulder, Colo.: Westview, 1993), pp. 125–165.
9. Emilie M. Hafner-Burton and Alexander H. Montgomery, "Power Positions: International Organizations, Social Networks, and Conflict," *Journal of Conflict Resolution,* Vol. 50, No. 1 (February 2006), pp. 3–27.
10. See, for example, Raab and Milward, "Dark Networks as Problems"; Arquilla and Ronfeldt, *Networks and Netwars;* Kenney, *From Pablo to Osama;* Cronin, "Behind the Curve"; Chestnut, "Illicit Activity and Proliferation"; and Sageman, *Understanding Terror Networks.*
11. Ronald H. Coase, "The Nature of the Firm," *Economica,* Vol. 4, No. 16 (November 1937), pp. 386–405; and Oliver E. Williamson, *Markets and Hierarchies: Analysis and Antitrust Implications: A Study in the Economics of Internal Organization* (New York: Free Press, 1975).
12. See, for example, Michael J. Piore and Charles F. Sabel, *The Second Industrial Divide: Possibilities for Prosperity* (New York: Basic Books, 1984); and Laurel Smith-Doerr and Walter W. Powell, "Networks and Economic Life," in Neil J. Smelser and Richard Swedberg, eds., *Handbook of Economic Sociology,* 2d ed. (Princeton, N.J.: Princeton University Press, 2005), p. 384.

cit networks. Clandestine organizations—whether terrorist groups, guerrilla movements, or drug-smuggling enterprises—face a unique set of constraints that distinguish them from their legal commercial counterparts, and their effectiveness cannot be reduced to models of economic efficiency. As a result, many advantages claimed for illicit networks in their confrontation with states must be tempered.

DEFINING NETWORKS

Despite growing scholarly attention to the network mode of organization, significant ambiguity remains about what constitutes a network. A formal definition describes a network as "a specific set of relations making up an interconnected chain or system for a defined set of entities that forms a structure."[13] This is a loose definition, designating nothing more than a set of linked elements (or "nodes"). It could refer to a system of computers as well as individuals and could embrace both market and hierarchical structures. In international relations, however, most follow Walter Powell in conceiving of networks as a distinct form of organization, separate from both hierarchies and markets, which link actors working toward common goals.[14] From this perspective, a network can be defined as "any collection of actors ($N > 2$) that pursue repeated, enduring exchange relations with one another and at the same time lack a legitimate organizational authority to arbitrate and resolve disputes that may arise during the exchange."[15] In contrast to markets, exchange relations in networks are enduring; in contrast to hierarchies, networks lack top-down command and authoritative dispute settlement.[16]

Networks come in many shapes and forms, but all are united by a family of structural properties that, taken together, support assumptions about their

13. Grahame F. Thompson, *Between Hierarchies and Markets: The Logic and Limits of Network Forms of Organization* (New York: Oxford University Press, 2003), p. 54.
14. Walter W. Powell, "Neither Market nor Hierarchy: Network Forms of Organization," *Research in Organizational Behavior,* Vol. 12 (1990), pp. 295–336.
15. Joel M. Podolny and Karen L. Page, "Network Forms of Organization," *Annual Review of Sociology,* Vol. 24, No. 1 (August 1998), pp. 58–59.
16. Two broad approaches to network analysis can be distinguished. Social network analysis seeks to reveal how relational ties among individuals affect social outcomes. See Mark Granovetter, "The Strength of Weak Ties," *American Journal of Sociology,* Vol. 78, No. 6 (May 1973), pp. 1360–1380. Organizational network analysis (ONA) focuses on the organizational level of analysis, examining how networked groups make decisions, pool resources, and engage in collective action. See Smith-Doerr and Powell, "Networks and Economic Life," p. 369. Viewing networks as a form of governance, as we do, favors an ONA approach because it assumes the existence of common goals, values, or other considerations sustaining collective action. Networks, on this approach, are seen not merely as sets of linked individuals but as self-conscious collective actors in world politics.

efficacy. First, whereas traditional hierarchies are based on top-down management, networks are flat and decentralized with decisionmaking and action dispersed among multiple actors exhibiting a high degree of local autonomy.[17] Although hierarchy in a traditional sense is absent from the network, the boundaries between networks and hierarchies are not always clear-cut. The existence of relatively few nodes with a large number of connections to other nodes ("hubs") may introduce an element of hierarchy into the otherwise flat network structure. What distinguishes networks from hierarchies is the capacity of lower-level units to have relationships with multiple higher-level centers as well as lateral links with units at the same organizational level.[18] Networks are never managed by a single (central) authority.

Second, unlike hierarchies, which can rely on authoritative rules and legal arbitration to govern relations, networks are self-enforcing governance structures disciplined primarily by reputation and expectations of reciprocity. As a result, networks tend to require higher levels of trust than other organizational forms.[19]

Third, unlike the impersonal, rule-guided relations that characterize interactions in hierarchies, networks tend to be based on direct personal contacts. As a result, they are often composed of members with similar professional backgrounds, interests, goals, and values. Relations and connections within networks tend to be informal and loosely structured. Finally, the lack of central authority and rule-guided interaction implies that decisionmaking and coordination in networks tend to be based on consensus and mutual adjustment rather than administrative fiat. (For a summary of differences between hierarchies and networks, see table 1.)

Beyond these core characteristics, networks differ in structure, size, and goals. Some networks are "open" insofar as they place no restrictions on membership; others are confined to small numbers of like-minded individuals. Some networks are dense, with a large number of connections between individual cells; others are more sparsely linked. Structurally, networks can be di-

17. Renate Mayntz, "Organizational Forms of Terrorism: Hierarchy, Network, or a Type Sui Generis?" MPIfG Discussion Paper, No. 04/4 (Cologne, Germany: Max-Planck-Institut für Gesellschaftsforschung, 2004); and Thompson, *Between Hierarchies and Markets,* pp. 22–24.
18. On hierarchy in networks, see Chris Ansell, "The Networked Polity: Regional Development in Western Europe," *Governance,* Vol. 13, No. 3 (July 2000), pp. 303–333, at p. 306; Albert Lászió Barabási, *Linked: The New Science of Networks: How Everything Is Connected to Everything Else and What It Means for Science, Business, and Everyday Life* (Cambridge, Mass.: Perseus, 2002); and Ranjay Gulati, Diana A. Dialdin, and Lihua Wang, "Organizational Networks," in Joel A.C. Baum, ed., *The Blackwell Companion to Organizations* (Oxford: Blackwell, 2002), pp. 281–303, at p. 289.
19. Powell, "Neither Market nor Hierarchy," pp. 301–304; Thompson, *Between Hierarchies and Markets,* p. 43; and Podolny and Page, "Network Forms of Organization," pp. 60–65.

Table 1. Characteristics of Networks and Hierarchies

	Networks	Hierarchies
Structure	Decentralized/horizontal	Centralized/vertical
Membership	Homogeneous	Diverse, professional
Unit relations	Trust-based, informal	Rule-based, formal
Decision mode	(Qualified) majority voting or top-down command	Consensus

vided into three types: the chain network where people, goods, or information move along a line of separated contacts and where end-to-end communication must travel through intermediate nodes; the "hub-and-spoke" (or "wheel network") where actors are tied to a central (but not hierarchical) node, and must go through that node to communicate with each other; and the all-channel network where everybody is connected to everybody else.[20] Terrorist and criminal networks tend to take the form of either chain or wheel networks, whereas all-channel networks are commonly associated with the internet world or some social movements.

ADVANTAGES OF NETWORKS

Much effort has gone into illuminating the benefits of networked cooperation. But the potential drawbacks have received far less attention. This section reviews some of the most common organizational advantages claimed for networks vis-à-vis hierarchical state authorities in the existing literature.

EFFICIENT COMMUNICATION AND INFORMATION PROCESSING. A key advantage claimed for the network is efficiency of communication and information processing. In traditional hierarchies, such as state bureaucracies, information typically passes through a centralized processing unit, increasing the risk of congestion and delay. It may be difficult to transmit information on the local characteristics of problems and potential solutions to central decisionmakers. By contrast, the decentralized yet tightly interconnected nature of networks means communication can flow unhindered from one part of the network to another, enabling actors to acquire, process, and act on local information faster than in centralized organizations.[21]

20. Arquilla and Ronfeld, *Networks and Netwars,* pp. 7–8.
21. Scharpf, "Coordination in Hierarchies and Networks," p. 135; Powell, "Neither Market nor Hierarchy," p. 325; and Wayne E. Baker and Robert R. Faulkner, "The Social Organization of Conspir-

Information not only flows more freely in networks; it is also thought to be of higher quality. According to Powell, "The most useful information is rarely that which flows down the formal chain of command. . . , rather, it is that which is obtained from someone whom you have dealt with in the past and found to be reliable."[22] Because cooperation is based on trust and reciprocity rather than on impersonal transactions, networks encourage people to share and collectively interpret information rather than merely pass it on, thereby creating new interpretations and connections.[23] As a result, networks are often thought to be more innovative than hierarchies.

SCALABILITY. A second advantage of networks is "scalability," that is, the ability to grow by adding sideways links to new individuals or groups. In principle, a loose organizational structure allows networks to expand freely, integrating new nodes as necessary. If new requirements or problems arise, networks can adapt by adding new links to groups with relevant expertise.[24] A networked structure also facilitates recruitment. Due to their dispersed, transnational structure, networks can tap into wider sets of resources such as diaspora populations, and local autonomy allows networks to tailor their message and activities to different communities, thereby increasing their support base.[25] Scalability is also enhanced by advances in information and communication technologies. As information flows and transfers of funds become quicker, cheaper, and more secure, the construction of complicated networked organizations over long distances becomes more feasible. A large literature documents how transnational, networked actors use the internet to raise funds, coordinate activities, and recruit new members.[26] The upshot, according

---

acy: Illegal Networks in the Heavy Electrical Equipment Industry," *American Sociological Review,* Vol. 58, No. 6 (December 1993), pp. 837–860, at p. 844.

22. Powell, "Neither Market nor Hierarchy," p. 304; and Keck and Sikkink, *Activists beyond Borders,* pp. 18–22.

23. Podolny and Page, "Network Forms of Organization," p. 62.

24. Smith-Doerr and Powell, "Networks and Economic Life," p. 384; Mayntz, "Organizational Forms of Terrorism," p. 12; and Podolny and Page, "Network Forms of Organization," p. 66.

25. Bert Klandermans, Hanspeter Kriese, and Sidney Tarrow, eds., *From Structure to Action: Comparing Social Movement Research across Cultures* (Greenwich, Conn.: JAI Press, 1988); and David A. Snow, E. Burke Rochford Jr., Steven K. Worden, and Robert D. Benford, "Frame Alignment Processes, Micromobilization, and Movement Participation," *American Sociological Review,* Vol. 51, No. 4 (August 1986), pp. 464–481.

26. See, for example, Michele Zanini and Sean J.A. Edwards, "The Networking of Terror in the Information Age," in Arquilla and Ronfeldt, *Networks and Netwars,* pp. 29–60; Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in Arquilla and Ronfeldt, *Networks and Netwars,* pp. 239–288; and Gabriel Weimann, "www.terror.net: How Modern Terrorism Uses the Internet," Special Report, No. 116 (Washington, D.C.: United States Institute of Peace Press, March 2004).

to the existing literature, is that networks can expand their scope and boost their ranks with great speed and at low cost.

ADAPTABILITY. A third advantage claimed for networks is adaptability to environmental changes. Compared to hierarchies, network boundaries are more easily redefinable and can adjust more rapidly to situational exigencies. As discussed, networks can "scale" to meet new requirements or needs. Similarly, loose coupling of nodes prevents locking in of ineffective relationships. If a particular organizational link is not providing the expected payoffs, it can be terminated at relatively low cost and replaced with alternative links.[27] A relative lack of physical infrastructure also enables networks to relocate operations from one geographic area to another in response to changing constraints. This provides a clear benefit for illicit groups that can migrate quickly from areas where the risks from law enforcement are high. For example, Michael Kenney describes how Colombian drug networks respond to police crackdowns by routinely moving their drug plantings and processing labs and creating fresh transportation routes, thereby escaping capture.[28]

RESILIENCE. Research on networks emphasizes their robustness and resistance to infiltration and fragmentation. The personal nature of network relationships—often based on ties of kinship, loyalty, and trust—means that networks are more resistant than more impersonal organizational forms to temptations of voice and exit.[29] Structural characteristics such as "loose coupling" and "redundant design" also reduce systemwide vulnerability. Loose coupling (i.e., minimal interaction and dependency among nodes) means that state authorities cannot use a compromised unit to roll up an entire network, as they might with a vertically integrated adversary.[30] Redundancy (i.e., the existence of a large number of structurally equivalent nodes) means that, unlike a hierarchical organization that can be disconnected or debilitated if a top node fails, a large number of nodes can be removed without causing a network to fragment. If one node fails, bypass links can be established around it, allowing business to continue as usual.[31] Such resilience is particularly useful to criminal actors that must evade detection and capture. The literature on drug trafficking documents how, to protect themselves from police, trafficking en-

27. Thompson, *Between Hierarchies and Markets*, p. 144.
28. Kenney, *From Pablo to Osama*.
29. Thompson, *Between Hierarchies and Markets*, p. 43.
30. Mayntz, "Organizational Forms of Terrorism," p. 14.
31. Duncan J. Watts, *Six Degrees: The Science of a Connected Age* (London: William Heinemann, 2003), pp. 285–286.

terprises often compartmentalize their participants into separate groups and limit communication among them.[32] Also, many criminal networks allegedly build redundancy into their active groups and leadership to prevent law enforcers from immobilizing the entire network by dismantling a single node.[33]

LEARNING CAPACITY. The existing literature highlights the advantages of networks over hierarchies when it comes to facilitating learning and innovation.[34] By promoting rapid transfers of information, it is said, networks allow participants to learn quickly about new events, opportunities, and threats. Networks also encourage learning through experimentation. In hierarchies, top-down command and heavy initial investments in dedicated machinery and routine tend to lock people into particular ways of working and discourage experimentation.[35] By contrast, a flat decisionmaking structure allows ideas and methods to be tested more readily, without having to wait for approval from above, thereby allowing wider sets of lessons to be learned.

Critical Questions and Historical Evidence

In current international relations literature, the advantages claimed for networks vis-à-vis hierarchies are typically assumed to apply to all networked actors, whether they are transnational advocacy groups, human rights coalitions, or criminal syndicates.[36] Terrorists and criminals—due to their constantly changing environments and their dependence on covertness—are believed to profit exceptionally from the network form. The 9/11 commission describes terrorist networks as agile, fast moving, and elusive, difficult for hierarchical states to combat.[37] Others depict such networks as "nimble, flexible, and adap-

32. Kenney, *From Pablo to Osama.*
33. Gerben Bruinsma and Wim Bernasco, "Criminal Groups and Transnational Illegal Markets: A More Detailed Examination of the Basis of Social Network Theory," *Crime, Law, and Social Change,* Vol. 41 (2004), pp. 79–84; Kenney, *From Pablo to Osama;* and Russell D. Howard and Reid L. Sawyer, eds., *Terrorism and Counterterrorism: Understanding the New Security Environment* (Guilford, Conn.: McGraw-Hill, 2004).
34. See, for example, Keck and Sikkink, *Activists beyond Borders;* Kenney, *From Pablo to Osama;* Powell, "Neither Market nor Hierarchy"; and Podolny and Page, "Network Forms of Organization," p. 63.
35. See, for example, Bonnie H. Erikson, "Secret Societies and Social Structure," *Social Forces,* Vol. 60, No. 1 (September 1981), pp. 188–210; and Kenney, *From Pablo to Osama,* p. 7.
36. See, for example, Arquilla and Ronfeldt, *Networks and Netwars;* and Keck and Sikkink, *Activists beyond Borders.*
37. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (New York: W.W. Norton, 2004), pp. 87, 399.

tive,"[38] as "liable to change . . . structure according to circumstances,"[39] and as "large, fluid, mobile, and incredibly resilient."[40] These somber assessments appear to be partly vindicated by the recent experiences of leading states in their confrontation with network-based adversaries. Iraq's fractured, unrelenting insurgency, the distressing evolution of media-savvy al-Qaida, and the apparently futile war against Colombian drug lords all suggest a world in which illicit networks are both formidable and adaptive.

Most clandestine networks, however, are not as agile and resilient as they are made out to be. In this section we seek to show why many illicit networks may be prone to inefficiencies and short life cycles. Our analysis expands the existing literature in two main ways. First, although a great deal of scholarly effort has sought to uncover and explain the advantages of networks, potential weaknesses and constraints have received far less attention. As Miles Kahler notes, successful networks are relatively easy to spot; failed ones much less so. Failures are seldom revealed or evaluated, either with regard to the formation of networks or their ability to achieve their stated goals. As a result, researchers may be overestimating the capacity of networks for collective action, and indeed the overall strength of the network form.[41] Also problematic is that researchers rarely evaluate networks explicitly against their organizational alternatives.[42] How do networks in international relations compare to other forms of governance? Are they, for example, superior or poorer at coping with change, stress, or failure?

A second limitation of the current literature is the insistence on treating contemporary networked threats as "new"—witness the emphasis on so-called new terrorism. The notion that contemporary criminal actors are fundamen-

---

38. Bruce Hoffman, "Al Qaeda, Trends in Terrorism, and Future Potentialities: An Assessment" (Santa Monica, Calif.: RAND, 2003), p. 12.
39. Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror* (New York: Columbia University Press, 2002), p. 79.
40. Peter Clarke, cited in *Economist*, "Waiting for al-Qaeda's Next Bomb," May 3, 2007.
41. Miles Kahler, "Collective Action and Clandestine Networks: The Case of Al-Qaeda," in Kahler, ed., *Networked Politics: Agency, Power, and Governance* (Ithaca, N.Y.: Cornell University Press, forthcoming).
42. See Smith-Doerr and Powell, "Networks and Economic Life." Sociologists in the social movement tradition have explored the comparative utility of a centralized bureaucratic model versus a decentralized, informal approach, but international relations scholars do not typically draw from this work. See, for example, John D. McCarthy and Mayer N. Zald, "Resource Mobilization and Social Movements: A Partial Theory," *American Journal of Sociology*, Vol. 82, No. 6 (May 1977), pp. 1212–1241.

tally different from those in the past makes comparative data difficult to find because it suggests history is obsolete.[43] Yet extant studies of terrorism, insurgency, and organized crime are far from obsolete when it comes to understanding today's networked threats. Opposition to the state has often taken a networked approach, as illustrated by the decentralized Greek resistance to the Ottomans in the early nineteenth century, the Muslim Brotherhood's loosely organized, dispersed resistance to the Egyptian state, and the sprawling international anarchist movement in the late nineteenth century. In the Middle East, informal, loosely structured networks of religion and political activism, sustained as much by personal ties as abstract ideas and common purpose, have a long history.[44] Existing research on these and similar entities provides a wealth of data about the strengths and weaknesses of networks.

Below we draw from these data to illuminate potential weaknesses of the network form. The analysis is guided by (and limited to) the question of what the distinct structural characteristics of networks—that is, limited central control, local autonomy, and informal, flexible interaction based on direct, personal relations—imply for the effectiveness and life cycle of an illicit actor. We do not address potential advantages or disadvantages stemming from other factors, such as the psychological profile or belief systems of criminal actors. Each subsection highlights an area of potential weakness of a networked structure and gives both theoretical and empirical reasons to support the claim, using highly prominent examples of networked cooperation in the history of terrorism, insurgency, and organized crime.[45] As such, they should be the most likely to confirm the advantages of network theory. Although we focus spe-

---

43. According to Ian O. Lesser, "The new tendency to organize in networks renders much previous analysis of terrorism based on established groups obsolete." See Lesser, "Introduction," in Lesser, Bruce Hoffman, John Arquilla, David Ronfeldt, and Michele Zanini, *Countering the New Terrorism* (Santa Monica, Calif.: RAND, 1999), pp. 1–6, at p. 2.

44. See Guilain P. Denoeux, *Urban Unrest in the Middle East: A Comparative Study of Informal Networks in Egypt, Iran, and Lebanon* (Albany: State University of New York Press, 1993).

45. The cases from which we draw are not chosen randomly to be broadly representative of the universe of illicit networks. Rather we have focused on prominent networks, which, due to the relative success of their activities, have captured significant media and scholarly attention. These cases should be most likely to confirm the theoretical advantages of a networked structure and thus represent hard cases from our viewpoint. We realize there are key differences in the operational procedures and constraints facing drug smugglers, terrorists, and revolutionaries. Still, we find, along with others (e.g., Matthew Brzezinski, "Re-engineering the Drug Business," *New York Times Magazine,* June 23, 2002, p. 48; and Kenney, *From Pablo to Osama*), that there are important structural commonalities in the way these types of groups organize, which justify a comparative analysis.

cifically on illicit actors, we suggest these weaknesses may apply to networks more generally.

Information Limitations and Communication Failure

The existing literature portrays networks as highly efficient information providers. Yet, networks may not always be superior organizational structures for gathering, sharing, and processing information. First, decentralization implies that searching for information in networks may be difficult and cumbersome. In principle, a central directory renders the problem of finding information trivial, even in a large, dispersed network. But central directories are expensive to establish and maintain, and may be impracticable in illicit networks due to security concerns.[46] Decentralized or "distributed" systems, on the other hand, tend to be less efficient information providers.[47] Because such systems lack a central directory to catalogue information, searches effectively involve each node querying neighboring nodes, which query other neighboring nodes until the information is found (or the search is abandoned). As a result, each unit of information tends to be associated with higher transaction costs than in a centralized system.

Compartmentalization of nodes, necessary for security reasons, may also present a barrier to effective information sharing in illicit networks. As discussed, criminal and terrorist networks often seek to minimize potentially destabilizing contacts between cells. To shield them from complicity, members are kept minimally informed about the activities of others, thereby making communication difficult. Dark networks may also find it hard to source reliable information from outsiders. According to the literature, a key advantage of the network is its structural access to wider, more diverse sources of information. Yet, sociological research on underground participation shows that illicit actors are often isolated from wider social communities.[48] Loyalty tends to

---

46. Secrecy makes information sharing difficult for any type of organization, including hierarchical ones such as, for example, the Central Intelligence Agency, but a decentralized networked structure compounds these difficulties due to the absence of reliable means for authenticating information and for controlling who gains access to sensitive data.

47. Duncan Watts gives the example of a purely distributed peer-to-peer internet network called Gnutella. Because it lacks, by design, a central directory, searches in a purely decentralized system such as Gnutella are often far less efficient than a Napster-like network, where queries go to a central high-capacity server. See Watts, *Six Degrees,* pp. 157–158.

48. Martha Crenshaw, "Decisions to Use Terrorism: Psychological Constraints on Instrumental Reasoning," in Donatella Della Porta, ed., *Social Movements and Violence: Participation in Underground Organizations* (Greenwich, Conn.: JAI Press, 1992), pp. 29–42; Donatella Della Porta, "On In-

run deeper when members are cut off from countervailing influences. Hence, terrorist and insurgent leaders often limit contact with the outside world, thereby restricting the in-flow of information to the network.

History provides numerous examples of networks that fail in their missions due to inefficient communication and information sharing or because isolation and secrecy undermine their ability to identify and react to critical changes in their environment. Problems of information sharing are implicated in the demise of the Quebec Liberation Front (known by the French acronym FLQ).[49] Although it portrayed itself, and was portrayed in the media, as a centralized, monolithic organization, the FLQ was a loosely organized network of militants, clustered around various charismatic personalities. No central leadership controlled FLQ "cells"—these were groups of friends and family sharing the ideal of an independent Quebec. Ronald Crelinsten's account of the 1970 October crisis emphasizes obstacles to effective communication and information sharing as a result of this decentralization. The crisis erupted when two friendly but physically separated cells failed to communicate their strategies to each other. The Liberation cell decided to kidnap a British diplomat. The Chenier cell, apparently not well informed about the strategy, carried out a separate kidnapping of Pierre Laporte, the Quebec labor minister. When the Liberation cell—taken by surprise by the Laporte kidnapping—announced publicly the FLQ would release both hostages if two of its demands were met, the Chenier cell insisted separately that all demands must be met or Laporte would be killed. Failures of communication and coordination deepened as the network was driven farther underground, until in late 1970 Laporte was killed and popular support for the network lost. What is striking about this example is that the FLQ cells were not initially feuding. Rather, as Crelinsten suggests, the loose network structure and lack of central authority made reliable communication and information sharing difficult, with the result that cooperation broke down. One might object that similar communication failures are less likely in the electronic age, where the internet, cell phones, and videoconferencing enable real-time communication across distances. But as we explain

dividual Motivations in Underground Political Organizations," in Della Porta, ed., *Social Movements and Violence*, pp. 3–28; and Donatella Della Porta, "Left-wing Terrorism in Italy," in Martha Crenshaw, ed., *Terrorism in Context* (University Park: Penn State University Press, 1995), pp. 105–159.

49. Ronald D. Crelinsten, "The Internal Dynamics of the FLQ during the October Crisis of 1970," in David C. Rapoport, ed., *Inside Terrorist Organizations* (New York: Columbia University Press, 1988), pp. 59–89.

below, modern information technologies do not solve all the problems of communication between geographically dispersed actors lacking central command, and police monitoring of phones and internet sites often makes reliance on such technologies perilous.

poor decisionmaking and excessive risk-taking

A second problem in networks involves strategic decisionmaking. In the theoretical literature, networks assume an almost organic ability to respond flexibly to the environment, weighing the options and adjusting their composition and operating procedures as needs change. Yet, real-world networks are not likely to be so smart. First, decisionmaking is unlikely to be as fast or as coherent as the literature suggests. In a network, as in a hierarchy, complex decisions have to be made regarding resource allocation, tactics, whether and when to use violence, what social and political levers to manipulate, and so on. Because these decisions will not flow from centralized leadership, decisionmaking is likely to be a complicated, protracted process as all members try to have a say—or go their own way.[50] Decisions also may not be respected as readily due to the lack of an authoritative stamp. As a result, resources may be used poorly, contradictory tactics selected, and activities carried out that serve parochial short-term interests rather than the larger mission.

Second, strategy may be virtually nonexistent, or at least rudimentary, without experienced central leadership. Local autonomy means operations can go forward without evaluation, coordination, and a sober assessment of the overall benefits and risks. Likewise, the absence of central direction implies that important tasks may be left unassigned or efforts duplicated, causing operational costs to spiral. Strategic processes may be further undermined by self-censorship. Although the literature highlights deliberation and free exchange of ideas as key advantages of networks, in reality, the norms of collective decisionmaking within cells and strong group loyalty—combined with fear of negative sanctions, even purging, if one does not go along with the majority—often lead members to keep off the agenda issues that are threatening to consensus building.[51] Free exchange of ideas is therefore not likely to be the norm in illicit networks, and deliberation and rational decisionmaking may suffer as a result.

---

50. Powell, "Neither Market nor Hierarchy," p. 318.
51. Gordon H. McCormick, "Terrorist Decision Making," *Annual Review of Political Science,* Vol. 6 (June 2003), p. 498.

Illicit networks are also prone to excessive risk taking. Sociologists find that decision processes within highly insulated underground organizations are prone to "groupthink," and various forms of delusion, including a sense of invulnerability, which encourage extreme risk taking.[52] Risk taking may also be induced by the pressure to reciprocate. Networks, like other organizations, thrive on results: terrorists must engage in violent attacks to maintain visibility; drug smugglers need to shift their goods lest they lose supplies and clients. Pressure to reciprocate, combined with the high reputation costs associated with failure, can induce recklessness, forcing members to choose a course of action before they are ready. Research on a Montreal criminal network reveals how a networked structure may induce risk taking.[53] This network was subjected to intense police surveillance and disruption over a two-year period. Shipments were routinely seized, but the network itself was allowed to survive so law enforcement could gather enough intelligence to bring it down fully. The effects of stress on the network are revealing. When seizures took place, traffickers tended to blame each other and worry about their own reputations instead of trying to learn how to avoid future seizures.[54] According to conversation logs, those involved with failed shipments grew increasingly reckless in their attempts to compensate for losses and get back into the network's good graces. Rather than seek to interpret their failures and revise their strategy, participants seem to have been so frazzled by their failures and dread of what might happen to them as a result that they were moved to irrational behavior. Although the threat of punishment might have the same effect in a hierarchical structure, it is likely that more formal patterns of cooperation, which give members a sense that their place in an organization is relatively stable and secure, rather than based precariously on informal reciprocity, might prevent similar recklessness.

Restrictions on scope and structural adaptability

As we have shown, networks are often depicted as highly elastic entities that combine, recombine, and expand to adapt to transformations in their environment. Yet, both common sense and empirical evidence suggest there are limits

52. A wide literature in sociology finds that decisionmaking by consensus induces risk-taking behavior, particularly in underground organizations. See, for example, Michael A. Wallach and Nathan Kogan, "The Roles of Information, Discussion, and Consensus in Group Risk Taking," *Journal of Experimental Social Psychology,* Vol. 1, No. 1 (1965), pp. 1–19, at p. 1. For an overview of this literature, see McCormick, "Terrorist Decision Making."
53. Carlo Morselli and Katia Petit, "Law-Enforcement Disruption of a Drug Importation Network," *Global Crime,* Vol. 8, No. 2 (May 2007), pp. 109–130.
54. Ibid.

to the scalability and structural adaptability of most networks. There are several reasons why networks, and illicit networks in particular, may find it difficult to scale. As discussed, because illicit networks cannot depend on hierarchy or the legal system to resolve disputes, they are crucially dependent on interpersonal trust. The high premium on trust both limits the feasible size of networks and restricts recruitment. It is well known, for example, that it is easier to generate trust and generalize expectations of reciprocity in small collectivities when the "social distance" between actors is short, and chains of action are not extended.[55] This favors small networks. It is also easier to generate trust when actors are homogeneous in outlook, life style, and culture. As a result, recruitment to illicit networks mostly proceeds through preexisting networks of personal relationships, typically ones that rest on kinship or previous bonding experiences.[56] For example, contemporary drug trafficking largely occurs within ethnically homogeneous groups, where kinship generates trust and reciprocity among criminals reluctant to transact with people they have not known for long periods.[57] Gerben Bruinsma and Wim Bernasco's analysis of Turkish heroin trafficking suggests the entire trade chains from production in Turkey to sale in Europe are based on close family relationships.[58] In Donatella Della Porta's sample of Italian Red Brigades, 70 percent of recruits had at least one friend involved already,[59] and in Marc Sageman's sample of mujahideen, at least 75 percent had preexisting bonds of family or friendship.[60] These recruitment practices restrict the scope of illicit networks, casting doubt on rapid expansion.

---

55. Thompson, *Between Hierarchies and Markets,* p. 45.
56. Raab and Milward, "Dark Networks as Problems"; Erikson, "Secret Societies and Social Structure," p. 195; and Klandermans, Kriese, and Tarrow, *From Structure to Action.* The constraint set by preexisting social networks on recruitment varies across criminal activities. For lower-risk activities, such as trade in stolen cars or some drug-trafficking activities, significant migration movements have stimulated the growth of extensive cross-border networks held together by shared ethnicity. See, for example, John McFarlane, "Transnational Crime as a Security Issue," in Carolina G. Hernadez and Gina R. Pattugalan, eds., *Transnational Crime and Regional Security in the Asia Pacific* (Manila: Institute for Strategic and Development Studies, 1999), p. 53. But, in general, the more dangerous and risky the activity, the more networks rely on strong personal ties. Thus, Martha Crenshaw finds that marijuana users are willing to share information or drugs with a wider range of people than the more endangered and hence more cautious users of heroin. See Crenshaw, "An Organizational Approach to the Analysis of Political Terrorism," *Orbis,* Vol. 39, No. 2 (Fall 1985), pp. 465–489. On this logic, terrorists are likely to be among the most cautious in whom they trust.
57. Brzezinski, "Re-engineering the Drug Business"; Kenney, *From Pablo to Osama,* p. 28; and Raab and Milward, "Dark Networks as Problems," p. 8.
58. Bruinsma and Bernasco, "Criminal Groups and Transnational Illegal Markets," p. 87.
59. Della Porta, "Left-wing Terrorism in Italy," p. 139.
60. Sageman, *Understanding Terror Networks,* pp. 111–113. Justin Magouirk, Scott Atran, and Marc

Networks grow not only by recruiting new members but also by linking sideways to other networked groups. Evidence suggests, however, that networks that seek to scale in this way often end up splintering as a result of differences of ideologies, goals, and strategies. The splintering of the network of Egyptian militants who assassinated President Anwar al-Sadat highlights the tendency toward fragmentation when networks attempt to grow by linking to other, like-minded groups.[61] The network of Islamic militants that assassinated Sadat in October 1981 was a loose coalition of autonomous groups that had decided the previous year to coordinate their activities. Although they shared the goal of establishing an Islamic state, these various groups held different views on how to achieve that goal, some favoring a violent coup and others focusing on a broad popular uprising. When presented with the opportunity to strike Sadat, local leaders disagreed widely on the desirability of such a strategy. This lack of unity, in turn, led to poor planning and preparation. To avoid dissent and possible leakage, many local leaders were informed of the plot very late—in some cases only hours before it unfolded. As a result, they were caught by surprise and ill prepared for the wave of arrests that followed. The insurrection that followed the assassination was crushed in a matter of days, and more than 300 members of the network were arrested and put on trial. Once the network was hit, it quickly fragmented, as it broke into rival groups.

The Egyptian militants are far from a unique example. There are numerous instances of networks that fracture when they attempt to scale. The original Palestinian Liberation Front (PLF), which was founded by Ahmad Jibril in 1959, merged with other nationalist militant groups in 1967 to form the Popular Front for the Liberation of Palestine (PFLP). In 1977 the PLF splintered from the PFLP due to internal conflict, and in 1983 and 1985 the organization split again into pro-Palestine Liberation Organization (PLO), pro-Syrian, and pro-Libyan factions, each of which claimed to represent the mother-organization.[62] The much-publicized split within the ranks of Jemaah Islamiyah (JI) in 1999–2000 occurred after new links between senior JI operatives and al-Qaida took the organization in a more militant direction, causing rifts among its leader-

---

Sageman document the prevalence of kin relationships within Jemaah Islamiyah in "Connecting Terrorist Networks," *Studies in Conflict and Terrorism,* Vol. 31, No. 1 (January 2008), pp. 1–16.

61. See Sageman, *Understanding Terror Networks,* pp. 30–33. For a more detailed account, see David Sagiv, *Fundamentalism and Intellectuals in Egypt, 1973–1993* (New York: Routledge, 1995), pp. 54–61; and Steven Brooke, "Jihadist Strategic Debates before 9/11," *Studies in Conflict and Terrorism,* Vol. 31, No. 3 (June 2008), pp. 201–226.

62. "In the Spotlight: The Palestinian Liberation Front (PLF)," Center for Defense Information, updated November 14, 2002, http://www.cdi.org/terrorism/plf.cfm.

ship.[63] Aum Shinrikyo, the cult known for the deadly sarin gas attack in Tokyo in 1995, experienced rapid growth in the late 1990s counting as many as 40,000 members around the world. However, unity suffered as a result. Around 2000, a leadership contest broke out between the founder, Shoko Asahara, and challenger Fumihiro Joyu, who sought to distance himself from the violent teachings of Asahara, and in 2007 the organization split in two. Today the cult's membership stands at about 1,500.[64]

That some networks disintegrate when seeking to expand does not suggest that all networks find it difficult to scale. Research suggests, however, that networks that grow too large often find it difficult to sustain unity of purpose, and that their effectiveness declines as a result. The main reason is the difficulty in coordinating behavior and nourishing agreement among large, diverse groups lacking central leadership. The Basque nationalist group ETA and the PLO both provide examples of networks that have struggled to sustain unity as they grew. The demise of the international anarchist movement also highlights the difficulty of sustaining community and commitment in dispersed networked structures. By the early twentieth century, scattered in Europe and the United States, the anarchists were exposed to a variety of countervailing influences, drawing them away from their commitment to transnational anarchism.[65] Historically, many nonstate organizations that have expanded abroad have found their base of popular support weakened as a result.[66] A networked structure that thrives on local empowerment often struggles to project a unified image of itself to the world. With various centers of power claiming to speak for the network, its legitimacy and very identity can easily be called into question. The decentralized Algerian insurgency in the early 1990s is a striking example.[67] The Islamic Salvation Front (known by the French acronym FIS), the Islamist party banned by the Algerian regime after it won parliamentary elections in 1991, had exiled leaders in both the United

63. See Magouirk, Atran, and Sageman, "Connecting Terrorist Networks"; and Elena Pavlova, "From a Counter-Society to a Counter-State Movement: Jemaah Islamiyah According to PUPJI," *Studies in Conflict and Terrorism,* Vol. 30, No. 9 (September 2007), pp. 777–800.
64. Holly Fletcher, "Aum Shinrikyo (Japan, Cultists, Aum Supreme Truth)," Council on Foreign Relations, Backgrounder, updated May 18, 2008, http://www.cfr.org/publication/9238/.
65. Martin A. Miller, "The Intellectual Origins of Modern Terrorism in Europe," in Crenshaw, *Terrorism in Context,* pp. 27–62.
66. See David C. Rapoport, "The International World as Some Terrorists Have Seen It: A Look at a Century of Memoirs," in Rapoport, *Inside Terrorist Organizations,* pp. 32–58.
67. Martin Stone, *The Agony of Algeria* (New York: Columbia University Press, 1997); and Michael Willis, *The Islamist Challenge in Algeria: A Political History* (Washington Square: New York University Press, 1997).

States and Germany. Concerned with building international support, these leaders were eager not to espouse violence for fear it would endanger the status of the FIS as a legitimate political party. But the FIS also had leaders in Algeria who refused to reject violence. Conflicting communiqués often emerged from various centers of power, and, as a result, it was unclear who represented the FIS and broader Islamist insurgency. No one had firm control over all the armed groups, and the violence of some ended up tainting the broader political movement, undermining popular support.[68] A similar schism appears to affect Gama'a al-Islamiyya (Islamic Group, or IG) today. IG, an international terrorist network seeking to create an Islamic state in Egypt and implicated in the 1993 World Trade Center bombing, split into violent and nonviolent factions after announcing a cease-fire in 1997. Since then, the network has continued to grow more divided as exiled leaders abroad have advocated the use of mass violence while members of the group's leadership in Egypt reject it.[69]

Not only scalability but also structural adaptability is likely to be limited in many networks. Indeed, networks ties may be "stickier" than the image of "loose coupling" suggests; contrary to conventional network wisdom, networks could be more resistant to change than bureaucratic ties. To be sure, a lack of physical infrastructure and an absence of bureaucracy ensure some flexibility. But consider that much of the flexibility claimed for networks stems from loosely coupled or "weak links," which can be easily redrawn and remodeled. In economics weak ties are seen as a boon because they give rise to more diverse sources of information, fresh perspectives on problems, and new collaboration opportunities. Most clandestine networks, however, are built on strong ties based on kinship and previous bonding experience. Adding or severing links may be difficult, and physical movement and relocation not so easy, when personal relationships are involved. Because networked cooperation builds on expectations of reciprocity, strong reputation constraints on breaking network ties may also limit flexibility.[70] Consequently, not only the ability of networks to grow but also their ability to adapt through restructuring themselves may be far more modest than the literature recognizes.

68. Willis, *The Islamist Challenge in Algeria,* p. 315.
69. U.S. Department of State, Office of the Coordinator for Counterterrorism, "Chapter 6: Terrorist Organizations," in *Country Reports on Terrorism,* April 30, 2008, http://www.state.gov/s/ct/rls/crt/2007/103714.htm.
70. Podolny and Page, "Networks Forms of Organization," pp. 61–62.

COLLECTIVE-ACTION PROBLEMS DUE TO COORDINATION

As suggested, networks face a variety of collective-action problems. A frequent source of collective-action failure is internal conflict. In-fighting commonly afflicts clandestine groups, whether modeled hierarchically or not,[71] but networks, with their lack of centralized control, are especially susceptible to internal strife. Local autonomy, though advantageous in some respects, easily nourishes the growth of competing centers of power with independent bases of legitimacy, loyalty, and material support. Challengers are more willing to assert themselves if central leadership is weak. In networks, moreover, rules and regulations about the use of tactics, allocation of resources, and so on are not formally established. As a result, competing centers of power may fight over such issues more readily, and without the aid of formal arbitration.

The PLO vividly illustrates how tensions can go unresolved in informal networks, regardless of close social linkages. This loose federation of nationalist groups historically suffered from acute infighting, as autonomous segments vied for control. Sponsor states such as Egypt, Syria, and the conservative Gulf monarchies deepened internal strife by funding rival groups, but they were only partly to blame for Palestinian fractiousness.[72] As David Schiller suggests, structural features typical of networks—the absence of central authority, the unchecked autonomy of rival groups, and the inability to arbitrate quarrels through formal mechanisms—made the PLO excessively vulnerable to outside manipulation and internal strife. ETA, which began as a diffuse, heterogeneous movement with limited central control, provides another example of network fractiousness.[73] In the 1960s, aiming for a broad-based insurgency against President Francisco Franco, it was open to people of widely different political and social backgrounds, some supporting Basque independence, others unification with the French Basque territories, still others self-rule within

71. See McCormick, "Terrorist Decision Making."
72. David Schiller, "A Battlegroup Divided: The Palestinian Fedayeen," in Rapoport, *Inside Terrorist Organizations,* pp. 90–108.
73. For this example, see Cyrus Ernesto Zirakzadeh, "From Revolutionary Dreams to Organizational Fragmentation: Disputes over Violence within ETA and Sendero Luminoso," *Terrorism and Political Violence,* Vol. 14, No. 1 (Winter 2002), pp. 66–92. Not only terrorist groups but also other networked actors are prone to disunity. Research on U.S. street gangs suggests that loosely configured gangs, lacking clear roles, a corporate structure, and central control, cannot effectively control the behavior of their members. A study of warring gangs in St. Louis, Missouri, revealed that gang homicides were more likely to take place within gangs than between them, mainly because of their lack of central control and discipline. See Scott H. Decker and David Curry, "Gangs, Gang Homicides, and Gang Loyalty: Organized Crimes or Disorganized Criminals," *Journal of Criminal Justice,* Vol. 30, No. 4 (July–August 2002), pp. 343–352.

Spain. Differences over the acceptability of violent tactics triggered serious internal friction, and splinter groups multiplied over the generations, with little in common except the franchise label "ETA."

Although fractiousness is certainly not uncommon in terrorist groups, a networked structure appears to nourish it. The Shining Path in Peru, one of the most cohesive, enduring insurgent organizations in the twentieth century, provides a helpful contrast. Research on the group's high degree of social cohesion and effectiveness suggests it was closely tied to its hierarchical structure, centered on the powerful leadership of Abimael Guzmán.[74] Jemaah Islamiyah is another case in point. JI under the leadership of Abdullah Sungkar was a highly centralized organization with a top-down chain of command and clearly defined objectives. Sungkar ruled JI with an iron hand and did not allow any rival centers of power to arise within the organization. After Sungkar's death in 1999, JI split into fractious groups as a militant minority under the leadership of Hambali broke with the moderate majority and carried out a series of terrorist attacks in Southeast Asia from 2000 to 2005. The nominal leadership of Sungkar's second in command, Abu Bakar Ba'asyir, has been largely unsuccessful in stemming fractiousness within what is now a much more loosely structured network.[75]

Distance coordination poses another obstacle to collective action. The network literature tends to assume away problems of distance. The internet and other communications technologies are thought to enable seamless cooperation among geographically dispersed actors. Yet, research on computer-supported collaborative work finds that such technologies do not solve all the problems of distance cooperation, and may generate new difficulties.[76] People

74. Gordon H. McCormick, "The Shining Path and Peruvian Terrorism," in Rapoport, ed., *Inside Terrorist Organizations,* pp. 109–128. Zirakzadeh, too, comes to this conclusion in his explicit comparison of the ETA with the hierarchical Shining Path; hierarchy helped prevent fragmentation of the Peruvian group. Zirakzadeh, "From Revolutionary Dreams to Organizational Fragmentation."
75. See Magouirk, Atran, and Sageman, "Connecting Terrorist Networks"; and Pavlova, "From a Counter-Society to a Counter-State Movement."
76. On the problems of distance collaboration, especially conflict, misunderstanding, and trust, see Pamela J. Hinds and Diane E. Bailey, "Out of Sight, Out of Sync: Understanding Conflict in Distributed Teams," *Organization Science,* Vol. 14, No. 6 (November–December 2003), pp. 615–632; Gary M. Olson and Judith S. Olson, "Distance Matters," *Human-Computer Interaction,* Vol. 15, Nos. 2–3 (September 2000), pp. 139–178; Catherine Durnell Cramton, "The Mutual Knowledge Problem and Its Consequences for Dispersed Collaboration," *Organization Science,* Vol. 12, No. 3 (May–June 2001), pp. 346–371; Pamela J. Hinds and Mark Mortensen, "Understanding Conflict in Geographically Distributed Teams: The Moderating Effects of Shared Identity, Shared Context, and Spontaneous Communication," *Organization Science,* Vol. 16, No. 3 (May–June 2005), pp. 290–307; Sirkka L. Jarvenpaa and Dorothy E. Leidner, "Communication and Trust in Global Virtual Teams," *Organization Science,* Vol. 10, No. 6 (June 1999), pp. 791–815; and Patricia Wallace, *The Internet in the*

easily misinterpret and misunderstand one another when they must rely on voice transmissions, email, and instant messaging. Without face-to-face interaction, people often fail to identify and correct for misjudgments.[77] Consequently, conflicts are more likely to erupt in geographically dispersed teams, as opposed to colocated ones. This research also casts doubt on the ability of dispersed networks to establish and preserve social cohesion. Face-to-face interaction is crucial in building a social-support structure for communication. People separated by significant distances often lack the contextual information to make sense of behavior, and as a result tend to be less cohesive and trusting than their face-to-face counterparts. The absence of a headquarters, though considered an advantage for security, may also undercut social cohesion in networks. A central base where recruits live, train, or plan activities together can be essential for building the trust that sustains collective action. Loyalty and commitment may be less easy to instill in networks that are transnational, dispersed, and reliant on temporary, makeshift bases.

Germany's experience with terrorism in the 1970s highlights these difficulties. Research comparing left- and right-wing groups suggests the dispersed, networked structure of right-wing groups severely reduced their cohesion.[78] The far more unified and successful left-wing terrorists tended to organize hierarchically, with professional management and clear divisions of labor. They were concentrated geographically in universities, where they could establish central leadership, trust, and camaraderie through regular, face-to-face meetings. Under interrogation, they rarely betrayed their comrades. By contrast, the right-wing networks were decentralized, scattered about the country, and involvement was often temporary. They were routinely infiltrated and their members arrested; those captured frequently betrayed their associates.

SECURITY BREACHES

Research on illicit networks emphasizes their resistance to infiltration and dismantlement. Yet, despite practices of "loose coupling" and "redundant design," which make networks less vulnerable to leadership interdiction and

---

Workplace: How New Technology Is Transforming Work (Cambridge: Cambridge University Press, 2004).

77. Cooperation that relies on distance technologies is also hampered by the difficulty of sharing communication aids. For example, in face-to-face meetings, a map is easily shared and participants can use gestures to communicate movements or locations. This efficient "war room" style of coordination, easily arranged for colocated teams, is far more difficult for dispersed team members using communications technologies.

78. See Frieldhelm Neidhardt, "Left-wing and Right-wing Terrorism Groups: A Comparison for the German Case," in Della Porta, *Social Movements and Violence*, pp. 215–235.

random arrests, networks are not necessarily more secure than hierarchical organizations. In fact, once networks are hit, they may unravel spontaneously as participants begin to blame one another, as suggested by the demise of the Montreal drug-trafficking network or the Egyptian assassins.[79] More generally, the absence of central authority, while protecting networks by leaving no obvious locus for attack, can seriously jeopardize security. Dispersed authority makes it difficult to monitor activities and screen new recruits. Rules for safe conduct are not defined and enforced centrally but often evolve locally in an impromptu, precarious way, which may undermine security.

Security breaches are easily observed in the experiences of underground networks. According to research on the Italian underground in the 1970, those militant left-wing organizations that experimented with a decentralized approach were highly vulnerable.[80] They typically engaged local leaders *(squadre),* who were relatively autonomous in their activities. Although local autonomy boosted grassroots recruitment, it was also risky. Because of their operational freedom, *squadre* were able to recruit whole groups of supporters without having to wait for background checks and approval from above. Internal security was fragile, and infiltration by the state rampant. Many groups, in fact, evolved in the direction of greater centralization precisely because of the risks associated with a networked strategy. The Red Brigades, for instance, instilled more hierarchy in their organization and stricter controls over the process of recruitment.

Communication practices among international drug traffickers also highlight the security liabilities of a decentralized approach. Research suggests that, although unofficial guidelines among drug traffickers discourage the use of cell phones and encourage coded language, coordination among actors on the street is often so demanding that agents communicate in an excessively simple, transparent manner that risks security.[81] As a former trafficker explained: "International dope smugglers have to make thousands of phone calls. There are many who say they never use the phone because it's too insecure. They are either lying or not doing any business." Referring to the use of coded language, he continued: "Any attempt at sophisticated coding quickly leads to disastrous misunderstandings. I have never heard or made a dope-

79. Of course, not all networks unravel easily, as the debate about torture demonstrates. Resilience in the face of opposition, however, often has more to do with the extreme loyalty of a few individuals than with a networked structure per se.
80. Della Porta, "Left-wing Terrorism in Italy."
81. Morselli and Petit, "Law-Enforcement Disruption of a Drug Importation Network."

smuggling call which isn't obviously just that."[82] Such practices may explain why communications among drug traffickers, as well as terrorists, are habitually intercepted by security services.

LEARNING DISABILITIES

Learning is crucial for illicit actors. To stay afloat in a hostile environment, criminals must learn to identify and circumvent rapidly shifting countermeasures, avoid past mistakes, and recover from missteps. In the existing literature, networks are cast as highly efficient learners.[83] As with much of the logic on networked effectiveness, however, the theoretical learning advantages of networks fit a legal, economic context better than the world of illicit actors. One reason networks are said to be good learners is that they facilitate rapid information flows, which allow actors to find out about new opportunities and threats. As we have shown, however, information does not necessarily flow freely in networks, especially illicit ones. Loose coupling, combined with pressure to separate the network from its social base for security reasons, tends to reduce social embeddedness and network connectivity, thereby making information sharing difficult. And, as Michael Kenney shows with respect to drug-trafficking networks, compartmentalization means individual cells often absorb only those lessons they have learned directly rather than benefit from the experience of others.[84]

Another alleged learning advantage of the network—its superior ability to produce "on-the-job expertise"—is also doubtful. Because networks build on personal relationships, they are said to be better than hierarchies at transmitting "tacit knowledge"—that is, knowledge that cannot be explicitly codified but is associated with learning-by-doing and hands-on techniques.[85] Yet, bureaucrats learn on the job too, and personal, mentored relationships also exist in hierarchies. Much like their networked adversaries, agents in counterterrorism and drug law enforcement learn when they operate in the field, and much like their networked adversaries, they can leverage social networks of friends,

---

82. Quoted in ibid., p. 17, of copy available online from the Social Science Research Network, http://ssrn.com/abstract?944829.
83. See, for example, Powell, "Neither Market nor Hierarchy"; and Thompson, *Between Hierarchies and Markets.* On the learning abilities of illicit networks, see especially Kenney, *From Pablo to Osama.*
84. See Kenney, *From Pablo to Osama,* p. 115. Many network scholars recognize that compartmentalization and secrecy may present impediments to learning, but they still insist that networks are better learners than bureaucracies. See, for example, ibid., p. 7.
85. Thompson, *Between Hierarchies and Markets,* pp. 121–123; and Kenney, *From Pablo to Osama.*

colleagues, and informers to learn about changing conditions on the ground. But agents have the added advantage of better access to formal training. Most agents receive training in a variety of fields, including investigation, surveillance, intelligence analysis, and undercover operations and technology, and many pursue advanced education.[86] The same amount of routinized knowledge is difficult to transmit in dispersed clandestine networks. The network literature tends to downplay the importance of formal instruction and skill transfer. Informal contacts facilitated by communications technologies are often considered sufficient to transmit skills among networked actors. For example, the literature is rife with examples of how terrorist manuals and bomb recipes can be downloaded freely from the internet. Yet, internet manuals and recipes (on bomb building and other tactics) are often too imprecise to be of practical use.[87] To learn how to use advanced weapons and tactics, already knowledgeable students must be taught by experts. It is no coincidence that some of the most successful militant organizations have relied on central training camps to teach their associates basic skills. Fatah, the PLO, Hezbollah, and the Taliban all built training camps where militants took courses on intelligence gathering, bombing, the organization of cells, and so on.[88] Such centralized learning camps, however, have proven a security liability in an age where these networks have been ferociously targeted by states.

A third barrier to learning in networks is lack of organizational memory. Organizations learn by distilling lessons and storing them in ways that are accessible to others, despite the turnover of personnel and passage of time.[89] To be sure, criminal enterprises can record knowledge, relying on manuals, notebooks, and computers.[90] Yet, there are limits to what can be written down or saved to a computer without compromising security. Informal organizational memories, dependent on error-prone human recollection, are unlikely to be as reliable as formal ones. Organizational memory may end up fragmented and

86. Michael Kenney, in *From Pablo to Osama*, p. 81, details the comprehensive training of "narcs" (narcotics police) but does not believe that this gives them any crucial advantage in the field.
87. See David E. Smith, "The Training of Terrorist Organizations," CSC Report, *Global Security .org,* 1995, http://globalsecurity.org/military/library/report/1995/SDE.htm; and Javier Jordan, Fernando M. Manas, and Nicola Horsburgh, "Strengths and Weaknesses of Grassroot Jihadist Networks: The Madrid Bombings," *Studies in Conflict and Terrorism,* Vol. 31, No. 1 (January 2008), pp. 17–39.
88. For an overview of illicit training camps, see Gunaratna, *Inside Al Qaeda,* pp. 93–101.
89. Barbara Levitt and James G. March, "Organizational Learning," *Annual Review of Sociology,* Vol. 14 (1988), pp. 319–338.
90. On these practices, see Kenney, *From Pablo to Osama,* p. 56.

fallacious, because no central authority is responsible for consolidating and vetting it. Thus, networked actors may not be able to translate lessons learned into solid improvements in organizational practice.[91]

History suggests illicit networks are far from nimble learners. As we have shown, in the Montreal drug network, police seizures did not prompt any sustained attempts to learn and adapt. Traffickers instead struggled ever more recklessly to get things back on the road to sustain their reputation, and the network collapsed. The persistent inability in the late nineteenth century of the anarchists to learn from past mistakes is another example. Research on the German anarchists, in particular, highlights security liabilities and learning difficulties flowing from a networked structure. The German anarchists were an informal group, largely autonomous within a broader transnational structure.[92] No one was responsible for establishing and enforcing security procedures. As a result, by the early 1880s, the Berlin police had thoroughly infiltrated their ranks and curtailed their activities. In response, individual anarchists attempted to institute changes that would enhance security. A London-based anarchist, Viktor Dave, proposed creating a small commission of known, trusted anarchists that would be responsible for smuggling *Freiheit*, their banned journal, to its subscribers on the continent. The smuggling process had previously been informal and unregulated, leading to frequent arrests of couriers. Rival leaders on the continent, however, felt that reliance on a central distribution center in London would heighten vulnerability. As no one was in overall charge, no central decision was made, and the police continued to infiltrate the group and arrest anarchists. Although they recognized the pitfalls of their practices, the anarchists could not transcend their networked structure to institute changes that would make them more secure.

Perils of Networking: The Case of al-Qaida

So far we have focused on limitations of the network form using theoretical and mainly historical evidence. But are clandestine actors in the twenty-first century more sophisticated users of the network form? In this section we con-

91. Michael Kenney documents this problem with respect to drug-trafficking networks. Kenney, *From Pablo to Osama*, p. 115.

92. On the anarchists and their structure, see Andrew R. Carlson, *Anarchism in Germany*, Vol. 1: *The Early Movement* (Metuchen, N.J.: Scarecrow, 1972), especially pp. 334–376; and James Joll, *The Anarchists* (London: Eyre and Spottiswoode, 1964).

sider a contemporary networked threat: al-Qaida.[93] Al-Qaida is a particularly good case in which to probe the presence of network weaknesses. Received wisdom about al-Qaida emphasizes classic advantages of a networked structure, including adaptability, resilience, and rapid learning.[94] In its evolution so far, al-Qaida has proved both adaptable and robust. From an essentially "visible" organization, running training camps and occupying territory in Afghanistan, al-Qaida has transformed itself into a global jihad movement increasingly consisting of associate groups and ad hoc cells all over the world.[95] Despite losing its base in Afghanistan, al-Qaida has not lost its ability to mount terrorist attacks. The attacks against the Ghriba synagogue in Tunisia in April 2002 provided the first signs of the movement's resiliency. These incidents were followed by attacks in Pakistan (May 2002); Kuwait, Yemen, and Indonesia (October 2002); Kenya (November 2002); Turkey (November 2003); Madrid (March 2004); London (July 2005); Jordan (November 2005); and Algeria (December 2007). Add to this a series of spectacular plots that have been foiled only by a concentrated international effort by police and intelligence services.

Yet, like its predecessors, the al-Qaida network reveals familiar weaknesses. In this section we highlight three points that cast doubt on the strength of al-Qaida as a networked actor. First, al-Qaida carried out its most successful missions when it was relatively hierarchically structured. The al-Qaida that perpetrated the September 11, 2001, attacks was not really organized as a network. Indeed, many of al-Qaida's traditional strengths seem to build on a hierarchical structure, which has been increasingly difficult to sustain as the organization has come under stress. Second, as the organization fans out into a more loosely structured network, it appears to be losing unity, cohesion, and collective-action capacity. To regain capacity for large-scale attacks, al-Qaida may have to recentralize at least some of its core activities; yet this will make it more vulnerable to attack. Third, although the al-Qaida network has perpetrated some spectacular terrorist attacks, many more plots have been foiled.[96]

93. Much has been written and said about al-Qaida, and we do not pretend to be experts. What we have to say is all based on publicly available information.
94. See, for example, Gunaratna, *Inside Al Qaeda;* David Benjamin and Steven Simon, *The Age of Sacred Terror: Radical Islam's War against America* (New York: Random House, 2003); Jason Burke, *Al-Qaeda: Casting a Shadow of Terror* (London: I.B. Tauris, 2003); and Sageman, *Understanding Terror Networks.*
95. Cronin, "How al-Qaida Ends."
96. A statement in November 2006 by Eliza Manningham-Buller, then director-general of the British Security Service, indicated that authorities were aware of nearly thirty plots, many with links to al-Qaida in Pakistan. See Bruce Hoffman, "The Myth of Grass-Roots Terrorism: Why Osama bin Laden Still Matters," *Foreign Affairs,* Vol. 87, No. 3 (May/June 2008), pp. 133–138.

That a majority of plots by the world's allegedly best-led and best-trained terrorist organization are foiled is perhaps of scant comfort to police chiefs and frightened publics, but it does throw doubt on the network as a superior organizational form.

HIERARCHY AS KEY TO SUCCESS

What is most revealing, perhaps, is the evidence that al-Qaida's most successful operations took place when the organization possessed a hierarchical structure. In the 1990s al-Qaida had a significant degree of hierarchy and formal organization in the top tier, though lower levels remained more loosely structured. Organizationally, the core of al-Qaida (central staff) was a tight hierarchy with Osama bin Laden at the top, supported by a *shura majlis* (consultative council). This leadership oversaw a tidy organization of committees with well-defined positions and responsibilities.[97] When defined to include its regional affiliates, al-Qaida assumed a more networked form with regional hubs acting as subcontractors, who maintained substantial autonomy.[98] But although some operations were carried out with local autonomy and limited hierarchical management, successful ones typically received close supervision from above. Indeed, the top tier closely managed the 1998 bombings of U.S. embassies in East Africa and the September 11 attacks. Moreover, al-Qaida until 2001 was not stateless; it used Afghanistan under the Taliban as a base to centrally plan and coordinate terrorist operations around the world. Despite conventional wisdom about the efficacy of dispersed networks, it appears therefore that many of al-Qaida's traditional strengths may have built on hierarchy and centralized training and coordination.

NETWORKED VULNERABILITIES

The loss of Afghanistan as a base in 2001 scattered al-Qaida, forcing it to adapt by becoming more decentralized and networked. Although observers disagree on the extent to which al-Qaida's core is still operationally intact, most experts agree that al-Qaida today operates less like a top-down structure and more like a loose umbrella group, offering inspiration and legitimacy to radical Islamists from varying backgrounds but not necessarily providing much strategic or tactical support.[99] To many the transformation of al-Qaida from a fairly central-

97. The second tier consisted of a military committee, a finance and business committee, a religious committee, and a media and publicity committee. See Gunaratna, *Inside Al Qaeda,* p. 77.
98. Kahler, "Collective Action and Clandestine Networks."
99. Some observers, such as Marc Sageman, argue that al-Qaida has ceased to exist as either an or-

ized hierarchical organization into a more diffuse transnational network has made it a more formidable enemy, better capable of scaling and of avoiding detection. But decentralization and segmentation have also exposed al-Qaida to the gamut of organizational dilemmas associated with a networked structure.

A major problem flowing from a looser networked structure is poorer security. Before the destruction of al-Qaida's logistical infrastructure, the consultative council considered and approved all major operations.[100] Members or associate groups would typically submit proposals to the council, which would select a small number for further development and assist with seed money, training, and tactical support. After al-Qaida was forced to decentralize into smaller operational units, affiliated groups started to act on their own initiative without centralized clearance for attacks and with limited links to the network. The Bali cell, which conducted the 2002 bombings, consisted of around twelve activists that apparently came together of their own initiative, chose their own target, and executed the attack independently.[101] The Madrid train bombings in 2004 were carried out by a local cell of Moroccan immigrants, which was inspired but not directed by al-Qaida.[102] The 2005 London bombings too were carried out autonomously.[103]

As one might expect, enhanced autonomy has led to security problems. Like

---

ganizational or an operational entity; others, such as Bruce Hoffman, insist that "the centre holds." They point to recent intelligence analyses by U.S. and British security services that suggest al-Qaida still exercises top-down planning and command and control capabilities from its new position along the Afghani-Pakistani border. See Hoffman, "The Myth of Grass-Roots Terrorism"; and National Intelligence Council, "National Intelligence Estimate," July 2007. We agree that al-Qaida has not been operationally "neutralized." Pursuit by U.S. and coalition forces has, however, forced it to grow much more dispersed and decentralized.

100. See Peter L. Bergen, *The Osama bin Laden I Know: An Oral History of Al Qaeda's Leader* (New York: Free Press, 2006).

101. The Bali bombing was implemented by a fringe within JI with no input from the majority of the organization, including high-level leadership. See Burke, *Al-Qaeda*, pp. 265–266; Magouirk, Atran, and Sageman, "Connecting Terrorist Networks"; and Pavlova, "From a Counter-Society to a Counter-State Movement."

102. See Jordan, Manas, and Horsburgh, "Strengths and Weaknesses of Grassroot Jihadist Networks"; Loren Vidino, "The Hofstad Group: The New Face of Terrorist Networks in Europe," *Studies in Conflict and Terrorism*, Vol. 30, No. 7 (July 2007), pp. 579–592; and Aidan Kirby, "The London Bombers as 'Self-Starters': A Case Study in Indigenous Radicalization and the Emergence of Autonomous Cliques," *Studies in Conflict and Terrorism*, Vol. 30, No. 5 (May 2007), pp. 415–428.

103. The group responsible for the London bombings appears to have received some support from al-Qaida's network in Pakistan, but the group was not formally linked to al-Qaida and had limited links to the network. See Vidino, "The Hofstad Group"; and Kirby, "The London Bombers as 'Self-Starters.'"

the London bombers in 2005, newcomers seek guidance, legitimacy, and tactical support from the network, where they can get it, but are not afraid to act independently. Relying on informal connections and rules of conduct and operating in the absence of institutionalized training or recruitment, many are strikingly naïve about security.[104] Some of the most prominent cells in Europe and North America, including those in Montreal, London, and Milan, were closely monitored by the police before being uncovered. Recent plots in Britain involved militants under easy surveillance for months and even years.[105] The group that orchestrated the Madrid bombings also provides a good example of amateurism in autonomous groups. Only one of the group's members had passed through training camps or had experience in terrorist campaigns.[106] The group's lack of professionalism meant it committed grave mistakes, which eventually led to its downfall. For example, the bombs the group's members used were of poor quality, and three of the thirteen bombs did not explode. One of these unexploded bombs provided information that led to arrests just days after the bombings.[107] The group's efforts to secure logistical support also put it in danger. Unlike the September 11 suicide pilots who maintained few ties with other individuals in the United States, the Madrid group needed to be in close contact with its social environment to gather logistical support. Lacking secure links to the al-Qaida network, the group's efforts to recruit members and acquire arms through local mosques brought them into contact with a Moroccan police informant, who was posing as an imam, and several police informants on drug matters who almost thwarted the plot.[108] This is far from an unusual case. In 2006 seven men in Miami reportedly planning attacks against the Chicago Sears Tower sought to work with someone they thought was an al-Qaida member who turned out to be an FBI informant.[109] Lacking formal avenues of access, these militants did not have a secure way of connecting with the greater al-Qaida community. As

104. For evidence of security naïveté, see Olivier Roy, *Globalized Islam: The Search for a New Ummah* (London: Hurst, 2004).
105. See, for example, John Ward Anderson and Karen DeYoung, "Plot to Bomb U.S.-bound Jets Is Foiled," *Washington Post,* April 11, 2006; and David Stringer, "London Subway Attackers Linked to Al-Qaida, Colluded with Other Terror Cells," Canadian Press Newswire, April 30, 2007.
106. See Jordan, Manas, and Horsburgh, "Strengths and Weaknesses of Grassroot Jihadist Networks."
107. Ibid.
108. Ibid.
109. Jerry Seper, "Miami Terrorism Suspects Planned 'War' against U.S.," *Washington Times,* June 29, 2006.

these examples show, informal links established by dispersed militants are often precarious.[110] The more the al-Qaida network attempts to expand through "weak links," the less secure it may become.

The lack of centralized sanctioning of missions is also proving perilous. To network enthusiasts, al-Qaida's increasingly diffuse structure encourages expansion and innovation through local experimentation. Yet, increased local initiative is a mixed blessing. Take the example of Zuhair Hilal Mohammed al-Tubaiti, who was arrested for planning an operation against U.S. naval vessels in the Strait of Gibraltar. Upon his arrest, he told the Moroccan authorities that al-Qaida had originally rejected him for a martyrdom mission. Reduced hierarchical control following the loss of the Afghan base empowered him to experiment on his own instead of waiting for approval from above.[111] Although he acted alone, his failure harmed the wider organization via his betrayal of sensitive information.

Al-Qaida has also displayed weaknesses in coordination and strategic planning.[112] The 1999 millennial plot against the Los Angeles airport fell apart when the plotters were identified and arrested, one by one, until Ahmed Ressam was left to carry it out on his own. Inexperienced and acting without reliable organizational support, he was easily caught as he tried to enter the United States with a car full of explosives. In 2000 the overloaded boat of explosives targeting the USS *The Sullivans* in the port of Aden actually began sinking before it could do any damage. The locally planned attack against U.S. naval vessels in the Strait of Gibraltar in 2002 appears to have crumbled as a result of communication failures.[113] If the London car bomb plot and Glasgow airport attack discovered in June 2007 are related to al-Qaida, these too reveal poor planning. Even the September 11 attacks show signs of strategic planning failure. Although it demonstrated al-Qaida's ability to hit its "far enemy" at

110. A case in point is Ishtiaque Parker, a student whom Ramzi Yousef, one of the conspirators in the 1993 World Trade Center bombing, attempted to recruit. Yousef wanted to use Parker to transport explosives but their connection was weak. Parker eventually betrayed information leading to Yousef's arrest in 1995. See Bill Keller, "Self-portrait of Informer: An Innocent," *New York Times,* February 21, 1995; and Sageman, *Understanding Terror Networks,* p. 109.

111. Francina Bester, "New Trends in Contemporary International and Transnational Terrorism," University of Pretoria, 2007.

112. For these examples, see Alan Cowell, "Police Find Two Car Bombs in Central London," *International Herald Tribune,* June 29, 2007; Elaine Sciolino, "Casablanca Bombers Were Probably Lost," *International Herald Tribune,* May 20, 2003; and Sageman, *Understanding Terror Networks,* pp. 45–56, 99–103.

113. See Bester, "New Trends in Contemporary International and Transnational Terrorism."

home, September 11 turned out to be a disaster for al-Qaida because it led to the destruction of its extensive hierarchical infrastructure in Afghanistan.[114] This outcome does not appear to have been anticipated. As Kahler notes, what is striking about the planning for September 11 is the apparent absence of efforts to comprehend or undermine the likely U.S. response: apart from escaping Afghanistan, the leadership does not appear to have made substantial efforts to disperse key assets such as their training camps. This and other strategic failures may be the result of a highly secretive organization that thrives on limited social embeddeness and whose members are therefore cut off from wider sources of information.[115] With increased decentralization, such problems are likely to worsen.

Learning too has proven feeble in an increasingly diffuse al-Qaida network. In particular, the loss of Afghanistan as a central headquarters for professional training has made learning a more improvised and unreliable affair. The Casablanca bombers, for instance, were trained haphazardly on weekend camping trips, and their homemade explosives were erratic, with only one resulting in mass casualties.[116] Improvised learning is also likely to reduce accountability.[117] In the camps, al-Qaida had the opportunity to evaluate trainees, choosing only the best for formal participation in operations. With less hierarchical oversight, members are now left to evaluate their own capacities and learn from their own mistakes. Rohan Gunaratna refers to al-Qaida as a "learning organization," noting that when bin Laden discovered his satellite phone conversations were being monitored, he used this knowledge to mislead and evade coalition forces targeting him at Tora Bora in 2001.[118] Yet al-Qaida at large has still not learned the lesson. Its informal networked militants continue using easily monitored phones. In 2004 London authorities tapped more than 100 phone lines during their operation against the militants planning the infamous fertilizer bomb attack.[119] Perhaps bin Laden is learning, but the broader network appears less advanced.

The main benefit of increased decentralization and segmentation is that it

114. Bergen, *The Osama bin Laden I Know.*
115. According to Miles Kahler, al-Qaida's relatively closed network simply did not provide it with useful information about the motivations and likely actions of its principal adversary, the United States. See Kahler, "Collective Action and Clandestine Networks."
116. Sageman, *Understanding Terror Networks.*
117. Bester, "New Trends in Contemporary International and Transnational Terrorism."
118. Gunaratna, *Inside Al Qaeda,* p. 107.
119. Stringer, "London Subway Attackers Linked to al-Qaida."

has enabled al-Qaida to scale by building informal links to regional hubs.[120] But although many see al-Qaida's increased reliance on informal connections to other groups as an indicator of increasing strength, it can equally be interpreted as a weakness.[121] Indeed, there are signs that growing inclusiveness is leading to a more disjointed and disunited movement. The al-Qaida network has involved ambitious upstarts such as Abu Musab al-Zarqawi, more traditional organizations such as Egyptian Islamic Jihad, regionally focused groups such as Jemaah Islamiyah, ragtag insurgents in Iraq, converts such as John Walker Lindh and Richard Reid, and "home-grown" militants living in Europe, often with little connection to the Middle East. As Richard Matthew and George Shambaugh note, it would be a grave mistake to assume that all the members of al-Qaida share an understanding of goals and strategy.[122] Problems of disunity could be seen already in the 1990s. Fawaz Gerges, for example, argues that the inner group was "riven by ethnic, regional, and ideological rivalries."[123] Such problems intensified in the late 1990s. After 1998, when bin Laden called for abandoning the struggle against the "near enemy" in favor of global jihad against the United States, al-Qaida lost many members who hesitated to take on the United States.[124] As the network fans out, new rifts are emerging. Challenging the West means different things to different cells that are often engaged in local power struggles. The increasing autonomy of leaders within the network has also fueled acute internal conflicts, limiting expansion and collective action. For example, when Ayman al-Zawahiri brought his Egyptian Islamic Jihad organization into the fold of al-Qaida, several of his top lieutenants opposed the merger and left.[125]

---

120. A sample of groups that are allegedly connected to al-Qaida includes the Moro Islamic Liberation Front (Philippines), Jemaah Islamiyah (Southeast Asia), Egyptian Islamic Jihad, al-Ansar Mujahidin (Chechnya), al-Gama'a al-Islamiyya (Egypt), the Abu Sayyaf Group (Philippines), Hezbollah (Lebanon), the Islamic Movement of Uzbekistan, the Salafist Group for Call and Combat (Algeria), and Harakat ul-Mujahidin (Pakistan). See Daniel Byman, "Al-Qaeda as an Adversary: Do We Understand Our Enemy?" *World Politics,* Vol. 56, No. 1 (October 2003), pp. 139–163, at p. 258; and Cronin, "How al-Qaida Ends," p. 33.
121. See Cronin, "How al-Qaida Ends," pp. 33–34.
122. Richard Matthew and George Shambaugh, "The Limits of Terrorism: A Network Perspective," *International Studies Review,* Vol. 7, No. 4 (December 2005), pp. 617–627.
123. Fawaz A. Gerges, *The Far Enemy: Why Jihad Went Global* (Cambridge: Cambridge University Press, 2005), p. 19, quoted in Kahler, "Collective Action and Clandestine Networks."
124. Sageman, *Understanding Terror Networks,* pp. 45–47; Burke, *Al-Qaeda,* p. 150; and Brooke, "Jihadist Strategic Debates before 9/11."
125. Roy, *Globalized Islam,* p. 73.

AN ADAPTIVE NETWORK OF A CENTRALIZED ORGANIZATION IN DECLINE?

The above discussion suggests a network plagued by internal conflict and coordination problems. The diverse, dispersed community that makes up al-Qaida is likely to grow increasingly fragile as the memories of Afghanistan fade. Al-Qaida clearly has relied on the common experiences of the mujahideen in Afghanistan and the Afghan training camps as a main source of identification and integration.[126] After the loss of the camps, militants from around the world can no longer meet face-to-face in a central location, where they might forge strong social ties, unity of purpose, and a clear sense of belonging. Contrary to the expectation of organizational network theory, the loss of a stable central base may reduce al-Qaida's ability to scale by attracting new recruits.[127]

Forcing al-Qaida to adopt a more networked structure may have done a lot to reduce the terrorist threat. Perhaps the best indication of the network's increased fragility is the changing nature of its operations. Al-Qaida continues to inspire violent actions around the world. Yet, following September 11, al-Qaida has demonstrated little ability to plan and execute complex attacks. Since 2001, terrorist actions linked to jihadist groups have nearly all been aimed at soft (nongovernmental) targets, and all appear to have been initiated by local groups with scant involvement by the al-Qaida leadership.[128] Indeed, Gerges notes, al-Qaida may have been reduced to "desperate local affiliates and cells," and what remains of the core is "an ideological label, a state of mind, and a mobilizational outreach program to incite attacks worldwide."[129] If al-Qaida as a brand name or ideology succeeds in inspiring widespread violence, then this is clearly a dangerous trend, but it is not one that can be attributed to the strength of the network itself.

Conclusion

The prevailing picture painted by mass media, public officials, and academics concerned with international terrorist organizations and other criminal net-

126. Raab and Milward, "Dark Networks as Problems," p. 20.
127. See Kahler, "Collective Action and Clandestine Networks." The reconfiguration of al-Qaida along the Pakistani border may provide a new "base" but is likely to be a poor match for the Afghan safe haven.
128. Sageman, *Understanding Terror Networks,* pp. 52–55.
129. Gerges, *The Far Enemy,* p. 40, quoted in Kahler, "Collective Action and Clandestine Networks."

works is that of a mounting danger, relentlessly on the increase around the world with governments severely hampered in their ability to combat it. But is this view justified? Theoretical arguments for why we should expect networks to be so formidable are unpersuasive, and a brief review of networks in their historical confrontations with states raises doubts about their effectiveness as actors.

To be sure, networks have many potential advantages, including flexibility, scalability, and resilience. Yet, networks cannot enjoy all these advantages at once. The network structure, though making it easier to survive, makes it far harder to engage in concerted action. Efficiency of information and communication, and hence ability to learn, often comes at the expense of covertness and security. Expansion through recruitment based on informal weak ties may enhance a network's potential impact, but it can also reduce trust and security, trigger internal strife, and intensify collective-action problems. As we have shown, a more centralized structure may often be better at dealing with complex tasks. In the end, several of the challenges facing transnational criminal organizations, including distance collaboration, collective action, learning, training, and security, are best tackled by more centralized hierarchical structures. Yet, if diffuse, clandestine, network-based groups seek to increase their organizational capacity through centralization, they will tend to generate new structural vulnerabilities that make them easier to target and neutralize.[130]

Knowing one's adversary, understanding how he is organized and what advantage this provides, is key to developing sound responses to security challenges. Many of today's transnational threats are said to be so dangerous precisely because they are evolving into diffuse networks. There is veritable nostalgia for the days of the highly centralized mafia and hierarchical drug cartels. To keep up with today's criminal networks, it is suggested, law enforcement must itself adopt a more networked structure. But this recommendation rests on uncertain logic and evidence. The very fact that problems such as drug trafficking and terrorism persist, despite law enforcement's efforts to combat them, does not imply that networks are superior to the bureaucracies pursuing them. Disadvantages claimed for hierarchies are often based on bad management and are not inherent to form. As we have demonstrated, from an organizational viewpoint, law enforcement agencies enjoy several advantages over clandestine networks, such as centralized information processing, moni-

130. Matthew and Shambaugh, "The Limits of Terrorism."

toring of activities, formal training, and reliable organizational memory. All this, combined with a significant force advantage, implies that states can inflict costs on illicit networks with a greater efficiency, and for longer periods of time, than illicit networks can with regard to states.

Illicit networks are themselves subject to several weaknesses that may be relatively easy for law enforcement to exploit. Generally, networks may be destabilized by (1) reducing the flow of communication and information through the network; (2) hampering decisionmaking and consensus formation; and (3) intensifying collective-action problems and security vulnerabilities.[131] As we have shown, a cursory look at the historical evidence suggests these sorts of failures occur spontaneously in many illicit networks when they come under stress. Law enforcement can precipitate them by targeting networks repeatedly, forcing actors to change their practices abruptly, or sowing doubt and mistrust through infiltration and manipulation of information. Counterterrorism officials may be able to take advantage of organizational splits within terrorist groups by appealing to more moderate members. Indeed, such splits can be encouraged. According to reports from prominent dissidents, the internal power struggle that ripped the Abu Nidal Organization (ANO) in 1989 and led to the execution of more than 150 of its members and 22 of its leaders was instigated by PLO agents who persuaded some members that the random violence perpetrated by ANO harmed the Palestinian cause.[132]

Terrorism and organized crime are complicated, eclectic phenomena that have multiple causes and require multifaceted responses. In this article we have sought only to draw attention to, and to question, structural features that are claimed to advantage networked criminals vis-à-vis law enforcement. Again, we are not arguing that illicit networks pose no significant threat to state security. But if they are formidable enemies, it is probably not due to their networked structure so much as other factors, such as the personal attributes of their members or their sheer depth in numbers. The argument that a hierarchical structure does not per se disadvantage state actors should not lead to complacency about the way illicit networks are combated, and there is much room for improvement in the way counterterrorism and drug law enforcement are practiced. As states have widely realized, we need better international re-

131. See Kathleen M. Carley, Ju-Sung Lee, and David Krackhardt, "Destabilizing Networks," *Connections,* Vol. 24, No. 3 (Winter 2001), pp. 79–92.
132. Youssef M. Ibrahim, "Arabs Say Deadly Power Struggle Has Split Abu Nidal Terror Group," *New York Times,* November 12, 1989.

sponses to transnational threats, along with smoother intelligence sharing and interagency cooperation. Red tape can also be profitably reduced. Yet, bureaucracy may still be better than its alternatives. Despite the current mood of skepticism about traditional, inflexible bureaucracies, centrally instituted changes do reduce inefficiencies. In a network, inefficient practices and red tape may be bypassed more easily by autonomous local players, but the resulting ad hoc solutions may prove counterproductive. Although law enforcement agencies may still have far to go, there is nothing inherent in the network form that makes it impossible for hierarchical state structures to combat networked adversaries.