International Studies Review (2005) 7, 617–627

The Limits of Terrorism: A Network Perspective[1]

RICHARD MATTHEW
School of Social Ecology and Center for Unconventional Security Affairs, University of California, Irvine

AND

GEORGE SHAMBAUGH
School of Foreign Service and Department of Government, Georgetown University

Capturing the spirit of the late 1970s and early 1980s, Robert Gilpin (1981) explained how the diffusion of technology and other capabilities was leading to the decline of US hegemony relative to rising challengers. After a brief hiatus during the halcyon decade of the 1990s that followed the end of the Cold War, the hegemon is once again under siege. This time, however, networks of discontented individuals and groups have joined the ranks of states in exploiting the diffusion of modern transportation, communication, and technology to challenge the dominant state(s) in the system (Deutsch 1966; Rosenau 1990; Rosenau and Czempiel 1992; Risse-Kappen 1995; Zacher and Sutton 1996; Slaughter 2004). Enabled or amplified by the technological innovations and diffusions that have characterized the last several decades, network-based threats include identity theft, drug trafficking, infectious disease, and terrorism (Matthew and Shambaugh 1998; Lilley 2003; Sageman 2004; Friedman 2005).

We agree with arguments that contend that network-based threats are difficult to defeat and pose a long-term challenge to security, especially at the individual level. But the resilience of networks is not limited to terrorists and criminals; it is a prominent feature of contemporary states and gives them considerable protection as well. Moreover, most networks face significant collective action problems that limit what they can achieve. These characteristics make it extraordinarily unlikely that terrorists or other such actors will be able to undermine the national or homeland security of countries or, indeed, achieve any long-term strategic goals (Matthew and Shambaugh 2005). Consequently, even though terrorism poses a grave and persistent threat to personal security and a wide range of devastating attacks are possible, we argue that its threat to national security is at times poorly characterized and, hence, misrepresented. The West is never likely to win a global war against terrorism or other network-based threats, but, like terrorists, nation-states can impose large costs on individuals or groups within the network. Their organizational structures enable them to do so with a greater efficiency and a greater degree of coordination over a longer period of time than their network-based adversaries. If diffuse terrorist groups succeed in overcoming the collective action problems of networks, their institutionalization will generate new preferences and vulnerabilities that may make them easier to control.

[1]This essay builds on a paper entitled "New Modalities of Power" that was presented at the annual meeting of the International Studies Association in Montreal, Canada on March 20, 2004. We would like to thank Michael Brown, Melissa Burman, Bryan McDonald, Erik Noreen, and Volker C. Franke for their comments on subsequent versions of the essay.

Published by Blackwell Publishing, 350 Main Street, Malden, MA 02148, USA, and 9600 Garsington Road, Oxford OX4 2DQ, UK.

In this essay, we begin with a brief discussion of networks. We next focus on four insights generated by using networks as a means for understanding threats and the interactions among potentially threatening actors in world politics. First, we argue that networks are easy to access but hard to destroy. In particular, even though economic, political, and technological networks enhance the ability of would-be assailants to attack individuals, they also give Western states a defensive advantage. Consequently, terrorists can readily threaten the security of individuals but can do relatively little to undermine homeland or national security. Second, the collective action problem of networks makes coordinated efforts within them difficult to maintain. As the numbers of terrorist or other network-based groups and the number of issues at stake increase, these problems multiply and the likelihood of fragmentation within the network grows. Third, although deterrence is not effective against an entire network, it can be effectively used in a more targeted manner against nodes within a network. Fourth, if network-based groups are able to increase their organizational capacity so they can pursue more elaborate and enduring goals, the higher levels of coordination will generate new preferences and new vulnerabilities that make them easier to target and neutralize. Beyond its usefulness as a descriptive tool, we argue that applying network theory to the problem of terrorism provides more general insights for international relations theory and practice. In this vein, we conclude with some general observations about the rise and fall of great powers and policy recommendations regarding national responses to network-based threats.

Basic Characteristics of Networks

The mathematician Albert-Laszlo Barabasi argues that two types of networks exist (Barabasi 2003; Watts 2003; see also Buchanan 2002; Matlis 2002). The first, which he calls random networks, are composed of nodes that are randomly linked to each other. In this structure, each node will tend to have about the same number of connections as all the other nodes. The Internet originated as a random network with a small number of similarly interconnected nodes. The value of this type of network becomes limited as it grows because it quickly becomes cumbersome to navigate. As the ratio between noise and useful information increases, the transaction costs of using the network rise dramatically. As a consequence, random networks tend to be used by a limited set of actors for specific purposes. For example, some schools use a telephone tree to transmit information quickly. The school principal calls five parents. Each parent then relays the information to four more parents who do the same, and so on. Each person (or node) has exactly five links to the overall network. Within minutes, hundreds of people can be personally contacted through this network. But as dramatic and effective as such a network is for this particular purpose, it cannot be navigated easily or readily used for other purposes.

Far more common in society are what Barabasi calls scale-free networks in which a relatively small number of nodes, referred to as hubs, develop connections to a very large number of other nodes (hence the term "scale-free"). Like Google on the Internet, the main stations of the postal system, or major airports, the hubs serve as focal points for linking nodes. The existence of hubs reduces transaction costs by providing routing, coordinating, and information functions that increase the ease and efficiency of navigating the network. Although early hubs, like the French Minitel or the US Internet company Prodigy, can quickly be replaced by more sophisticated coordination systems like Yahoo, these changes do not alter the diacritical characteristics of the scale-free network.

These characteristics can be summarized as follows: scale-free networks display a *power distribution* (as opposed to a normal distribution) in which a small number of nodes may have an enormous number of links, far above the average links per node

for the whole network. There is an *absence of hierarchy* to shape stocks and flows in the network, although there are *preferential attachments* based on seniority and fitness as well as *clustering*. Networks are *dynamic* entities well suited to growth and change and, yet, *robust* in the face of an array of challenges. Among their great assets are their abilities to *shrink the distance* between any two nodes by finding efficient routes between them and to connect nodes through rerouting when a pathway is blocked. Finally, they are not amenable to reductionist analytical strategies; individual nodes or defined relationships within the network disclose very little about the network as a whole, and, hence, understanding the whole requires a holistic or systems approach.[2]

As anyone who has ever used the Internet knows, a wide range of actors can easily take advantage of the navigation opportunities offered by scale-free networks. For example, just as scholars might use Google to conduct research on the web, tourists can use it to obtain travel information, patients can surf for medical links, and terrorists can use it to recruit, communicate, identify targets, and acquire expertise and technology. As we have argued elsewhere, the same webs that empower contemporary economic and political systems generate incentives, capabilities, opportunities, and vulnerabilities for illicit actors that have important implications for human and national security (Matthew and Shambaugh 1998). In addition to exploiting existing networks, entrepreneurs can also establish hubs within scale-free networks or create new networks that may be utterly autonomous or strategically linked to other networks by defendable bridges, as an island may be linked to the mainland.

From a security perspective, scale-free networks have a clear advantage over other random or hierarchical ways of structuring relationships in that their diffuse, decentralized structure decreases their system-wide vulnerability. System-wide vulnerability is low because so many nodes have to be removed before a network begins to fragment and collapse. This fact was a primary motivation for DARPA's original design of the Internet, which was based on creating enough redundant links to ensure that the system could survive a nuclear attack against the United States (Internet History 2005). The fact that scale-free networks are easy to access but difficult to destroy has important implications for terrorism, which we consider in the next section.

Limitation 1: Networks Are Easy to Access, But Hard to Destroy

Because scale-free networks are easy to access and navigate, they are useful to terrorists in several ways, including:

1. Terrorists can use networks as an empowering resource in recruiting, training, and preparing for an attack.
2. Terrorists can use networks as delivery systems.
3. Terrorists can use networks as targets.
4. Terrorists can use networks after an attack for propaganda purposes.

More than a decade ago, Daniel Deudney and John Ikenberry (1991/1992) argued that one reason why the Soviet Union fell apart was that it lost control of information. Technology gave Russians access to alternative sources of information and made it possible for Soviet citizens to compare their world with the Western world and draw their own conclusions about which system was faring better in different areas. Totalitarianism was defeated, at least in part, by information technology that challenged its performance claims.

[2]This description of networks is drawn from Barabasi (2003).

Ironically, this technology has proven to be a mixed blessing for the West. Combined with the openness of Western political and economic systems, many analysts contend that another outcome has been to magnify the West's vulnerability to transnational threats like terrorism. Frightened by the openness it once championed, the post-September 11 US public has supported a neoconservative takeover of the executive, legislature, and judiciary branches of government. This change, some analysts have argued, has undermined the systems of checks and balances conceived by the founding fathers and gravely diminished political debate (Chomsky 2002). So dominant is this perception of vulnerability that the only policy solution on the table so far involves significant constraints on individual freedom marketed as essential tradeoffs for satisfactory levels of personal and national security.

We argue that this line of policy thinking is not well supported by reason or evidence. It is certainly the case that terrorists and other criminals can use existing networks for the four purposes identified above. It is also true that filters and other measures designed to keep such activities from happening will often be ineffective or so intrusive as to undermine the values they seek to protect. The war on drugs, begun in 1973, illustrates the problem well (Schaffer 2005). For 30 years, enormous sums of money have been expended, drug cartels have been dismantled, and many US citizens and others have been jailed, but the flow of drugs and the percentage of the population using them have not diminished. The costs and inconveniences of the drug war do not seem to be justified by the results.

Most of this policy-oriented discussion ignores an important point: the multiple scale-free networks inherent in democracy, the scale-free economic networks imbedded in advanced capitalism, and the scale-free transportation and communication networks that we rely on every day may be easy to access and attack, but they are also tremendously resilient and hence very difficult to disable or destroy. Individual nodes in any of these networks can be reached and harmed, but an extensive and almost inconceivable multinodal attack would be required before the networks themselves could truly be disabled.

In short, networks do define much of the Western world today and, as a result, terrorism poses a very real (but nonetheless statistically small) threat to personal security everywhere. Terrorists can reach anyone and often attack with impunity; their acts have flooded the world's media with images of innocent, unsuspecting people destroyed as they go about their daily business. However, in any traditional sense of the term national or "homeland" security, the threat to the United States as a state, or to the West in general, has often been exaggerated.

The speed with which the United States recovered from the September 11 attacks and with which Spain and the United Kingdom have recovered from al-Qaeda acts in 2004 and 2005, respectively, lend empirical support to what network theory predicts. Of course, predictions have not been the strong suit of international relations theory, but we believe that claims about the devastating potential or likely consequences of another act of terrorism on US soil tend to underestimate the country's great resilience and multifaceted strength, attributes that are amplified by the networks that have come to fill its political and economic space.

In addition, the multiple scale-free networks that make up Western societies are overlaid by organized legal systems that enable political leaders to mobilize and exploit these webs to achieve common objectives. Indeed, when faced with threat, democracies in general, and the US democracy in particular, are remarkably quick to mobilize and very willing to follow a strong leader and apply massive amounts of force, even if doing so is very costly (Small and Singer 1976; Doyle 1983a, 1983b; Zacher and Matthew 1995). Under the condition of total war—that is, war that involves the entire nation—the values, beliefs, practices, and institutions of a democracy can experience a rapid transformation as it acts to preserve itself. In fact, this transformation is often a matter of policy insofar as democracies typically have

the legal capacity to implement martial law, streamline decision making, and consolidate authority and resources.

In less extreme circumstances, the US government and other groups in the West are increasingly taking advantage of scale-free networks at the global level to optimize cooperation in areas like security. According to Anne-Marie Slaughter (2004:214), "networks of government officials—police investigators, financial regulators, even judges and legislators—increasingly exchange information and coordinate activity to combat global crime and address common problems on a global scale."

Limitation 2: Networks Are Easy to Create, But Hard to Control

Terrorists can access existing networks; they can also create new ones. For example, al-Qaeda has used its prestige and technological aptitude to bring together disparate terrorist entities for a wide range of interactions loosely unified by an anti-US, anti-Israel, or anti-Western attitude. The interconnected nature of a scale-free terrorist network with hubs like al-Qaeda makes it possible to coordinate terrorist activities on an ad hoc basis. Hence, disparate groups may find ways to benefit from the financing, arms shipments, logistical support, camaraderie, and other assets of kindred nefarious actors who can be accessed through such hubs. However, from the perspective of any node, a hub is a means, not an end. Therefore, loyalty to it may be entirely contingent on the value of the connecting service. If Google were disabled or increased the cost of its service, users could shift rapidly to another search engine without significant consequences. Similarly, if the kingpin of a drug cartel is arrested or killed, mules and dealers are likely to shift to another source rather than invest time trying to resurrect the hub that has been disabled.

Following the success of the September 11 attacks, Osama bin Laden was able to establish his group as a hub for global terrorism, and al-Qaeda quickly became a focal point for a network of terrorist groups seeking to challenge the West. It would be a mistake, however, to assume that all the members of this network share a common understanding of goals and strategy. What we call "the collective action problem of networks" suggests that the ability to reach a consensus on goals and ends will increase in difficulty with the number of nodes in the network and the number of issues they seek to address.[3] Challenging the West means different things to different cells. Moreover, matters are further complicated because many are engaged in very local power struggles. In his review of recent studies of al-Qaeda, Daniel Byman (2003) provides a long list of loosely connected motivations for joining the network. These include disparate grievances about US foreign policy in places such as Iraq, Pakistan, and Saudi Arabia; hatred of Israel; concerns about civil versus religious governance; anger about perceived injustices against the Muslim world; concerns about the intrusion of global markets and culture into traditional societies; and a variety of highly particular, local issues. Consequently, although many groups may be attracted to al-Qaeda because of its high profile or to Iraq because of the relative ease of attacking US personnel there, it is unlikely that a network structure will be conducive to mobilizing the many nodes around a more concrete and constructive agenda leading to an enduring legacy.

Of course, a coalition of terrorists may form and be held together by a common overriding objective—such as driving the United States out of the Middle East—even if its members disagree over how best to achieve this objective or have other interests. But, according to Ernst Haas (1980), coalitions based on this type of

[3]William Riker (1982) provides a very useful analysis of the impact that increases in the number of actors (voters) and the number of competing objectives (alternatives) have on Condorcet cycles. Although Riker focused on the problems of aggregating individual preferences in a voting system, the same insights apply to the question of coordinating group actions toward a common goal.

"fragmented" linkage also tend to be difficult to maintain. Although charismatic leadership, dramatic successes, and the demonization of an adversary can bolster fragmented linkage, studies of the "rally around the flag effect" suggest that these effects are transient and tend to fade quickly unless direct and immediate benefits or threats accrue to the individual members of the coalition (Shambaugh and Josiger 2004). This finding leads to the suggestion that any coalitions of terrorists brought together by bin Ladin following the successful attack on the United States will be situational and hard to maintain.

Furthermore, and somewhat ironically, the dramatic effects of the attack on the United States tend to undermine the sustainability of any coalition of terrorists based on fragmented linkage because (a) it will be hard to create something with a similar level of effect, and (b) it showed how little effect even such a dramatic attack had on al-Qaeda's overarching proclaimed objectives (like driving the United States out of the Middle East). It also clarified the specific benefits and specific costs that each individual terrorist cell incurred as a result of the events of September 11 and their aftermath. This information gives future would-be terrorists a baseline against which to assess the promises made by al-Qaeda and how going along with al-Qaeda could help or hurt their ability to reach their particular goals. For some, the benefits of September 11 and its aftermath likely outweighed the costs, but for others the costs likely have outweighed the benefits. The more the costs and benefits have varied around the network (both before and after September 11) and the more transparent these differences have become, the less cohesive the network is likely to be.

Constituted as a global network, terrorism has acquired a relatively stable force multiplier that makes it easier for attackers to cooperate and hence to achieve higher levels of success in causing harm and fear. Nonetheless, as we observed earlier, hubs are a means, not an end; stability is achieved by servicing different end users, not by mobilizing disparate entities around a shared vision and strategy. Al-Qaeda may attract terrorists to South Asia or to Iraq, but control over them will not be reliable and may never emerge at all. In terms of national security, such a threat is quite unlike that posed by the Soviet Union or China.

The crusades of the Middle Ages provide a compelling and familiar historical example of this problem. The Catholic Church was able to bring diverse people together, but it was unable to manage them. In 1096, the First Crusade was initiated by Urban II. He succeeded "in summing up and fusing in a single ideal a whole range of aspirations which were contemporarily powerful" (Keen 1967:99). By gathering opportunities for spiritual, martial, and economic ambitions together, people with markedly different fears, needs, and desires were briefly united to serve the church. But the church was not able to control the many expressions of extreme piety, wanton avarice, and excessive violence exhibited by the groups that it had stitched together. Moreover, the mass of crusaders had virtually no success over two centuries in recovering the holy lands (Matthew 2002).

Responding to Contemporary Global Terrorism

Global terrorism poses a complicated security dilemma for those who seek to "detect, disrupt, defeat, and deny" it. The inability to anticipate the precise objective of an entrepreneurial terrorist or the specific way in which he or she may use an existing network makes it very difficult to apply a deterrent strategy relative to the network as a whole. The plethora of available alternatives and the objectives that they could serve makes prohibitive the costs of identifying all would-be culprits within a network and demonstrating the resolve necessary to impose penalties on them should they act in nefarious ways. At the same time, if the preferences and vulnerabilities of individual nodes can be identified, then they can be targeted. Although deterring a specific node from taking advantage of a preexisting network

does not reduce the ability of others to do so, it may at least reduce the number of nefarious users. Thus, even though the United States could not deter the September 11 attacks, its swift retaliation can act as a deterrent by persuading others that the costs to terrorists of this type of attack are likely to exceed the gains.

Deterrence strategies are not likely to be effective against the network as a whole, but they may be effective at the microlevel when targeted against individual nodes. Insights from the theory of complex interdependence suggest that even though the network structure decreases the "vulnerability interdependence" of each node or unit by providing it with multiple pathways or alternatives in the event of an attack against the network, the network structure also increases the "sensitivity interdependence" of each node by tying it to actions taken by or against others in the network (Keohane and Nye 1977). This means that even though the network is resilient and invulnerable, individual units are very sensitive to attacks directed against the network.

The concept of "sensitivity interdependence" suggests that members of a network will be sensitive to—that is, incur short-term costs or benefits as a result of—the actions of others or actions taken for or against others in the network. The redundancy links create strategic alternatives that may reduce those costs and, consequently, their vulnerability. But unlike moving from Yahoo to Google, if the cost of switching to new nodes is not negligible or instantaneous, then even short-term costs may be prohibitive to individual units. Thus, disabling a financial center in a terrorist network may impose sufficient short-term costs to incapacitate a particular cell even though, given enough time, it could find alternate sources of financing. This issue is going to affect the weakest members of the network the most in part because, as Walter Enders and Todd Sandler (2005) demonstrate, attacks will be deflected by defense systems and, hence, will always gravitate toward soft targets. As Stuart Kaufman (1996a, 1996b) and Barry Posen (1993) have independently argued, when individual actors feel at risk and cannot rely on the network to protect them—as when ethnic groups experience "emerging anarchy" within a state—their individual vulnerability will increase even if the vulnerability of the state (or network) remains low (see also Roe 1999). If a subgroup is suddenly compelled to provide for its security, it must assess whether any neighboring group is a threat.[4]

This sensitivity interdependence suggests that individual nodes may be deterred and may suffer from security dilemma dynamics if they perceive themselves to be vulnerable even when the network is secure. Thus, the network-wide costs of an attack are not that high, but the vulnerability of any individual in the network is high. Individuals, therefore, may want to introduce defense measures, such as antivirus software on computers. But adding filters adds costs that reduce the attractiveness of the network and can lead to a spiral model situation: virus—antivirus—more sophisticated virus—more sophisticated antivirus—and so on.

In short, the September 11 attack made it clear how vulnerable each node in a network is, and caused an enormous amount of suffering and damage. But no progress was made toward any of the larger goals of al-Qaeda. The attacks placed costs on neutral and sympathetic parties, as did the response to the attacks. Targeted deterrence within Afghanistan and Pakistan cannot disable the network, but it may lead to the eradication of some threatening nodes and hubs and should be pursued when intelligence is reliable. The security dilemma is frustrating, but one should take comfort in the fact that these attacks are somewhat like random acts of violence. They cause fear and mobilize angry responses, but they are utterly bereft of creative or constructive power. They can cause harm but they cannot lead to change in any systematic manner shaped by principles of justice or shared interest.

[4]This theme was also developed by Jack Snyder and Robert Jervis at a Conference on Civil War and the Security Dilemma held at Columbia University in February, 1997. See http://www.ciaonet.org/conf/iwp01/

On our part, we cannot deter "global terrorism" per se, because it is not a unified agent but rather a diffuse network that coalesces and disperses. Nonetheless, we can deter its elements when we are made aware of them. Rhetoric about the war on terrorism and statements that attribute a high level of unity and capacity to al-Qaeda are misleading and run the risk of wasting resources fighting an enemy that does not exist in the form imagined. At this level, the large goals expressed by bin Laden to the media are of less interest than are the tactical linkages he is able to forge.

The Dilemma of Global Terrorism

Networks have given terrorists unprecedented access to resources, delivery systems, targets, and media and have protected them from being easily decimated or even controlled through traditional security strategies. But the networks terrorists attack and abuse are themselves resilient and hard to destroy. Indeed, the network structure terrorists have adopted poses a serious collective action problem for them. To overcome these limitations on contemporary global terrorism, it will be necessary for terrorists to adopt a structure that can mobilize and sustain the sort of constructive political power that could actually achieve broader objectives—such as overthrowing secular rule in the Middle East, installing more religious regimes on the model of Iran, and driving the West out of the Islamic world.

This problem has received considerable attention in the field of political science. For example, in his classic work *Leviathan*, Thomas Hobbes argued that, in the absence of centralized power in a hierarchical organization, particular interests will tend to undermine collective action and degenerate into conflict. Centralization provides order and continuity, but it also introduces a new set of interests. Should al-Qaeda move along this path toward a hierarchically organized form of global terrorism, there is good reason to believe that its priorities will shift toward ensuring its survival, maintenance, and well-being as an organization. Robert Michels (1999) called this the "iron law of oligarchy" by which leaders begin to value the organization in ways that may lead them to reject behavior that could put that organization at risk.

The example of the Front de Liberation du Quebec (FLQ) illustrates this point well. In the late 1960s and early 1970s, it engaged in minor symbolic acts of terrorism, such as bombing targets in places that officials were notified in advance to clear. These acts escalated to two kidnappings and murders. The government of Canada, led by Prime Minister Pierre Trudeau, declared martial law, and the FLQ found itself sharply circumscribed in what it could achieve as well as largely unsupported by the public, including those who supported the idea of Quebec independence. The only way to advance its political agenda was to develop an organization that could tap into the grievances in Quebec and the desire for statehood without inviting such harsh reprisals. The Parti Quebecois was formed to do precisely this. And, consistent with Michel's "iron law of oligarchy," it immediately distanced itself from terrorism and the FLQ, although there were clearly some personal ties between the two groups. The Parti Quebecois eschewed all violence, competed in provincial elections, and took control of Quebec's provincial government in 1976. It held a referendum on independence, which was defeated. Upon the defeat, the Parti Quebecois declared that, although it would retain its original ambition of becoming a sovereign state, it would now focus its energy on the routine affairs of government—such as economic performance, health care, education, and law and order. This split the party as some felt that it had traded its very purpose for political legitimacy and success.

A very similar process is evident among environmental nongovernmental organizations such as Earth First!, which has been described as a terrorist organization engaged in acts such as tree spiking. Earth First! formed in 1979 in part because of

the sentiment of some environmental activists that Greenpeace, established in 1971, was not aggressive enough in its direct action campaigns. When Earth First's director, Dave Foreman, was compelled to negotiate with the Department of Justice and agreed to leave Earth First!, abandoning its tactics and moving to Washington apparently in the expectation of achieving larger successes for conservation, some of his followers regarded him as betraying the cause. In short, through this strategy of mainstreaming, mobilization goes up, along with the potential for generating and exercising more constructive forms of power, but the focus shifts to a common agenda and the appeal of violence declines quickly.

These changes have important implications for security dilemma dynamics and deterrence. If, optimistically, such a change occurs and generates a socializing impact on terrorist networks, then the organizations themselves face security dilemma dynamics. As the new organization acquires a desire to protect itself and develop legitimacy, it must distance itself from its more radical elements—as the Parti Quebecois and Earth First! did—in order to avoid a backlash against the organization as a result of their more violent or disruptive activities. If, pessimistically, the organization becomes more radicalized (as the Nazi party did), then the security dilemma acts very much as it would for states or other highly organized actors.

Deterrence is much easier under the former scenario because the interests, objectives, and vulnerabilities of the terrorist network become much more centralized and clearly identified. Pessimistically, if increased levels of organization make the terrorists more virulent, it also makes it much easier to identify unacceptable costs, communicate resolve, and focus deterrent strategies against the organization as a whole. Optimistically, if the organizing process has a socializing and moderating impact, then it will generate additional vulnerabilities associated with the quest for legitimization and political participation. The transformation can also create a legitimate political actor representing grievances worthy of political debate. Should al-Qaeda move in this direction, it would probably change its name and key personnel, and the world would consider negotiating with it.

Conclusions and Policy Recommendations

Recognizing the dynamic nature of network-based terrorism has important political and theoretical implications. First, we believe that terrorists can and will exploit existing networks easily, a threat that is hard to contain or defeat through traditional security strategies. Furthermore, the political, economic, social, and technological networks that are interwoven throughout our society make the United States and other countries more or less undefeatable by terrorism. Terrorism poses a threat to the personal security of individual US citizens, but its current formulations do not threaten our homeland security. Facing al-Qaeda is dispiriting and frustrating, but it is not the same as facing the Soviet Union or a potentially aggressive China, opponents who could, if provoked coordinate extensive offensive and defensive actions over great distances and time periods.[5] This last statement has critical policy implications because it suggests that US security policy should be focused more explicitly on protecting individuals at high risk and neutralizing specific terrorists rather than on the general threat of terrorism pitched as the leading national security issue.

Second, the collective action problem of networks suggests that to move beyond the pursuit of opportunistic actions, terrorists must evolve into more cohesive and hierarchical organizations. As a first step, terrorists may create nodes or hubs through which they can disseminate information and other resources. These types

[5]One could, however, imagine weapons of mass destruction migrating into a network-based structure as a result of the redistribution of expertise after the Cold War, an occurrence that could pose an enormous global threat and a possibility that argues for devoting considerable attention to the evolving challenge of nuclear proliferation.

of activities can facilitate terrorist activities of otherwise disparate cells, but the resulting coordination is likely to be based on either tactical or fragmented linkage and will be fleeting. Just as support for President Bush declined as the rally around the flag effect following the September 11 attacks dissipated among the US public, support for al-Qaeda is likely to dissipate as the specific costs and benefits of its actions and the government's response become apparent to individual terrorists and terrorist cells. Thus, even though al-Qaeda may be able to facilitate continued attacks against US forces in Iraq or help widespread groups carry out their particular objectives, its ability to generate a broadly coordinated effort, like a joint attack against specified Western targets around the globe, or achieve broader common goals, like getting the West out of Saudi Arabia, is virtually nil. Al-Qaeda may be able to facilitate small victories by individual terrorist cells, but it cannot win in the "global war on terrorism."

In contrast, if network-based terrorist groups are successful in creating a more hierarchical structure, the increased organization and higher levels of coordination will likely generate new preferences and new vulnerabilities that make these hierarchical terrorist networks easier to target and neutralize. The "iron law of oligarchy" mentioned earlier highlights the tendency for increased organizational structure to be matched by a shift in preferences away from ideological objectives toward the preservation of the organization. Optimistically, this may have a pacifying effect on terrorists who seek to become legitimate political actors like the PLO or the Parti Quebecois. Pessimistically, if, instead, the terrorist organization becomes a more unified and virulent adversary, like the Nazi party, the increased organizational structure should increase its vulnerability by making it easier to identify, attack, and neutralize.

Gilpin (1981) suggested that the diffusion of technology helped to explain why hegemons are likely to decline relative to their rivals. Discontented individuals, groups, and other nefarious nonstate actors have readily exploited modern networks to challenge the dominant states of the system. These states are under siege by adversaries who exploit their economic, political, and technological networks to nefarious ends and appear to be invulnerable to their defenses. Network analysis suggests, however, that collective action problems are likely to inhibit the ability of terrorists and other network-based threats to achieve long-term goals or to engage in complex coordinated activities. Ultimately, the superior coordinating capacities of states give them a strategic advantage over those who would challenge them.

References

BARABASI, ALBERT-LASZLO. (2003) *Linked*. New York: Plume.

BUCHANAN, MARK. (2002) *Nexus: Small Worlds and the Groundbreaking Science of Networks*. New York: W.W. Norton.

BYMAN, DANIEL L. (2003) Al-Qaeda as an Adversary: Do We Understand Our Enemy? *World Politics* 56:139–163.

CHOMSKY, NOAM. (2002) *9-11*. New York: Metropolitan Books.

DEUDNEY, DANIEL, AND G. JOHN IKENBERRY. (1991/1992) The International Sources of Soviet Change. *International Security* 16(Winter):74–118.

DEUTSCH, KARL. (1966) *Nationalism and Social Communication: An Inquiry into the Foundations of Nationality*. New York: Wiley.

DOYLE, MICHAEL J. (1983a) Kant, Liberal Legacies, and Foreign Affairs, Part 1. *Philosophy and Public Affairs* 12:205–235.

DOYLE, MICHAEL J. (1983b) Kant, Liberal Legacies, and Foreign Affairs, Part 2. *Philosophy and Public Affairs* 12:323–353.

ENDERS, WALTER, AND TODD SANDLER. (2005) After 9/11: Is It All Different Now? *Journal of Conflict Resolution* 24:259–277.

FRIEDMAN, THOMAS L. (2005) *The World Is Flat: A Brief History of the Twenty-First Century*. New York: Farrar, Straus, and Giroux.

GILPIN, ROBERT. (1981) *War and Change in World Politics*. Princeton: Princeton University Press.

HAAS, ERNST. (1980) Why Collaborate: Issue Linkage and International Regimes. *World Politics* 32:357–405.

INTERNET HISTORY. (2005) Available at http://www.freesoft.org/CIE/Topics/57.htm

KAUFMAN, STUART. (1996a) An International Theory of Inter-Ethnic War. *Review of International Studies* 22:149–172.

KAUFMAN, STUART. (1996b) Spiraling to Ethnic War: Elites, Masses, and Moscow in Moldova's Civil Society. *International Security* 21(2):108–138.

KEEN, MAURICE. (1967) *A History of Medieval Europe*. London: Routledge & Kegan Paul.

KEOHANE, ROBERT O., AND JOSEPH NYE. (1977) *Power and Interdependence: World Politics in Transition*. Boston: Little, Brown.

LILLEY, PETER. (2003) *Dirty Dealing: The Untold Truth about Global Money Laundering, International Crime, and Terrorism*. New York: Kogan Page.

MATLIS, JAN. (2002) Scale-Free Networks. *ComputerWorld*, November 4.

MATTHEW, RICHARD. (2002) *Dichotomy of Power: Nation Versus State in World Politics*. Lanham: Lexington Books.

MATTHEW, RICHARD, AND GEORGE SHAMBAUGH. (1998) Sex, Drugs and Heavy Metal: Transnational Threats and National Vulnerabilities. *Security Dialogue* 29(2):163–176.

MATTHEW, RICHARD, AND GEORGE SHAMBAUGH. (2005) Terrorism and International Relations Theory: Enduring Concepts, New Ideas, and the Interpretation of Transnational Threats. Paper presented at the annual meeting of the International Studies Association, Honolulu, March.

MICHELS, ROBERT. (1999) *Political Parties: A Sociological Study of the Oligarchical Traditions in Modern Democracies*. Translated by Eden and Ceder Paul. New Brunswick: Transaction Publishers.

POSEN, BARRY. (1993) Societal Security, State Security, and Internationalism. In *Identity, Migration, and the New Security Agenda in Europe*, edited by Ole Weaver, Barry Buzan, Morten Kelstrup, and Pierre Lemaitre. London: Pinter Press.

RIKER, WILLIAM. (1982) *Liberalism against Populism*. San Francisco: Freeman.

RISSE-KAPPEN, THOMAS. ED. (1995) *Bringing Transnational Relations Back In: Non-State Actors, Domestic Structures, and International Institutions*. Cambridge: Cambridge University Press.

ROE, PAUL. (1999) The Interstate Security Dilemma: Ethnic Conflict as a "Tragedy"? *Journal of Peace Research* 36:188–192.

ROSENAU, JAMES N. (1990) *Turbulence in World Politics: A Theory of Change and Continuity*. Princeton: Princeton University Press.

ROSENAU, JAMES N., AND ERNST-OTTO CZEMPIEL. (1992) *Governance without Government: Order and Change in World Politics*. Cambridge: Cambridge University Press.

SAGEMAN, MARK. (2004) *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press.

SCHAFFER, CLIFFORD. (2005) Basic Facts on the War on Drugs. Available at http://www.druglibrary.org/schaffer/library/basicfax.htm

SHAMBAUGH, GEORGE, AND WILLIAM JOSIGER. (2004) Public Prudence, the Policy Salience of Terrorism and Presidential Approval Following Terrorist Incidents. Paper presented at the annual joint conference of the International Security and Arms Control Section of the American Political Science Association, the International Security Studies Section of the International Studies Association, and Women in International Security, Washington, October.

SLAUGHTER, ANNE-MARIE. (2004) *A New World Order*. Princeton: Princeton University Press.

SMALL, MELVIN, AND J.DAVID SINGER. (1976) The War-Proneness of Democratic Regimes. *Jerusalem Journal of International Relations* 1:50–69.

WATTS, DUNCAN J. (2003) *Six Degrees: The Science of a Connected Age*. New York: W.W. Norton.

ZACHER, MARK W., AND RICHARD A. MATTHEW. (1995) Liberal International Theory: Common Threads, Divergent Strands. In *Controversies in International Relations Theory: Realism and the Neo-Liberal Challenge*, edited by Charles W. Kegley, Jr. New York: St. Martin's Press.

ZACHER, MARK W., AND BRENT A. SUTTON. (1996) *Governing Global Networks: International Regimes for Transportation and Communications*. Cambridge: Cambridge University Press.