2008

A Tale of Two Networks: Terrorism, Transnational Law, and Network Theory

Christopher J. Borgen
St. John's University School of Law

A TALE OF TWO NETWORKS: TERRORISM, TRANSNATIONAL LAW, AND NETWORK THEORY

Christopher J. Borgen*

I. INTRODUCTION

Talk of networks and "network theory" has become almost ubiquitous in the field of counterterrorism. Terrorist organizations are networks. Terrorists have been empowered by the Internet, ethnic diasporas, and cellphones—networks all.[1] Many of the putative targets of terrorists—electrical grids, oil pipelines, and transportation systems, to name a few—are themselves networks. And, perhaps less often mentioned, terrorists are increasingly hampered by national and international laws that foster cooperation and coordination among states—a network of laws.

From "smart mobs" to "netwars," from narcotrafficking to the Internet, network theory has provided insights into decentralized social organizations and their coordinated action. Both sides in the "War on Terror" are networked and are themselves networks. This essay is the tale of two networks: what happens when the network of terror and the network of law collide.

Part II will briefly introduce the network theory and use it to describe the mechanisms of al Qaeda's terror network. Part III will turn to how network theory has affected counterterrorism strategy, particularly emphasizing intelligence analysis and the use of legal regimes to

---

* Associate Professor of Law, St. John's University School of Law. This essay benefited from the comments of participants of the Counter-Terrorism Symposium (April 20, 2007) sponsored by the Oklahoma City University School of Law and the Memorial Institute for the Prevention of Terrorism. I am especially indebted to conference organizer Professor Marc Blitz. I am also grateful to the editors and staff of *Oklahoma City University Law Review* for their fine editorial work. Any mistakes are solely my own.

1. JOHN ROBB, BRAVE NEW WAR: THE NEXT STAGE OF TERRORISM AND THE END OF GLOBALIZATION 11 (2007).

leverage strengths. Part IV will return to network theory more broadly and ask how the network of law can be adjusted to be more effective in disrupting the terrorists' network. This essay concludes that, despite the hostility of the Bush Administration to international law and that Administrations' efforts to circumvent existing domestic legal regimes, the network of domestic and international laws, including the protection of civil liberties, is a crucial component to a successful counterterrorism strategy.

II. THE NETWORK OF TERROR AND FOURTH GENERATION WARFARE

A. Constructing Terror Networks

Since September 11, al Qaeda—a relative newcomer as far as terrorist groups are concerned—has become the center of attention in the global conflict against terrorist organizations. For the American public, it has become symbolic of the people and groups who would strike at the United States. But for other would-be terrorists, al Qaeda's successes on September 11 have provided a lesson about organization, strategy, and tactics.[2] Al Qaeda provides us with an example of how violent organizations such as terrorist groups, separatist movements, and gangs are evolving and adapting.

Prior to September 11, al Qaeda was organized much like other older terrorist groups, using a "hub-and-spokes" design with Osama bin Laden and his close advisors at the center, and ties going out to operational cells at the end of the spokes.[3] However, since the War in Afghanistan disrupted the hub-and-spokes architecture, al Qaeda has reorganized itself by using cells made up of individuals who all know each other (known in network theory as "all-channel connectivity"), and each cell may know one or two people in one or two other cells.[4] Thus, there are

2. *Id.* at 139.

3. *See* David Ronfeldt, *Al-Qaeda and its Affiliates: A Global Tribe Waging Segmental Warfare, in* INFORMATION STRATEGY AND WARFARE: A GUIDE TO THEORY AND PRACTICE 35, 35 (John Arquilla & Douglas A. Borer eds., 2007), *available at* http://www.rand.org/pubs/reprints/2008/RAND_RP1371.pdf (noting that, due to outside pressure, al Qaeda may have for a time shifted from its original hub-and-spokes design to a scattered cluster design, but as of 2007 it may have evolved into a multi-hub network).

4. *See* John Arquilla & David Ronfeldt, *The Advent of Netwar (Revisited), in* NETWORKS AND NETWARS: THE FUTURE OF TERROR, CRIME AND MILITANCY 9 (John Arquilla & David Ronfeldt eds., 2001) (stating al Qaeda now has "a more distributed design characterized by dispersed small zones of all-channel connectivity linked loosely

areas of high connectivity, each of which is linked to one or two other such areas of high connectivity. This is sometimes referred to as a "scattered-cluster design."[5]

Such an architecture frustrates traditional methods of law enforcement and military strategy. For example, when law enforcement was arrayed against traditionally hierarchical organizations such as Mafia crime families, the police usually could identify the leadership of the criminal enterprise. There, the problem usually turned on connecting a specific group of leaders to certain crimes. However, but for certain well-known figures such as Osama bin Laden and Ayman al Zawahiri, al Qaeda-type networks are usually run by "relative unknowns."[6] Thus, what we often call "al Qaeda" is not really one organization with one command structure; it is a swarm of small organizations that cooperate when it is advantageous to do so.[7] Similarly, the insurgency in Iraq has been described as being comprised of "seventy-five to one hundred small, diverse, and autonomous groups."[8]

Moreover, these organizations learn from each other. Innovations that work are replicated, while those that fail are either set aside or tinkered with until they are useful. It is a "bazaar of violence," as exemplified in Iraq, where information and resources are bought, sold, and shared, but the bazaar is going global.[9] Tactics that are being tested in the streets of Baghdad are being imported to operations in Europe and elsewhere.[10] Groups are cognizant of each others' innovations. One can find American neo-Nazis opining on the lessons al Qaeda has learned about network-based operations.[11]

Thus, while al Qaeda itself may not be as dangerous as it once was, the other organizations that it inspires have become more dangerous. Even if, or when, al Qaeda is destroyed, this new mode of conflict will

---

by chains").

5. *Id.*

6. ROBB, *supra* note 1, at 139.

7. *See id.* at 4.

8. *Id.*

9. *Id.* at 15-16.

10. John Sullivan, *Policing Networked Diasporas*, SMALL WARS J., July 9, 2007, http://smallwarsjournal.com/blog/2007/07/print/policing-networked-diasporas/.

11. William Crotty, *International Terrorism: Causes and Consequences for a Democratic Society*, *in* DEMOCRATIC DEVELOPMENT AND POLITICAL TERRORISM: THE GLOBAL PERSPECTIVE 523, 524 (William Crotty ed., 2005) (quoting Jessica Stern describing a discussion with a neo-Nazi).

remain with us.[12] And so, it is important to not only focus on al Qaeda as an organization, but also on what al Qaeda heralds about armed conflict.

B. Network as Strategy: Fourth Generation Warfare

There is little doubt that the nature of armed conflict is changing in profound ways. Some call the period we are entering the "fourth generation" of warfare ("4GW"), a term that was defined in a seminal article in the *Marine Corps Gazette* in 1989,[13] and was recently reconsidered by John Robb in his book Brave New War.[14] By this nomenclature, the mass warfare exemplified by the Napoleonic Wars is considered the first generation.[15] The Industrial Revolution spurred the second generation, which was typified by the harnessing of entire economies to produce war materiel and which reached its peak in the deployment of new weapons systems in World War I.[16] The third generation was a reaction to the second, and was based on new strategies of maneuver warfare.[17] This generation was fully realized in World War II with the use of the blitzkrieg.[18] The Cold War was typified by fears of Russian tanks storming through the Fulda Gap. The laws of armed conflict shifted and adapted in each of these instances to respond to the new ways that war was fought. But in each case, the change in law was an attempt to curb the worst proclivities, not enable them.

The rise of nuclear weapons made it difficult for states to fight each other without running the risk of mutual annihilation.[19] This, in turn, caused states to turn to low-intensity conflict and proxy wars.[20] Such "small wars," combined with the advent of cheap and powerful computers and global communication, has heralded 4GW. This is an era of "super-empowered" individuals who are able to act in a manner —for

12. *See* Lisa J. Campbell, *Applying Order-of-Battle to Al Qaeda Operations*, *in* NETWORKS, TERRORISM AND GLOBAL INSURGENCY 129, 132 (Robert J. Bunker ed., 2005).

13. William S. Lind et al., *The Changing Face of War: Into the Fourth Generation*, MARINE CORPS GAZETTE, Oct. 1989, at 22, 22-26, *available at* http://www.d-n-i.net/fcs/4th_gen_war_gazette.htm.

14. ROBB, *supra* note 1.

15. Lind et al., *supra* note 13.

16. *Id.*

17. *Id.*

18. *Id.*

19. MARTIN VAN CREVELD, THE TRANSFORMATION OF WAR 194 (1991).

20. *Id.*

good or evil—that formerly had been the preserve of states.[21] Future wars by groups "we today call terrorists, guerillas, bandits, and robbers" will be organized along "charismatic lines" of individual leadership as opposed to the formal bureaucracy of the modern state.[22]

The same forces of globalization that have transformed how governments and businesses operate are also transforming violent criminal groups. The Information Revolution has also revolutionized the organization and the use of force. On one level, the Internet simply makes it easier to find information, equipment, and recruits.[23] The Internet also allows violence to be commanded via remote control; for example, there are jihadi websites from which viewers can watch (via webcam) and detonate with the click of a button actual bombs in the streets of Baghdad.[24] Besides the connectivity of the World Wide Web, ever greater levels of computing power have been commodified: a modified Playstation 2 game console has the ability to control a missile to target.[25] Home videogames have gone from Missile Command to commanding missiles. Advances in other areas of technology could be similarly exploited by terrorists; for example, advanced fermenting equipment can be used to manufacture biological weapons.[26] These are but two examples of the "decentralization of the tools of warfare."[27]

Advances in communications have also facilitated an evolution in how terrorists organize themselves. By and large, terrorist organizations are no longer top-down hierarchies.[28] They are decentralized networks, a web of relationships linking "nodes" (which may be individuals, cells, organizations, states, and other networks).[29] Each "node" can serve different functions (such as fund raising, organizing, or executing a plan) for different operations. Decentralization means that nodes do not generally wait for orders but are entrepreneurial in finding targets of opportunity and organizing the resources needed for a particular

21. ROBB, *supra* note 1, at 27, 30.

22. CREVELD, *supra* note 19, at 197.

23. JESSICA STERN, THE ULTIMATE TERRORISTS 10 (1999).

24. *See, e.g.*, *'Wired For War' Explores Robots On The Battlefield*, NPR, Jan. 22, 2009, http://www.npr.org/templates/story/story.php?storyId=99663723.

25. ROBB, *supra* note 1, at 9.

26. STERN, *supra* note 23, at 10.

27. ROBB, *supra* note 1, at 74.

28. *See, e.g.*, CHARLES PEÑA, WINNING THE UN-WAR: A NEW STRATEGY FOR THE WAR ON TERRORISM 107 (2006).

29. *See id.* (describing the nodes of al Qaeda's network as being individual operatives, terrorist cells, and states).

operation.

Moreover, as exemplified in Iraq, different nodes from within a terrorist network learn from each others' experiences, and different terrorist networks learn from each other. Such "open-source warfare . . . starts with a plausible promise," such as "we will hamper the U.S. invaders," and then shares "tactics, weapons, strategies, target selection, planning methods, and team dynamics," which are all open to community improvement.[30] Improvised Explosive Devices, better known as "IEDs," are an example of development via such open-source warfare.[31]

These various developments in organized violence—the ability to trigger violence at a distance, the commodification of computing power, the expansion of communication capabilities, the shift from hierarchical to networked organization, and the sharing and improvement of tactics and technology, are combined with an older strategy of irregular warfare: "to waste the strength of the strong—to bleed the target state dry morally and economically."[32] Targeting the state economically is linked to striking at the legitimacy of the state.[33] As the energy, security, and communications systems of a state are repeatedly disrupted, the bonds of social cohesion fray and break. Ayman al Zawahiri has said that al Qaeda will "'provoke and bait' the United States into 'bleeding wars' on Muslim lands," ultimately causing the people of the United States to lose the will to fight and cause the United States to pull out of Muslim countries.[34] Put another way, "when the strong fight the weak, they become weak."[35] Moreover, as Martin van Creveld argues, "he who fights terrorists for any period of time is likely to become one himself."[36]

C. Describing Terrorist Networks

With these general observations about 4GW as background, the focus can turn to describing the parts of a terrorist network. The three

30. ROBB, *supra* note 1, at 116.
31. *Id.* at 135.
32. *Id.* at 27.
33. *Id.* at 5; *see also* Robert J. Bunker, *Introduction and Overview: Why Response Networks?*, *in* NETWORKS, TERRORISM AND GLOBAL INSURGENCY, *supra* note 12, at 1, 2.
34. Philip H. Gordon, *Can the War on Terror Be Won?*, 86 FOREIGN AFF., Nov./Dec. 2007, at 53, 57.
35. ROBB, *supra* note 1, at 28.
36. *Id.* at 201.

main types of actors are states, transnational groups or networks, and individuals. In addition, each of the types of actors can play one or more of three basic roles: leader, supporter, and footsoldier.

i. Actors

Individuals. Perhaps the most common mental image one has of a terrorist network is of a loose organization made up of individuals. What is important to emphasize in 4GW, though, is that because terrorism does not necessarily require large amounts of funding to have a large impact, individuals are more powerful than ever.[37] At times, individuals can act in a manner that had previously been the preserve of states. Such "superempowered individuals," to use Thomas Friedman's term, are able to use new technologies to prosecute old hatreds or ambitions.[38]

States. Although many policymakers speak of "state-sponsored" terrorism as if it is a single thing, there is actually a continuum of different types of state sponsorship ranging from active control to a mere coincidence of interests between state and terrorist.[39] Some states may act as sponsors of specific acts of terrorism through financial assistance, arms transfers, the provision of intelligence, etc.[40] Iran's relationship with Hezbollah is one such example. States can also act as a node in a terrorist network by providing safe harbor or a hideout for terrorists.[41] Afghanistan's relationship with al Qaeda prior to September 11 is the most commonly cited example. Moreover, states can play an inadvertent role in terrorist networks when failed states act as recruiting grounds or sites for organization. Angola, Liberia, Sierra Leone, Sudan, and the Democratic Republic of the Congo are among failed states that could play such roles for various networks.[42]

37. *See* THOMAS L. FRIEDMAN, THE LEXUS AND THE OLIVE TREE 13 (1999) (regarding the increase in power of individuals).

38. *Id.*

39. Neal A. Pollard, *Globalization's Bastards: Illegitimate Non-State Actors in International Law*, *in* NETWORKS, TERRORISM AND GLOBAL INSURGENCY, *supra* note 12, at 40, 62-63.

40. *See* OFFICE OF THE COORDINATOR FOR COUNTERTERRORISM, U.S. DEP'T OF STATE, COUNTRY REPORTS ON TERRORISM 2007 171 (2008), http://www.state.gov/documents/organization/105904.pdf.

41. *See, e.g., id.* ("Iran and Syria routinely provided safe haven . . . to terrorist organizations.").

42. Robert I. Rotberg, *The New Nature of Nation-State Failure*, *in* THE BATTLE FOR HEARTS AND MINDS: USING SOFT POWER TO UNDERMINE TERRORIST NETWORKS 79, 86 (Alexander T.J. Lennon ed., 2003).

Transnational groups or networks. One insight into networks is that one network can actually act as a node in another network.[43] Regarding jihadist terrorist networks, diaspora communities in western states can be useful in providing a source for recruitment as well as a comfortable base of operations for extremist cells.[44]

ii. Roles

The various actors can play different roles in the pursuit of a terrorist enterprise. Thus, a single actor can play multiple roles, or only one.

Leaders. Although terrorist networks find willing recruits among the poor and marginalized, many terrorists, especially among the leadership, are well-educated and socio-economically advantaged.[45] For example, Omar Sheikh, believed to have masterminded the killing of Danny Pearl, has a personal wealth of $800,000.[46] Mohammad Atta, the operational commander of the September 11 attacks, was from an upper-middle-class family.

Using al Qaeda's structure as a model, terrorist networks can be described as having three levels of leadership: strategic planners, regional leaders, and tactical commanders.[47]

Supporters. Supporters provide logistical and financial support to the leaders and footsoldiers who actually undertake acts of violence and disruption. They can be individual "money men" like Bin Laden, states such as Iran, or charitable organizations. Charity to the poor is one of the central pillars of Islam and is known as "zakat."[48] Unfortunately, zakat can be exploited by terrorist networks that divert funds given to a myriad of legitimate charity groups to terrorist operations.[49] Moreover, the network of informal financial transfer sites, or hawallas, throughout the Muslim world and diaspora provide a means to move large sums of money via small, largely undocumented transfers.[50]

---

43. *See* PEÑA, *supra* note 28, at 108 (describing al Qaeda as a "network of networks").

44. Sullivan, *supra* note 10.

45. Irm Haleem, *Pakistan, Afghanistan, and Central Asia: Recruiting Grounds for Terrorism?*, *in* DEMOCRATIC DEVELOPMENT AND POLITICAL TERRORISM: THE GLOBAL PERSPECTIVE, *supra* note 11, at 121, 129.

46. *Id.*

47. MICHAEL A. SHEEHAN, CRUSH THE CELL: HOW TO DEFEAT TERRORISM WITHOUT TERRORIZING OURSELVES 54 (2008).

48. Haleem, *supra* note 45, at 133.

49. *Id.*

50. *See* Rachana Pathak, Note, *The Obstacles to Regulating the Hawala: A Cultural*

Footsoldiers. The tip of terrorism's spear is the footsoldier, the person who carries out an attack, sets a bomb, and so on. Sometimes, footsoldiers are not closely tied to the leaders or supporters.[51] Then-Director of Central Intelligence George Tenet, in testimony before the Senate Foreign Relations Committee, stated that bin Laden's organization and other terror groups are "plac[ing] emphasis on developing surrogates to carry out attacks."[52] Once again using al Qaeda as an example, it

> seems to have relatively few senior leaders, a greater number of highly trained lieutenants, anywhere from 50,000 to 70,000 trained foot soldiers from its camps in Sudan and Afghanistan, and an indeterminate (but increasing) number of relatively untrained volunteers like Richard Reed, Jose Padillo [sic], and an unknown number of recruits in Iraq.[53]

Counterterrorism strategy can be aimed at one or more of these various actors or the roles that they play. However, experience has shown that leadership is a key asset. Network theory posits that leaders that are gateways for different parts of the network to access each other (for example, the financial backers who supply money and the operatives who spend money) are particularly important nodes in a network. Thus, as one expert explained, "while a decentralized network is more robust than a centralized one, it can still be destroyed (or severely degraded) if enough of the individual leadership nodes are eliminated such that cells of the organization are not effectively connected."[54] Besides key connections, some nodes possess skill sets that are difficult for terrorists to replace. As Michael Sheehan, the former Deputy Commissioner for Counterterrorism of the New York Police Department, explains, "[r]adical hotheads are easy to find, and plots to attack the United States are even more plentiful. But it takes a special person—with the right

---

Norm or a Terrorist Hotbed?, 27 FORDHAM INT'L L.J. 2007, 2009-10, 2018, 2026-27 (2004).

51. *See, e.g.*, ROBB, *supra* note 1, at 137.

52. *Current and Projected National Security Threats to the United States: Hearing Before the S. Select Comm. on Intelligence*, 107th Cong. 4 (2001) (prepared statement of George J. Tenet, Director, Central Intelligence Agency), *available at* https://www.cia.gov/news-information/cia-the-war-on-terrorism/pub_statements_terrorism.html.

53. David P. Auerswald, *Deterring Nonstate WMD Attacks*, 121 POL. SCI. Q. 543, 550 (2006).

54. PEÑA, *supra* note 28, at 102.

measure of ideological fervor, discipline, and leadership ability—to organize a small group to assemble a bomb and conduct an attack."[55] In short, "[r]adical dreamers . . . are a dime a dozen in al Qaeda. A tactical leader such as Atta is their single most important asset."[56]

D. Implications for U.S. Policy

This description of the structure of al Qaeda, along with the insights of network theory, leads to certain implications for U.S. counterterrorism policy. "[P]rior to 9/11, the response to [terrorist] attacks was basically defensive. The U.S. government posed the question 'How can we keep bombers away from our barracks and embassies?' instead of 'How can we crush the terrorists' capability to organize these attacks?'"[57] In short, "good defenses do help protect targets, but if you don't crush the cell, the terrorists will find another target."[58] Towards this goal, we particularly want to deplete al Qaeda and similar terrorist networks of their tactical commanders.

One of the core ideas in this essay is that "a strategic principle for the network age [is that] the advisable way to out-compete is to out-cooperate."[59] Absent some level of cooperation, national bureaucracies are unlikely to be effective against transnational terrorist networks.[60] This is true regarding both military power and law enforcement.

This leads to various implications for U.S. foreign policy. First of all, a simple military assault alone will not be enough to destroy a decentralized network. Moreover, the threat of military force is unlikely to prevent future terrorist attacks.[61] David Auerswald describes the two types of deterrence policy, which are deterrence by denial and deterrence by punishment. "[D]eterrence by denial uses the *threat* of defeat to prevent the attack before it occurs. . . . Deterrence by punishment is a difficult but possible strategy against nonstate actors. It requires

55. SHEEHAN, *supra* note 47, at 48.
56. *Id.* at 49.
57. *Id.* at 18.
58. *Id.* at 50.
59. Arquilla & Ronfeldt, *supra* note 4, at 14.
60. *Id.* at 14-15.
61. *See* SHEEHAN, *supra* note 47, at 4; *see also* Ronald D. Lee & Paul M. Schwartz, *Beyond the "War" on Terrorism: Towards the New Intelligence Network*, 103 MICH. L. REV. 1446, 1448 (book review) (paraphrasing Phillip Heymann's observation that "[t]he United States . . . faces a series of different enemies, who are not likely to be eliminated or even diminished by deployment of traditional military forces").

convincing signals that we could identify *whom* to retaliate against."[62] But modern terrorist networks are mobile, with little permanent infrastructure. While some nodes may actually be states, such as Afghanistan when it provided a safe-haven, the invasion of a particular state may force the network to reorganize like a flock of birds changing direction; but it is unlikely to destroy the whole network.

While military force is part of an effective counterterrorism strategy, it is not the key to such a strategy. As one commentator put it, "[i]f [our leaders] fall prey to the illusion that this is World War III—and that it can be won like a traditional war—they risk perpetuating the conflict."[63] More often than military deployments, combating transnational terror networks will require complex intelligence and law enforcement operations. Effectively cracking down on al Qaeda requires targeting domestic terrorism in various states to make it difficult for al Qaeda to find bases of support.[64] The goal is to collapse the network by striking at crucial nodes and linkages. Random arrests are ineffective as "[a] significant fraction of nodes [in a highly connected network] can be randomly removed without much impact on [the network's] integrity."[65] As Michael Sheehan explains, "[u]ndercover agents, informant networks, and phone and e-mail intercepts are the most effective weapons we have."[66] And they will need to be used to find the operational leaders and the people who are the communication hubs from one cell to another.[67]

Thus, governments are fighting the network of terrorism by building their own networks, and focusing on collapsing terrorist networks.[68] Even in the case of military force, coordination and cooperation amongst allies is key. U.S. special operators are "most successful when they operate in partnership with local forces."[69]

Network theory has not only revolutionized terrorist organizations, but anti-terrorist efforts as well. Two key examples are the revolution in intelligence-analysis techniques and the evolution of transnational legal

62. Auerswald, *supra* note 53, at 547.
63. Gordon, *supra* note 34, at 65.
64. Haleem, *supra* note 45, at 140.
65. MARC SAGEMAN, UNDERSTANDING TERROR NETWORKS 140 (2004).
66. SHEEHAN, *supra* note 47, at 4.
67. SAGEMAN, *supra* note 65, at 141.
68. Arquilla & Ronfeldt, *supra* note 4, at 13.
69. SHEEHAN, *supra* note 47, at 110.

regimes meant to foster cooperation and coordination.[70]

III. THE COUNTERTERRORISM NETWORKS AND THE RULE OF LAW

The intelligence community is not generally known for the widespread sharing of information among different spy agencies. The various intelligence agencies within the U.S. intelligence community have been criticized—especially in the months following September 11—for being too parochial, and for "stovepiping" intelligence vertically in their own agencies without the benefit of insight, critique, or additional intelligence from other agencies.[71] Since September 11, the emphasis has been on turning the intelligence community from a row of stovepipes into an interactive network.

A. The Intelligence Network

As the U.S. intelligence community learned more about how al Qaeda planned and executed attacks, it reconsidered how the intelligence community itself was organized:

> Al Qaeda operatives organized their plots in a hivelike fashion, with collaborators from Afghanistan to London using e-mail, instant messaging and Yahoo groups; rarely did a single mastermind run the show. To disrupt these new plots, some intelligence officials concluded, American agents and analysts would need to cooperate just as fluidly—trading tips quickly among agents and agencies. Following the usual chain of command could be fatal. "To fight a network like Al Qaeda, you need to behave like a network," John Arquilla, the influential professor of defense at the Naval Postgraduate School, [said].[72]

For example, responding to the risks posed by extremist cells within diaspora communities requires counterterrorism policies that "build upon community policing and develop the cultural understanding and

70. For a consideration of cross-border governmental and bureaucratic networks, see generally ANNE-MARIE SLAUGHTER, A NEW WORLD ORDER (2004).

71. *See, e.g.*, NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 408 (2004).

72. Clive Thompson, *Open-Source Spying*, N.Y TIMES MAG., Dec. 3, 2006, http://www.nytimes.com/2006/12/03/magazine/03intelligence.html.

community trust required to recognize the emergence of extremist cells, radicalization, efforts to recruit terrorists, and efforts to exploit criminal enterprises or gangs to further terrorist activities."[73] Network theory shows us that diaspora communities must not be treated as impenetrable enclaves. If they were, then they would become useful nodes for a terror network, promising both anonymity and resources. However, if the state develops policies to incorporate those communities into the broader civil society, they can become part of the network of counterterrorism. Of course, one must keep in mind that, to a certain extent, some of these communities want to be separate in order to maintain and foster particular cultural practices. It is not suggested that that be changed. What is important, though, is to build links with these communities to strengthen the understanding that security is a mutual concern and that cooperating on issues of security in no way affects the communities' ability to practice their culture.

The Bush Administration's use of network theory in the gathering of intelligence—from data mining to widening the use of wiretaps to John Poindexter's "Total Information Awareness"—has been well documented elsewhere. The goal is to generate enough data through travel patterns, call and e-mail intercepts, financial transactions, and so on, for analysis that would show linkages between people and expose hidden networks. Such network mapping may display chimeras—linkages and persons with very close degrees of separation, but who are not actually part of an actual network. The hope is that it will also uncover cells via their behavior and associations.

The civil liberties issues of some of these tactics—such as lowering the bar on wiretapping and data mining the activities of people who have not even been suspected of any crime—are significant. However, these issues have been well analyzed elsewhere and are beyond the scope of this short essay. Rather, this essay will turn to another aspect of network theory in the intelligence community—how networks are changing and how information is distributed and organized among intelligence analysts.

As one commentator explained, "[t]he most valuable spy system is one that can quickly assemble disparate pieces that are already lying around—information gathered by doctors, aid workers, police officers or security guards at corporations."[74] Keeping with the norm of

73. Sullivan, *supra* note 10.
74. Thompson, *supra* note 72.

stovepiping, the computer systems of the various intelligence agencies could share information only within their proper agency, but not across agencies.[75] According to Dale Meyerrose, the former Chief Information Officer for the Director of National Intelligence, "'We've had this 'need to know' culture for years . . . . Well, we need to move to a 'need to share' philosophy.'"[76]

The move from stovepiped analysis to networked analysis is being facilitated by "web 2.0" tools such as collaborative reference works, blogs, and social-networking programs.[77] Such collaborative technologies facilitate rapid accretion and revision of information. To take an example from outside the intelligence community, Wikipedia had a page online about the London transit-system bombings "barely minutes after the attacks."[78] The CIA has started its own collaborative reference, "Intellipedia," which allows analysts with adequate security clearance to log in and contribute to entries on different topics of research and analysis.[79] Intellipedia has grown from 20,000 registered users in July 2007 to over 35,000 users in July 2008.[80] It has approximately 48,000 article pages and has received approximately 1.6 million edits.[81]

The CIA has also been impressed by the use of blogs to disseminate information and foster discussion among people who normally would not be interlocutors. One CIA blog concerning the avian flu was so successful that it became the Administration's most important resource on that issue.[82]

The intelligence community is even getting its own version of the popular social-networking site, Facebook.[83] Called A-Space, it allows communication and networking among analysts in the nation's sixteen intelligence agencies. Michael Wertheimer, the Assistant Deputy

75. *Id.*

76. *Id.*

77. *See, e.g.*, Central Intelligence Agency, Intellipedia Marks Second Anniversary, https://www.cia.gov/news-information/featured-story-archive/intellipedia-marks-second-anniversary.html; *see also* D. Calvin Andrus, *Toward a Complex Adaptive Intelligence Community: The Wiki and the Blog*, 49 STUDS. IN INTELLIGENCE, 2005, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no3/html_files/index.html.

78. Thompson, *supra* note 72.

79. *Id.*

80. Central Intelligence Agency, *supra* note 77.

81. *Id.*

82. Thompson, *supra* note 72.

83. Larry Shaughnessy, *CIA, FBI push 'Facebook for spies'*, CNN.COM, Sept. 5, 2008, http://www.cnn.com/2008/TECH/ptech/09/05/facebook.spies/index.html.

Director of National Intelligence for Analysis, explains that, "'It's a place where not only spies can meet but share data they've never been able to share before .... This is going to give them for the first time a chance to think out loud, think in public amongst their peers, under the protection of an A-Space umbrella.'"[84]

These tools attempt to facilitate the accumulation of information and collaboration in its analysis by breaking down hierarchies and fostering interconnection within a large population of analysts.[85] In this sense, information networks have different practical effects than terror networks. Terror networks compartmentalize in order to make it difficult to "crash" the whole network. By contrast, analytical networks are meant to open access across most or all of the network in order to have as large a group as possible working on any one problem.

However, the fact that these tools build a massively interconnected network is also their greatest weakness. As blogs, wikis, and social-networking sites allow many people to see and edit the same information, should a hacker enter the network, they would have the same wide-ranging access. Even without positing that a hacker may get into the system, such web 2.0 tools risk exposing intelligence sources to analysts who may be willing to sell what they know to other parties (or just do so accidentally).[86] The implementers of these new technologies are aware of these risks, and thus plan to undertake network analysis of their own networks:

> The creators of A-Space do not want it to be used by some future double agent such as Jonathan Pollard or Robert Hanssen to steal America's 21st-century secrets.
>
> "We're building [a] mechanism to alert that behavior. We call that, for lack of a better term, the MasterCard, where someone is using their credit card in a way they've never used it before, and it alerts so that maybe that credit card has been stolen," Wertheimer said. "Same thing here. We're going to actually do patterns on the way people use A-Space."[87]

There are two serious concerns about the move towards networked

84. *Id.*
85. *See id.*
86. Thompson, *supra* note 72.
87. Shaughnessy, *supra* note 83.

information and analysis in the intelligence community. The first is that the culture of the intelligence agencies—and particularly issues of career advancement—are an impediment to some of these innovations. The ability of an analyst—and their prospect for promotion—"'is judged by [their] reports. And that gets in the way of developing knowledge socially, where it becomes very difficult to know who added or revised what.'"[88]

The second concern is that the sharing of information poses its own civil liberties problems. As David Weinberger of Harvard's Berkman Center said, "'I don't want the N.S.A. passing on information about innocent Americans to local cops in San Diego . . . . Those laws exist for good reasons.'"[89]

This brings us to the other main counterterrorism network for our consideration, the network of law.

B. Law's Network

While some who seek new techniques of counterterrorism treat the law and civil liberties as at best irrelevant, or at worst an impediment to an effective national security strategy, the law is actually one of the first places where network theory affected counterterrorism efforts. The network of domestic and international laws aimed at foiling terrorism, and also at protecting civil liberties, has never been more relevant.

The web of domestic and international law, also called transnational law,[90] has three major functions in the struggle against terrorism: (a) it allows for a united front by coordinating anti-terrorism laws and

88. Thompson, *supra* note 72.

89. *Id.*

90. "Transnational law" is a term coined by Phillip Jessup "to include all law which regulates actions or events that transcend national frontiers. Both public and private international law are included, as are other rules which do not wholly fit into such standard categories." PHILLIP C. JESSUP, TRANSNATIONAL LAW 2 (1956). Jessup viewed this law as encompassing relations between states, relations between individuals, and relations between states and individuals; he wanted a term which would identify "the law applicable to the complex interrelated world community which may be described as beginning with the individual and reaching on up to the so-called 'family of nations' or 'society of states.'" *Id.* at 1. Anne-Marie Slaughter has chosen a narrower definition, setting the bounds of transnational law as "all municipal law and a subset of intergovernmental agreements that directly regulate transnational activity between individuals and between individuals and state governments." Anne-Marie Slaughter Burley, *International Law and International Relations Theory: A Dual Agenda*, 87 AM. J. INT'L L. 205, 230 (1993).

regulatory frameworks;[91] (b) it provides laws and litigation regimes that facilitate enforcement of those anti-terrorism laws; and (c) it allows rule-of-law programs in transitional countries to assist social stability and play a part in making it more difficult to recruit new footsoldiers. The first two of these roles are considered in this essay, as they are closely related to each other. The function of rule-of-law programs as a component in counterterrorism is an important question, and one that has been under-explored. However, it is in need of a longer analysis in a separate article and is beyond the scope of the task at hand.

Law's network is, as a first step, a network of treaties providing a (nearly) uniform set of basic characteristics among the main anti-terrorism treaties. The main anti-terrorism conventions include:

1. Convention for the Suppression of Unlawful Seizure of Aircraft (1970);[92]
2. Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (1971);[93]
3. Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons (1973);[94]
4. Convention on the Physical Protection of Nuclear Material (1980);[95]
5. Convention Against the Taking of Hostages (1979);[96]
6. Airports Protocol to the Montreal Convention (1988);[97]
7. Unlawful Acts Against Maritime Navigation (1988);[98]

---

91. For an in-depth discussion of the coordination of national security policy among multiple states, see Amos N. Guiora, *International Cooperation in Homeland Security* (Univ. of Utah S.J. Quinney Coll. of Law Legal Studies Research Paper Series, Research Paper No. 057-08-09, 2008), *available at* http://ssrn.com/abstract=1160067.

92. Convention for the Suppression of Unlawful Seizure of Aircraft, Dec. 16, 1970, 22 U.S.T. 1641, 860 U.N.T.S. 105.

93. Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, Sept. 23, 1971, 24 U.S.T. 564, 974 U.N.T.S. 178.

94. Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, Dec. 14, 1973, 28 U.S.T. 1975, 1035 U.N.T.S. 167.

95. Convention on the Physical Protection of Nuclear Material, Mar. 3, 1980, T.I.A.S. No. 11,080, 1456 U.N.T.S. 124.

96. International Convention Against the Taking of Hostages, Dec. 17, 1979, T.I.A.S. No. 11,081, 1316 U.N.T.S. 205.

97. Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, Feb. 24, 1988, S. TREATY DOC. NO. 100-19, 27 I.L.M. 627.

98. Convention for the Suppression of Unlawful Acts Against Maritime Navigation, Mar. 10, 1988, 1678 U.N.T.S. 221.

8. Unlawful Acts Against Fixed Platforms (1988);[99]
9. Convention for the Suppression of Terrorist Bombing (1998);[100] and
10. Convention for the Suppression of the Financing of Terrorism (1999).[101]

With some minor alterations, these treaties have many common characteristics. In general, each treaty (a) provides for individual criminal liability for the proscribed acts;[102] (b) requires states that are parties to the treaty to make offenses punishable;[103] (c) contains a "prosecute-or-extradite" regime requiring a party to either prosecute any alleged offenders over whom they have jurisdiction concerning the alleged acts or to extradite them to another treaty party that is able to properly establish jurisdiction and prosecute;[104] and (d) establishes a duty on all state parties to assist a prosecuting state should they request help.[105]

Let us consider the most recent of these conventions, which is the International Convention for the Suppression of the Financing of Terrorism.[106] This convention provides the groundwork for increased regulatory coordination among member states to track money transfers. This can be especially useful given the informal transfer methods using hawallas.

It also allows for accounts to be frozen, which picks away at the funding links of a terror network.[107] While some complain that the amount of money blocked in the bank accounts of, for example, the Iranian Revolutionary Guards, is small, "this view fails to put financial warfare in a strategic context. Blocking bank accounts of key groups and individuals puts the spotlight on them and thereby increases the risks to

99. Protocol to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, Mar. 10, 1988, 1678 U.N.T.S. 304.

100. International Convention for the Suppression of Terrorist Bombings, G.A. Res. 52/164, U.N. Doc. A/RES/52/164 (Jan. 9, 1998) [hereinafter Bombings Convention].

101. International Convention for the Suppression of the Financing of Terrorism, G.A. Res. 54/109, U.N. Doc. A/RES/54/109 (Dec. 9, 1999) [hereinafter Financing Convention]. For a more comprehensive list of anti-terrorism treaties, see generally M. CHERIF BASSIOUNI, INTERNATIONAL TERRORISM: MULTILATERAL CONVENTIONS (1937-2001) (2001).

102. *See, e.g.*, Bombings Convention, *supra* note 100, art. 4.

103. *See, e.g.*, *id.*

104. *See, e.g.*, *id.* art. 6.

105. *See, e.g.*, *id.* art. 10.

106. Financing Convention, *supra* note 101.

107. *See id.* art. 8.

any company or government doing business with them."[108] In other words, it degrades the links of the network. "In many respects, conventional economic warfare is like carpet bombing; financial warfare is like [a] precision strike."[109] While globalization facilitates the anonymous funding of terrorists, it also provides means to attack terrorist financing.[110] Such regulatory coordination, when combined with the insights of network theory, can be an effective tool:

> When combined with advances in social network mapping, [financial warfare] can give a highly detailed picture of an elite's communication and financial structure that can be used for targeting. . . .
> Watching how money flows out of a country in a crisis can be an important tip-off to who is in the know and who is at least partially responsible for national decisions.[111]

Besides assisting in government coordination, the network of anti-terrorism laws also pluralizes enforcement.

First, the "prosecute-or-extradite" norm widens the number of states that can prosecute a suspected terrorist for a specific act. Normally, one would expect that prosecution would come from a state that had a direct link to the event, such as having the crime take place within its jurisdiction or having one of its nationals killed. But, under the prosecute-or-extradite norm, a suspected terrorist may be prosecuted by any state party to the relevant treaty. So, for example, any state party to the Hijacking Convention can prosecute a suspected hijacker if the states with the most immediate link choose not (or are unable) to do so. This norm approximates universal jurisdiction, at least among the state parties.

Various domestic laws further pluralize enforcement by allowing private individuals to not only sue suspected terrorists, but also the states that support them.[112] In certain ways, this melding of private action with

108. Paul Bracken, *Financial Warfare*, FOREIGN POL'Y RES. INST., Sept. 2007, http://www.fpri.org/enotes/200709.bracken.financialwarfare.html.

109. *Id.*

110. Thérèse Delpech, *The Imbalance of Terror*, *in* THE BATTLE FOR HEARTS AND MINDS: USING SOFT POWER TO UNDERMINE TERRORIST NETWORKS, *supra* note 42, at 65, 71.

111. Bracken, *supra* note 108.

112. *See* Sean D. Murphy, *State Jurisdiction and Jurisdictional Immunities*, 94 AM. J.

public purpose is similar to the "private attorney general" model of securities enforcement and antitrust regulation. The most common form of suit is a tort suit against an alleged terrorist. Even if the plaintiff wins, it may be largely a moral victory as it may be very difficult to find any assets of the defendant's to attach for satisfaction of the judgment.

This concern may be one of the driving reasons behind legislation that has enabled suits directly against states that are alleged sponsors of terrorism. Normally, states would be immune from the jurisdiction of U.S. courts. However, the Antiterrorism and Effective Death Penalty Act (AEDPA)[113] amended the Foreign Sovereign Immunities Act[114] to permit a claimant who alleged state-supported terrorism to execute a judgment against property owned by that state that is used for a commercial activity within the United States.[115]

While these legal regimes that broaden the scope of who may enforce counterterrorism norms essentially expand the counterterrorism network, some of them do so at a significant price. For example, the attachment of diplomatic assets in a private suit can call into question the ability of the United States to fulfill its obligations under the U.S.-Iran Claims Tribunal, the Vienna Convention on Diplomatic Relations,[116] and the United Nations Headquarters Agreement.[117]

IV. THE NETWORK OF LAW AND THE WAR ON TERROR

Law's network—the panoply of domestic and international law that coordinates regulation, assists law enforcement cooperation, and multilateralizes enforcement—is itself a critical part of the larger counterterrorism network, which is properly understood as a network of networks. Unfortunately, recent pronouncements have treated international law as hampering U.S. policy at best, and as a weapon

---

INT'L L. 117, 117-18 (2000).

113. Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 110 Stat. 1214 (codified as amended in scattered sections of the U.S.C.).

114. Foreign Sovereign Immunities Act of 1976, Pub. L. No. 94-583, 90 Stat. 2891 (codified as amended at 28 U.S.C. §§ 1330, 1602-1611 (2006)).

115. Antiterrorism and Effective Death Penalty Act § 221, 110 Stat. at 1241-43. *See also* Murphy, *supra* note 112, at 117.

116. Vienna Convention on Diplomatic Relations and Optional Protocol on Disputes, Apr. 18, 1961, 23 U.S.T. 3227, 500 U.N.T.S. 95.

117. Murphy, *supra* note 112, at 124. *See also* Agreement Between the United Nations and the United States of America Regarding the Headquarters of the United Nations, U.S.-U.N., June 26, 1947, 61 Stat. 3416.

against U.S. interests at worst. For example, the 2005 National Defense Strategy warned that "Our strength as a nation state will continue to be challenged by those who employ a strategy of the weak using international fora, judicial processes, and terrorism."[118] Some U.S. commentators have started using the term "lawfare" to describe law being used as a weapon, often against America.[119] Rather than viewing the rule of law as an asset, it has suddenly become characterized as a liability.

And yet, in 4GW, the rule of law, both domestic and international, is one of our greatest strengths. Unlike previous generations, guerilla conflicts are, in the words of John Robb, "primarily moral conflicts" where "[t]he key is maintaining moral cohesion."[120] Referring to the arguments of Israeli military strategist Martin van Creveld, Robb explains the dilemma of a democracy embroiled in a 4GW conflict:

> [W]hen the strong are seen beating the weak (knocking down doors, roughing up people of interest, and shooting ragtag guerillas), they are considered to be barbarians. This view, amplified by the media, will eventually eat away at the state's ability to maintain moral cohesion and drastically damage its global image.
>
> As the state's soldiers continue to fight weak foes, they will eventually become as ill disciplined and vicious as the people they are fighting, due to frustration and mirror imaging . . . . Citizens lose their feeling of solidarity with the goals of their government when they perceive it to be acting immorally.[121]

One of the most dangerous effects of terrorism is thus not the destruction of the actual attack or the fear of the general populace, but the withering away of liberal democracies into knee-jerk police states due to their over-reactions. Far from enhancing the security of their citizens, police states do not generate more reliable intelligence, they reduce domestic and international moral cohesion, and they often run

118. DEP'T. OF DEF., NATIONAL DEFENSE STRATEGY OF THE UNITED STATES 9 (2005), *available at* http://www.defenselink.mil/news/Mar2005/d20050318nds2.pdf.

119. Phillip Carter, *Legal Combat: Are Enemies Waging War in Our Courts?*, SLATE, Apr. 4, 2005, http://slate.com/toolbar.aspx?action=print&id/2116169.

120. ROBB, supra note 1, at 27.

121. *Id.* at 28-29.

afoul of global opinion.[122] In short, such police states breed more fear and discontent at home, as well as hamper cooperation abroad.

There has been no evidence shown that the repudiation or reinterpretation of our international legal obligations, the weakening of constitutional protections against torture, widespread domestic wiretapping, or lengthy detention without trial have enhanced our security in a meaningful way.[123] While it is true that we have not suffered a major attack since September 11, there is no evidence that a major attack was prevented by one of these techniques of questionable legality. To the other extent, these techniques have worn away at our constitutional protections, have driven deep wedges into our political culture, and have undermined some of our most important diplomatic relationships.

Some would respond that such measures are only necessary for the duration of the conflict. But how shall we know that this war is at an end? We cannot expect the eradication of all terrorism. The answer heard most often is that the war will be over when the threat from al Qaeda is extinguished. But this is a bit of linguistic sleight-of-hand. Al Qaeda as we knew it is largely gone. Much, if not most, of its original senior leadership has been killed and its original bases have been destroyed. But al Qaeda 2.0 lives on, and when one understands the nature of terror networks, it is likely that some type of entity named al Qaeda may exist for quite a long time. What we now call al Qaeda is often comprised of people who began their activities after September 11, and with little direct link to bin Laden. It is a mushrooming of new cells with similar goals and symbols, each of which can act as a node in a broader network. Al Qaeda is becoming more of the rallying cry of a movement than a single coherent organization.

The problem is that the foe we are fighting—a transnational terror network—is not a state, and so the normal signifiers of the end of a war—peace treaties, summit conferences, and the like—simply do not apply here. Fourth generation warfare may seem new, but some old verities apply. Despite new technology, it is a conflict where the psychological aspect is central, and where it is important that we not be seen as jettisoning who we are simply because of who we fight. Consequently, the rule of law is vital in this twilight struggle because it

122. *Id.* at 156-57.

123. *See* Kelly Ann Moore, Op-Ed., *Take Al Qaeda to Court*, N.Y. TIMES, Aug. 21, 2007, at 19 (explaining the strengths of federal courts in anti-terrorism cases).

helps define who we are by what we fight for. It helps maintain the moral cohesion that we need in order to prevail in a 4GW conflict. And, notwithstanding claims that it is necessary to rewrite our constitutional order and reject our international obligations (based on evidence that we cannot be allowed to see), it is poor strategic thinking to sell short the network of law.

International terrorism does not threaten the very survival of our country. However, the idea of America can die a sort of death by a thousand self-inflicted cuts in which we continually slice away at some basic part of who we are in reaction to various threats and stresses. This is one of the insights of the theories of 4GW and yet, somehow, it is the key lesson that the Bush Administration had missed.[124]

"The key factors that spawned international terrorism show no signs of abating over the next [ten to] fifteen years."[125] In the coming years, "[w]eak governments, lagging economies, religious extremism, and youth bulges will align to create a perfect storm for internal conflict in certain regions."[126] Victory in the struggle against terrorism "will come not when Washington and its allies kill or capture all terrorists or potential terrorists but when the ideology the terrorists espouse is discredited, when their tactics are seen to have failed, and when they come to find more promising paths to the dignity, respect, and opportunities they crave."[127]

In this regard, fostering the rule of law in the societies that are the breeding grounds for terrorism is important. But, in order to do that, supporting the rule of law within and among our own societies is a necessary step.

---

124. For two recent critiques of the Bush Administration's treatment of international law within the "War on Terror," see TOM FARER, CONFRONTING GLOBAL TERRORISM AND AMERICAN NEO-CONSERVATIVISM: THE FRAMEWORK OF A LIBERAL GRAND STRATEGY (2008); PHILIPPE SANDS, LAWLESS WORLD: AMERICA AND THE MAKING AND BREAKING OF GLOBAL RULES FROM FDR'S ATLANTIC CHARTER TO GEORGE W. BUSH'S ILLEGAL WAR 223-39 (2005). *But cf.* BENJAMIN WITTES, LAW AND THE LONG WAR: THE FUTURE OF JUSTICE IN THE AGE OF TERROR (2008) (arguing that September 11 has led to a foundational moment in which we must re-balance the relationship of civil liberties and national security to address the new threats of transnational terrorism).

125. 2020 PROJECT, NATIONAL INTELLIGENCE COUNCIL, MAPPING THE GLOBAL FUTURE: REPORT OF THE NATIONAL INTELLIGENCE COUNCIL'S 2020 PROJECT BASED ON CONSULTATIONS WITH NONGOVERNMENTAL EXPERTS AROUND THE WORLD 15 (2004), *available at* http://www.foia.cia.gov/2020/2020.pdf.

126. *Id.* at 14.

127. Gordon, *supra* note 34.

V. CONCLUSION

Understanding the phenomenon of terrorism in the early twenty-first century requires an appreciation of how networks operate. Terrorist organizations more than ever are organized as non-hierarchical, scattered-cluster networks.

The targets of terrorist networks are the very infrastructure of modern industrial societies: electrical grids, oil pipelines, and the World Wide Web. Terrorist networks seek to weaken states by crashing the networks upon which states rely.

In response to these threats, states have created a variety of policies ranging from military invasion, to intelligence operations, to law enforcement investigations. However, of the various tools at its disposal, the Bush Administration had been wary, if not hostile, to using the network of transnational law to respond to the network of terrorists.

Non-hierarchical international networks defy a unilateral response. There is no single country that can be invaded to crash the whole network. There is no single person to capture or kill. Rather, key nodes throughout the network have to be disabled and linkages have to be cut. This requires a coordinated, multilateral response. The web of anti-terrorism treaties have provided the groundwork for policy and law enforcement coordination.

It is important that the right nodes are attacked. This will require good intelligence. While network theory proposes some possibilities regarding information acquisition—such as broadening the scope of phone and e-mail surveillance and cross-referencing the results—there are serious civil liberty concerns. But network theory also provides insights as to the *process* of intelligence analysis that may lead to better collaboration and more accurate reports that can serve in our efforts to frustrate or destroy terrorist organizations.

However, it is important to keep in mind that the goal of al Qaeda, and of groups like it, is to sap our strength and fray our social cohesion. For these reasons, a crucial part of the network of law is not only the laws that enable us to strike at the terrorists, but also those laws that protect our way of life, our freedoms, and our liberties. While times of conflict often cause a certain rebalancing of the relationship of individual rights to national security, it is vital to keep in mind that such rebalancing should be as a small as possible. If we change who we are, then we have handed the terrorist what they want.

The network of laws should not be understood, in the words of the

Department of Defense, as "a strategy of the weak." Rather, it is the shield that protects our society both from the terrorists and from our own worst inclinations.