The New York Times Magazine

More Articles in Magazine >

NYTimes.com Go to a Section

Log In - Register Now

SEARCH

NYT Since 1981 ▼ Search

IDEA LAB

Can Network Theory Thwart Terrorists?

By PATRICK RADDEN KEEFE

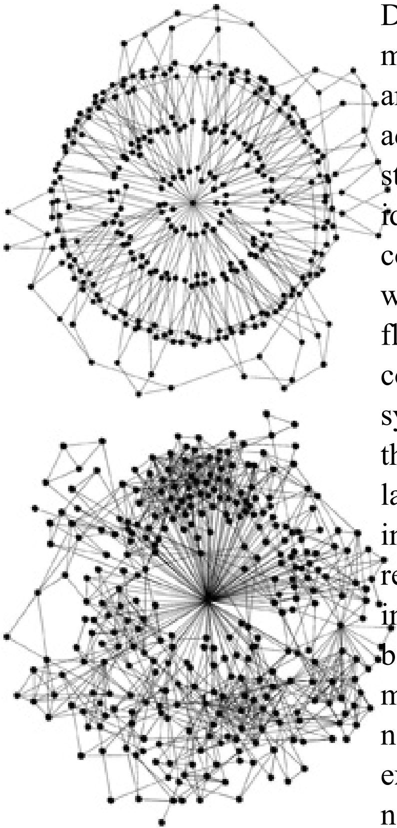
Published: March 12, 2006

Sign In to E-Mail This

Printer-Friendly

Save Article

Recent debates about the National Security Agency's warrantless-eavesdropping program have produced two very different pictures of the operation. Whereas administration officials describe a carefully aimed "terrorist surveillance program," press reports depict a pervasive electronic net ensnaring thousands of innocent people and few actual terrorists. Could it be that both the administration and its critics are right? One way to reconcile these divergent accounts — and explain the administration's decision not to seek warrants for the surveillance — is to examine a new conceptual paradigm that is changing how America's spies pursue terrorists: network theory.



Computer Rendering by Sergi Valverde and Ricard V.

During the last decade, mathematicians, physicists and sociologists have advanced the scientific study of networks, identifying surprising commonalities among the ways airlines route their flights, people interact at cocktail parties and crickets synchronize their chirps. In the increasingly popular language of network theory, individuals are "nodes," and relationships and interactions form the "links" binding them together; by mapping those connections, network scientists try to expose patterns that might not otherwise be apparent.

Solé/ICREA/Complex Systems Lab
A Pattern Language Network relationships in a digital circuit (top) and a television circuit (bottom).

Researchers are applying newly devised algorithms to vast databases — one academic team recently examined the e-mail traffic of 43,000 people at a large university and mapped their social ties. Given the difficulty of identifying elusive terror cells, it was only a matter of time before this new science was discovered by America's spies.

In its simplest form, network theory is about connecting the dots. Stanley Milgram's finding that any two Americans are connected by a mere six intermediaries — or "degrees of separation" — is one of the animating ideas behind the science of networks; the Notre Dame physicist Albert-Laszlo Barabasi studied one obvious network — the Internet — and found that any two unrelated Web pages are separated by only 19 links. After Sept. 11, Valdis Krebs, a Cleveland consultant who produces social network "maps" for corporate and nonprofit clients, decided to map the hijackers. He started with two of the plotters, Khalid al-Midhar and Nawaf Alhazmi, and, using press accounts, produced a chart of the interconnections — shared addresses, telephone numbers, even frequent-flier numbers — within the group. All of the 19 hijackers were tied to one another by just a few links, and a disproportionate number of links converged on the leader, Mohamed Atta. Shortly after posting his map online, Krebs was invited to Washington to brief intelligence contractors.

Announced in 2002, Adm. John Poindexter's controversial Total Information Awareness program was an early effort to mine large volumes of data for hidden connections. But even before 9/11, an Army project called Able Danger sought to map Al Qaeda by "identifying linkages and patterns in large volumes of data," and may have succeeded in identifying Atta as a suspect. As if to underline the project's social-network principles, Able Danger analysts called it "the Kevin Bacon game."

Given that the N.S.A. intercepts some 650 million communications worldwide every day, it's not surprising that its analysts focus on a question well suited to network theory: whom should we listen to in the first place? Russell Tice, a former N.S.A. employee who worked on highly classified Special Access Programs, says that analysts start with a suspect and "spider-web" outward, looking at everyone he contacts, and everyone those people contact, until the list includes thousands of names. Officials familiar with the program have said that before individuals are actually wiretapped, computers sort through flows of metadata — information about who is contacting whom by phone or e-mail. An unclassified National Science Foundation report says that one tool analysts use to sort through all that data is link analysis.

The use of such network-based analysis may explain the administration's decision, shortly after 9/11, to circumvent the Foreign Intelligence Surveillance Court. The court grants warrants on a case-by-case basis, authorizing comprehensive surveillance of specific individuals. The N.S.A. program, which enjoys backdoor access to America's major communications switches, appears to do just the opposite: the surveillance is typically much less intrusive than what a FISA warrant would permit, but it involves vast numbers of people.

In some ways, this is much less alarming than old-fashioned wiretapping. A computer that monitors the metadata of your phone calls and e-mail to see if you talk to terrorists will learn less about you than a government agent listening in to the words you speak. The problem is that most of us are connected by two degrees of separation to thousands of people, and by three degrees to hundreds of thousands. This explains reports that the overwhelming number of leads generated by the N.S.A. program have been false positives — innocent civilians implicated in an ever-expanding associational web.

This has troubling implications for civil liberties. But it also points to a practical obstacle for using link analysis to discover terror networks: information overload. The National Counterterrorism Center's database of suspected terrorists contains 325,000 names; the Congressional Research Service recently found that the N.S.A. is at risk of being drowned in information. Able Danger analysts produced link charts identifying suspected Qaeda figures, but some charts were 20 feet long and covered in small print. If Atta's name was on one of those network maps, it could just as easily illustrate their ineffectiveness as it could their value, because nobody pursued him at the time.

One way to make sense of these volumes of information is to look for network hubs. When Barabasi mapped the Internet, he found that sites like Google and Yahoo operate as hubs — much like an airline hub at Newark or

O'Hare — maintaining exponentially more links than the average. The question is how to identify the hubs in an endless flow of records and intercepted communications. Scientists are using algorithms that can determine the "role structure" within a network: what are the logistical and hierarchical relationships, who are the hubs? The process involves more than just tallying links. If you examined the metadata for all e-mail traffic at a university, for instance, you might find an individual who e-mailed almost everyone else every day. But rather than being an especially connected or charismatic leader, this individual could turn out to be an administrator in charge of distributing announcements. Another important concept in network theory is the "strength of weak ties": the most valuable information may be exchanged by actors from otherwise unrelated social networks.

Network academics caution that the field is still in its infancy and should not be regarded as a panacea. Duncan Watts of Columbia University points out that it's much easier to trace a network when you can already identify some of its members. But much social-network research involves simply trawling large databases for telltale behaviors or activities that might be typical of a terrorist. In this case the links among people are not based on actual relationships at all, but on an "affiliation network," in which individuals are connected by virtue of taking part in a similar activity. This sort of approach has been effective for corporations in detecting fraud. A credit-card company knows that when someone uses a card to purchase $2 of gas at a gas station, and then 20 minutes later makes an expensive purchase at an electronics store, there's a high probability that the card has been stolen. Marc Sageman, a former C.I.A. case officer who wrote a book on terror networks, notes that correlating certain signature behaviors could be one way of tracking terrorists: jihadist groups in Virginia and Australia exercised at paint-ball courses, so analysts could look for Muslim militants who play paint ball, he suggests. But whereas there is a long history of signature behaviors that indicate fraud, jihadist terror networks are a relatively new phenomena and offer fewer reliable patterns.

There is also some doubt that identifying hubs will do much good. Networks are by their very nature robust and resistant to attack. After all, while numerous high ranking Qaeda leaders have been captured or killed in the years since Sept. 11, the network still appears to be functioning. "If you shoot the C.E.O., they'll hire another one," Duncan

Watts says. "The job will still get done."

Patrick Radden Keefe, a Century Foundation fellow, is the author of "Chatter: Dispatches from the Secret World of Global Eavesdropping."

More Articles in Magazine >

RELATED ARTICLES

Scientists Debate What to Do When Findings Aid an Enemy (September 25, 2001)

RELATED SEARCHES

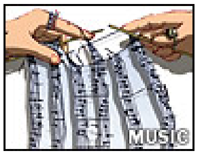
Science and Technology | National Security Agency | Terrorism

INSIDE NYTIMES.COM

Charles Taylor's Rise and Fall

The Ghost in the Baghdad Museum

Making of a Toddler Supergroup



Digital Composer

Gretchen Mol: Portfolio by Jeff Koons