NEWS

Counterterrorism's New Tool: 'Metanetwork' Analysis

Researchers have created sophisticated new programs to probe beneath the surface of social interactions. How well do they work against terrorists?

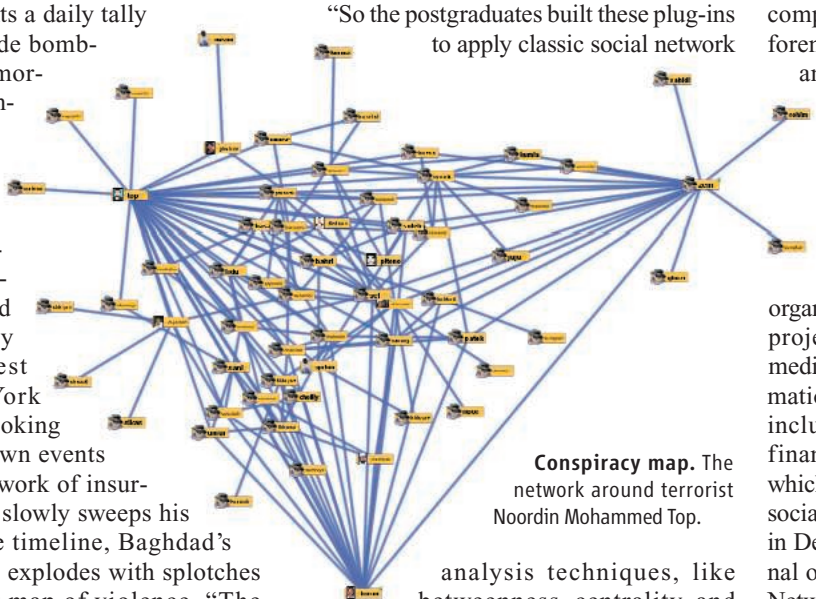
PALO ALTO, CALIFORNIA—In a comfortable Silicon Valley boardroom, a world away from the hellish violence of Iraq, Shyam Sankar projects a satellite map of Baghdad on a screen. "Now let's look at the geospatial distribution of significant acts," says the software engineer.

With a few clicks of his computer mouse, he creates a timeline below the map. What looks like a city skyline rises up over April and May 2008. But rather than skyscrapers, each bar represents a daily tally of carnage: suicide bombings, shootings, mortar attacks, and improvised explosive device (IED) detonations. The data come from a collaboration of researchers at Princeton University and the U.S. Military Academy at West Point in New York state. They are looking behind these known events to a shadowy network of insurgents. As Sankar slowly sweeps his cursor across the timeline, Baghdad's Sadr City district explodes with splotches of color—a heat map of violence. "The attacks turn out to be correlated over time and space with the construction of this security wall," says Asher Sinensky, tracing a line across the district.

Insights like these are crucial for U.S. and Iraqi forces trying to predict the insurgents' next moves. Sankar, 27, and Sinensky, 29, are "forward-deployed engineers" here at Palantir Technologies, the software company behind this data analysis platform. Business is booming.

"Here's work we're doing with the Naval Postgraduate School," says Sinensky. A blizzard of tiny boxes appears, all interconnected by a web of lines. "This is the network of people connected to Noordin Mohammed Top," a recruiter for the group Jemaah Islamiyah and Southeast Asia's most wanted terrorist. The graph represents the suspects' known communications and relationships, as well as their known involvement with terrorist plots, distilled from unclassified data provided by the International Crisis Group headquartered in Brussels. "You have this huge ball and it's somewhat meaningless," Sinensky says. He selects a command from a drop-down menu.

"So the postgraduates built these plug-ins to apply classic social network analysis techniques, like betweenness, centrality, and eigenvector centrality." He executes a command and names appear, ranked by a calculation of their importance as nodes in the network. "It's no surprise that Noordin is first," says Sinensky. "But what about these next two? Maybe these are people I should focus some resources on."



Conspiracy map. The network around terrorist Noordin Mohammed Top.

CREDIT: STEFFEN MERTEN COURTESY OF PALANTIR

A decade ago, most research on social networks was abstract and academic. But in the wake of the 11 September 2001 attacks, "there was an explosion of interest" in applying this research to warfare, says Kathleen Carley, a computer scientist at Carnegie Mellon University in Pittsburgh, Pennsylvania. Palantir is just one of many companies vying for a piece of the military funding. Academic network scientists such as Carley are also diving in, competing for lucrative U.S. military contracts and grants.

In spite of the boom, there is sharp disagreement about how effective social network analysis has been for counterterrorism. Some worry that in the rush to catch terrorists, the U.S. military has put too much faith in social network analysis. One former U.S. official even claims that applying these methods in war zones has led to unethical practices (see sidebar, p. 410).

Tangled webs

Just weeks after the 2001 plane hijackings in the United States that killed some 3000 people, it emerged that the attacks were not the work of a government but a team of international terrorists: 19 hijackers and dozens of people providing funding and logistical support. "The intelligence community was in a complete hysteria," says Marc Sageman, a forensic psychiatrist who has analyzed this and other militant networks for the U.S. government since the 1980s. U.S. government officials "turned to anyone" who could help assess this new threat and prevent another attack.

Among the first to be tapped was Valdis Krebs, a management consultant who studies social networks within organizations. "A terrorist cell is essentially a project team like any other," he says. The media provided a "nonstop stream" of information about the 11 September network—including their meetings, residences, and financial transactions around the world—which Krebs used to map a "quick and dirty" social network. Krebs published his analysis in December 2001 in *Connections*, the journal of the International Network for Social Network Analysis. One node in particular—Mohamed Atta—stood out in his network graph. "Atta scores the highest on all network centrality metrics—Degrees, Closeness, and Betweenness," Krebs concluded in his paper. "Degrees reveals [the intensity of] Atta's activity in the network. Closeness measures his ability to access others in the network and monitor what is happening. Betweenness shows his control over the flow in the network—he plays the role of a broker." Atta was indeed the ringleader and a member of al-Qaeda, the terrorist organization that claimed responsibility for the 11 September attacks through its spokesman, Osama bin Laden. Soon after, says Krebs, he and other

Published by AAAS

Investigating Networks: The Dark Side

A few months ago, Lawrence Wilkerson, a former U.S. State Department official and Army colonel, issued a scathing criticism of how the United States has conducted war in recent years. He also painted a nightmare scenario of how social network science can be applied in a battle zone. Describing how U.S. forces gathered intelligence to identify networks of insurgents after the 2003 invasion of Iraq, Wilkerson outlined something he called "the mosaic philosophy." The strategy, he claims, was similar to sequencing a genome. But instead of assembling millions of strands of DNA, investigators worked with data from interrogations of thousands of civilian prisoners.

Wilkerson wrote in a 17 March 2009 article at The Washington Note—a political commentary Web site—that the U.S. military relied on network analysis "computer programs" so that "dots could be connected and terrorists or their plots could be identified." Now based at the New America Foundation, a think tank in Washington, D.C., Wilkerson wrote that "it did not matter if a detainee were innocent." According to Wilkerson, the objective of the mosaic approach was to "extract everything possible … to have sufficient information about a village, a region, or a group of individuals. … Thus, as many people as possible had to be kept in detention for as long as possible to allow this … to work."

Wilkerson told *Science* that his allegation is based on "classified documents to which I had access from 2000 to 2005" as chief of staff for former U.S. Secretary of State Colin Powell. He puts the total number of people detained in Iraq and Afghanistan at 50,000. He says he does not know which computer program or researchers were involved. The U.S. Department of Defense declined to comment. The allegation could not be independently verified.

The general strategy of casting a wide net for intelligence gathering was familiar to all network researchers contacted by *Science* (see main text), but many expressed disbelief that it was carried out on such a grand scale in Iraq and Afghanistan. "Very scary if true," says Marc Sageman, a network researcher and longtime U.S. military contractor, but it would be "incredible." He adds that it would never work, even if it were tried.

Researchers who create network analysis computer programs have had similar reactions. Software engineers at one of the industry leaders, Palantir Technology in Palo Alto, California, say they had never heard of such abuses. And Wilkerson's "computer program" could not have been theirs, says Palantir CEO Alexander Karp, because the company only recently started courting the U.S. military for contracts. "If we ever learned that something like this was going on, we would immediately pull out," he adds.

Only one researcher contacted by *Science* had heard of the mosaic philosophy. "It's not a

network researchers were "invited to many meetings and briefings in Washington, D.C."

By 2003, U.S. defense officials had expanded the web of threats beyond the 11 September terrorists to include networks of "insurgents" in Afghanistan and Iraq. In October of that year, the U.S. Army created a research task force devoted to countering IEDs, which the U.S. Department of Defense described as "the weapon of choice for adaptive and resilient networks of insurgents and terrorists." Part of the strategy was to apply network analysis to the available data—from types of devices to people funding, building, and deploying them.

According to Sageman, the results were disappointing. "The network approach didn't really work to catch bad guys," he says. It was limited partly by the rigidity of the underlying field of mathematics, graph theory. "We are good at modeling static networks," he says, "but networks like these change over time. And we don't yet have a dynamic graph theory." When one terrorist is caught or killed, for example, "he is replaced by a cousin" with different social links. "Changing a single link can completely change the graph," he says, but the theory doesn't accommodate this. It's even harder to accommodate growth. "We don't have a decay function that can reliably remove the noise," says Sageman. As a result, the bigger your network model grows, the noisier its gets—and "the less you see."

Deadly clues. Researchers have struggled to model the Iraqi insurgent networks behind IED attacks.

The flaws of counterterrorism network analysis, according to Krebs, run deeper than math. "It is also about understanding sociology," he says. No matter how good a network model is, it can't provide insights if researchers aren't "paying attention to the right things and therefore collecting the right data." Without accounting for the content of communication, social network analysis runs into the "pizza delivery guy problem": confusing regular contact with significant contact.

As an illustration of the problem, Sageman points to a report on the 7 July 2005 bombing of the London Underground, issued in May by the U.K. Intelligence and Security Committee, titled *Could 7/7 Have Been Prevented?* Using network analysis, the researchers traced the relations between plotters, yielding a chaotic tangle of links. "They couldn't learn anything from this graph," says Sageman. "It's a hairball!" (U.K. government officials declined to provide *Science* with a publishable high-resolution version, citing "security reasons.")

Going meta

According to Ian McCulloh, a U.S. Army major who teaches network analysis at the Military Academy, the way forward is a tech-

CREDITS: AP IMAGES

Published by AAAS

term used in academia. It's used in the military," says Kathleen Carley, a computer scientist at Carnegie Mellon University in Pittsburgh, Pennsylvania, who does network analysis research for the U.S. military. "I am not part of the mosaic thing." Carley does not dismiss the strategy as ineffective. Without knowing exactly how the interrogations and data analysis were carried out, she says, "I don't think you can decide whether it's unworkable or not."

Asked if the mosaic philosophy is actively applied by U.S. military or intelligence agencies, Wilkerson says emphatically that it is not. Revelations about the torture of prisoners by U.S. forces have "caused the pendulum to swing the other way," he says. "The only place I still hear about its applicability and possible use is at the [National Security Agency]. … There, its use is to mine huge databases comprised of information gained from e-mails and telephone calls."

"Is this the dark side of networks? … I think it probably is," says Brian Uzzi, a network scientist at Northwestern University in Evanston, Illinois. "All powerful methods grow a dark side. Their power is eventually used irresponsibly. I think the real fear here is that a method that has a reputation for finding new insights is falsely used." **–J.B.**

Analytical fodder? A former U.S. official alleges that innocent people in Iraq and Afghanistan were interrogated to feed data into terrorist network models.

CREDIT: AP IMAGES

nique called "dynamic metanetwork analysis." McCulloh learned the technique from Carley, his adviser for a Ph.D. he completed at Carnegie Mellon last year. Carley and McCulloh say their models can deal with change in terrorist networks over time. And whereas classic social network analysis deals only with the question of "who" in networks, says Carley, "metanetworks include the who, when, what, where, why." By capturing these layers, metanetworks "begin to get at culture," she says. "You have to go beyond the communication network to consider the distribution of norms, attitudes, and beliefs, … the distribution of roles across gender, ages, and subgroups," she says. "But the programs to do that go way beyond general social network analysis."

Carley has developed computer programs of her own to do that. She says that one of them, the Organizational Risk Analyzer (ORA), helps analysts "use information about people to 'connect the dots.' Then, ORA examines this network and finds those dots, those people, who represent a threat to the overall system." The program uses both network theory and social psychology to calculate people's "cognitive demand," which Carley defines as a measure of things such as "how many others they need to interact with, how many activities they are involved with, how complex those activities are, [and] how many resources they need to handle." In the case of a business, an analyst can use ORA to identify employees who are crucial for a company's survival. The same applies for a network of insurgents.

McCulloh and Carley used metanetwork analysis to analyze 1500 videos made by insurgents in Iraq. "The insurgents would videotape most of their attacks as propaganda," says McCulloh. "As of March 2006, we had something like almost three out of every four U.S. deaths [on tape]." Carley extracted data from these videos, he says, "made a big network out of it, and ran a fragmentation algorithm which clustered them into little groups. And when you go back and look at the videos in those groups, you see forensic clues that identify who some of the insurgent cells were." The details extracted from the videos are classified, "because we worry that the insurgents will learn what we're using," McCulloh says. He and Carley worked with the U.S. military to "operationalize" the technique in Iraq. U.S. commanders there are faced with too much information and too little time to act on it. McCulloh says that Carley's metanetwork software helps them find clues and patterns—boosting the chances of catching or killing insurgents.

McCulloh claims that the technique has yielded dramatic results. "Sniper activity in Iraq is down by 70%," he says, and he's confident that IED deaths also dropped because of the insights provided by Carley's programs, although he can't cite data. "It's a simple application of metanetwork analysis," he says.

But Sageman is skeptical that military progress in Iraq can be chalked up to network analysis. "I'm not convinced [metanetworks] have helped at all," he says. "An easier explanation [for the drop in sniper attacks] might be the tribal uprising" against the insurgency in Iraq. "There's no way to know, and that's a big problem with this field in general." Carley counters that Sageman "doesn't understand the methods."

If not all researchers are sold on counterterrorism network analysis, the U.S. military certainly is. The Army established a network science center in Aberdeen, Maryland, 2 years ago. This year, the U.S. Army Research Lab is committing $162 million to a new program, the Network Science Collaborative Technology Alliance, to get academic, industry, and military researchers working on "network-centric warfare."

Carley is one of the academics applying for military funding. She says that network analysis is ready for war. A decade ago, models could handle only simple information about "hundreds" of people at once. But now, she says, "network analysis tools can handle millions or tens of millions of nodes." **–JOHN BOHANNON**

Published by AAAS