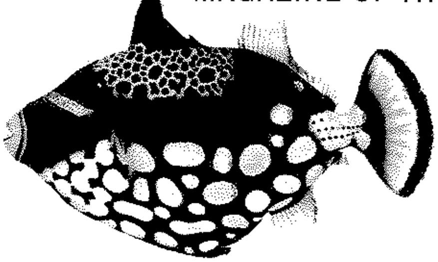
Math vs. Terror | Enzyme Enigmas | Meet Mr. Lucy

www.sciencenews.org

Science News

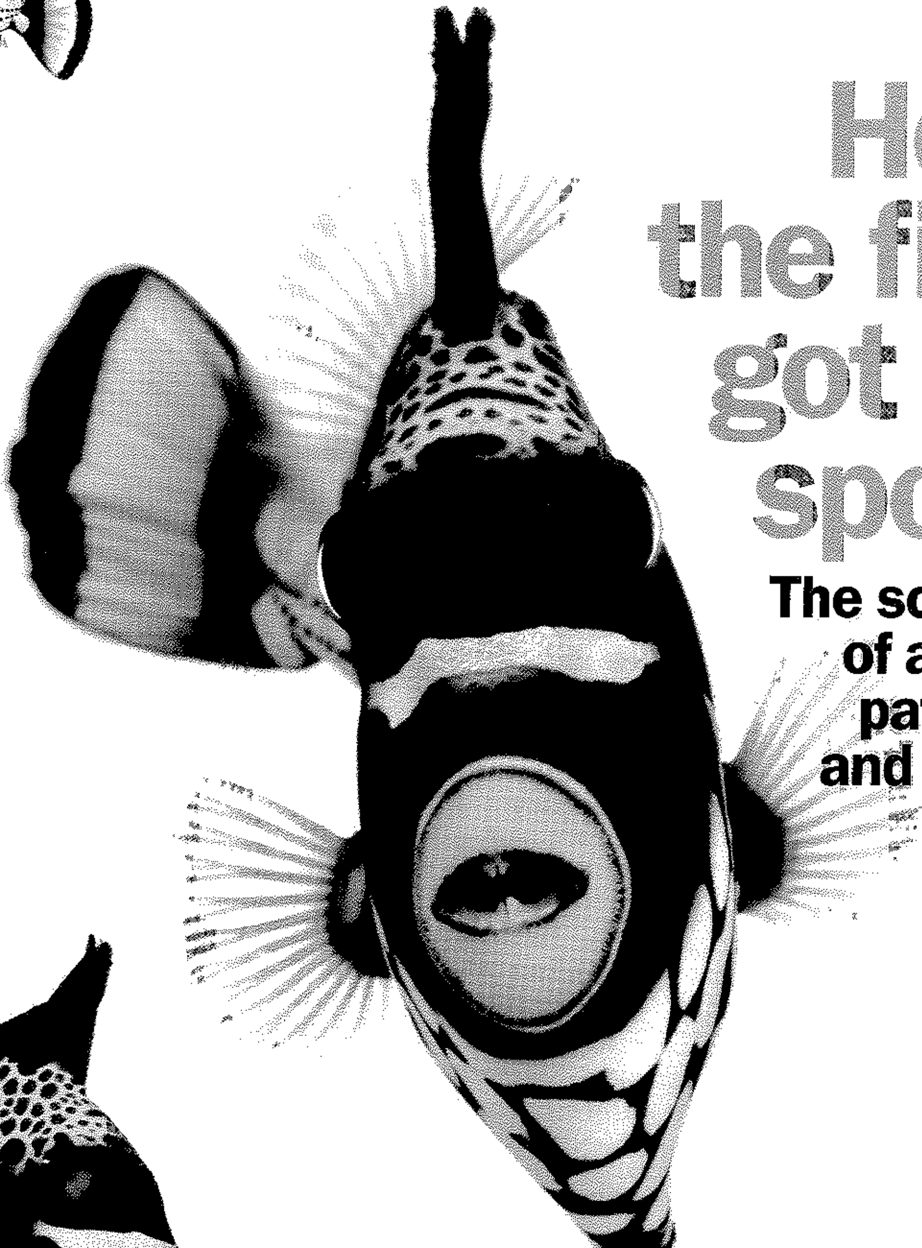
MAGAZINE OF THE SOCIETY FOR SCIENCE & THE PUBLIC ■ JULY 17, 2010



Neutrinos Challenge Relativity

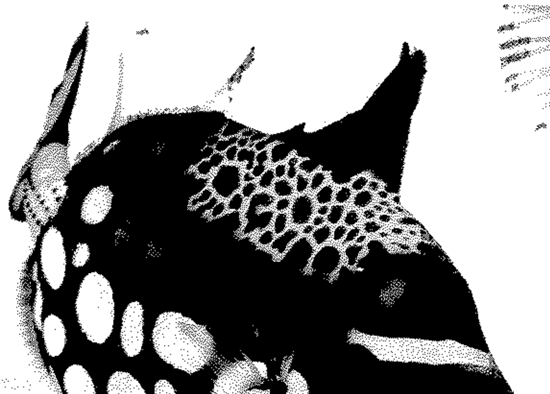
Blind Mice Regain Sight

Your Brain on Snakes



How the fish got its spots

The science of animal patterns and prints



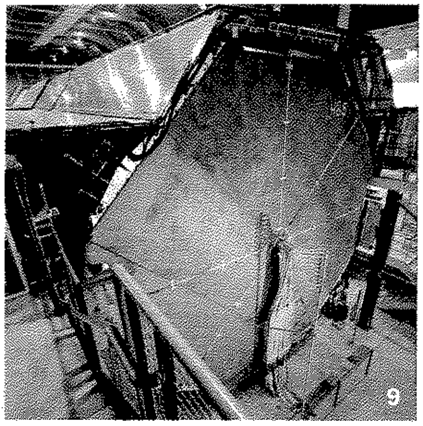
$3.95

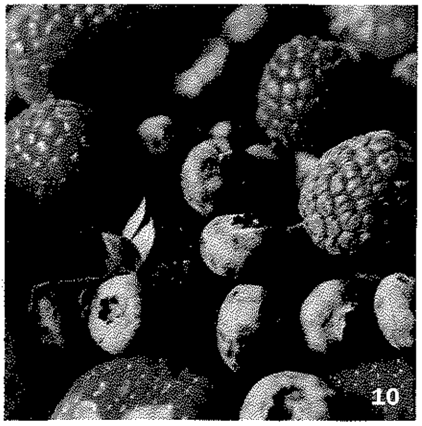
30>

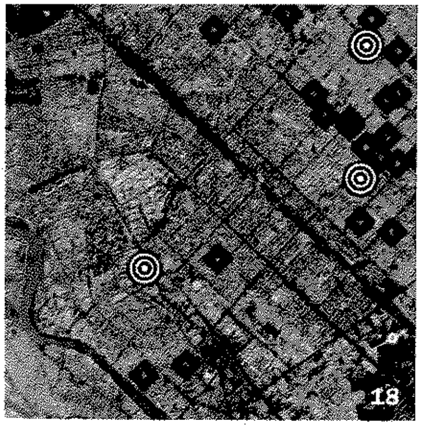
0 71486 02941 0

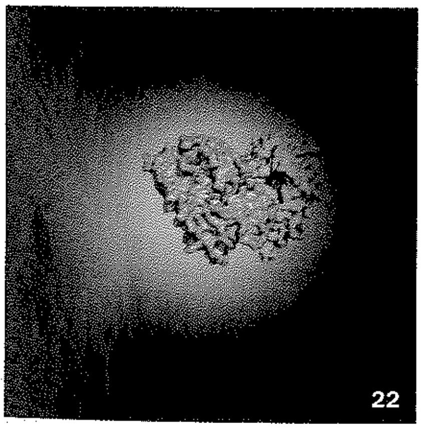
JULY 17, 2010 • VOL. 178 • NO. 2

ScienceNews









In The News

Features

Departments

COVER Scientists are learning how animals like the clown triggerfish, *Balistoides conspicillum*, create their colorful patterns. *Photos © Eric Isselée/ Dreamstime.com*

ScienceNews
MAGAZINE OF THE SOCIETY FOR SCIENCE & THE PUBLIC

EDITORIAL, ADVERTISING AND BUSINESS OFFICES
1719 N Street NW, Washington, DC 20036 **Phone** (202) 785-2255
Subscriptions subs@sciencenews.org **Editorial/Letters** editors@sciencenews.org
Advertising/Business snsales@sciencenews.org
Texterity Digital edition provided by Texterity, www.texterity.com
Science News (ISSN 0036-8423) is published biweekly, for $54.50 for 1 year or $98 for 2 years (international rate $80.50 for 1 year or $161 for 2 years) by Society for Science & the Public, 1719 N Street NW Washington, D.C. 20036.
Preferred periodicals postage paid at Washington, D.C., and an additional mailing office.
Subscription Department: PO Box 1205, Williamsport, PA 17703-1205. For new subscriptions and customer service, call 1-800-552-4412.
Postmaster: Send address changes to *Science News*, PO Box 1205, Williamsport, PA 17703-1205. Two to four weeks' notice is required. Old and new addresses, including zip codes, must be provided.

FROM THE EDITOR

Using math to fight terror could be a good strategy

Old paradigms never die — they just create conundrums for slow learners.

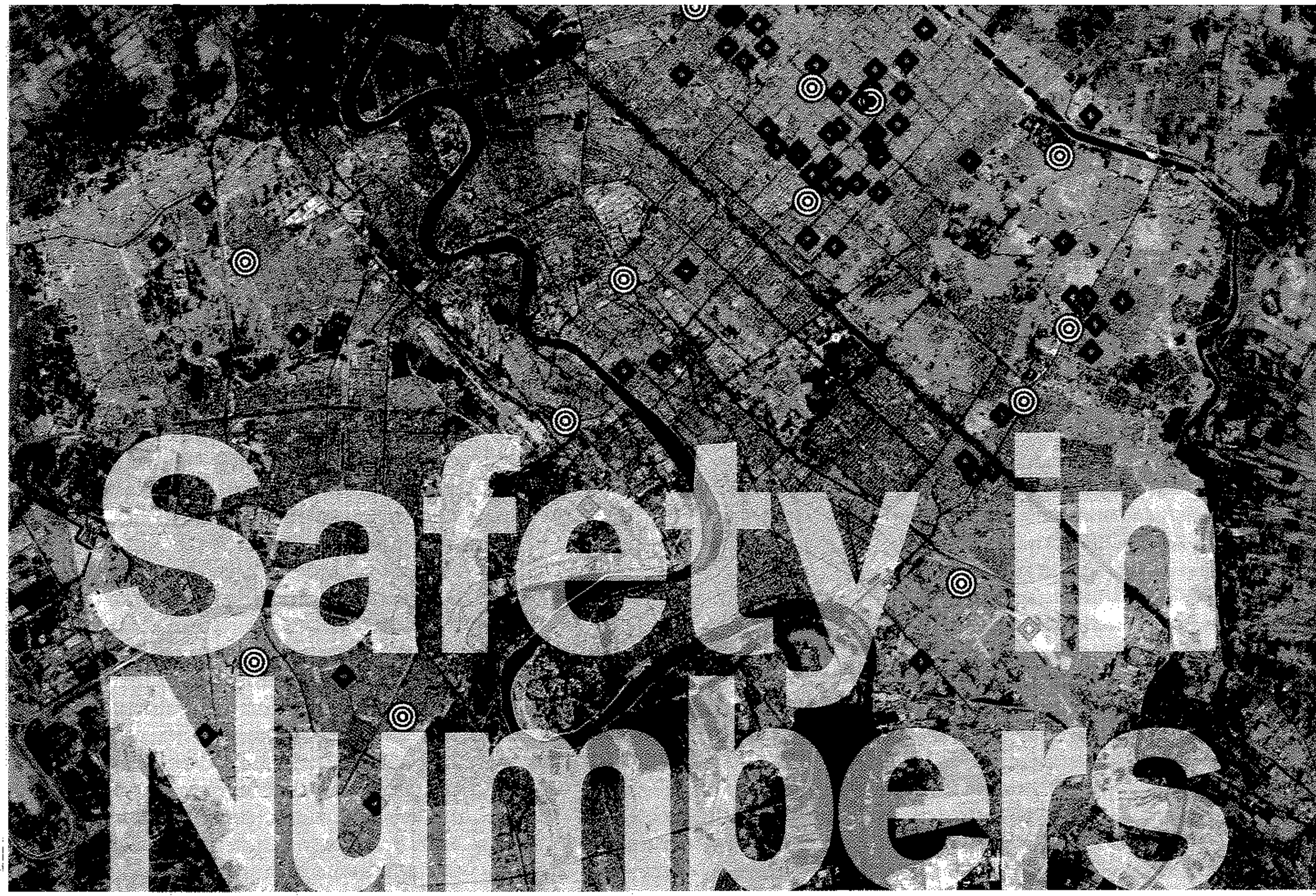
In the print journalism world, for instance, the old paradigm of readers paying for paper with ink on it has been eroded by electronic delivery via various digital devices ranging from laptops to app phones. Sure, many readers still prefer paper, and the best publishers maintain the quality of their traditional physical product. But sustaining economic viability will also require strategies that embrace new media and develop creative methods for delivering credible content in unconventional forms.

In a very similar way, governments seeking to preserve national security can no longer intelligently rely only on the past paradigms of superior military muscle. Enemy forces are no longer restricted to armies supported by political states defined by geography. Threats of deadly punishment do not deter combatants whose strategy often relies on suicide to begin with. Brute force cannot always cope with foes that don't fight by conventional rules of engagement.

Consequently, counterterrorism strategists ought to be interested in adopting some unconventional methods themselves. And, as Laura Sanders describes in this issue (Page 18), some such methods might be rooted in mathematics. In real-life versions of the sort of thing you'd see on the TV show *Numb3rs*, mathematicians have devised ways of analyzing the organization of terrorist cells, identifying key leaders and locating likely sites of hidden weapons caches.

Many of these approaches involve game theory — the science of choosing strategies. Game theory originated in economics and was made famous by the book and movie *A Beautiful Mind*. One of its lessons is that there is rarely only one right strategy in a competitive situation, because your enemy could predict it and choose effective countermeasures. It's almost always better to adopt a "mixed strategy," which means choosing with some element of randomness from among various possible actions.

In other words, game theory says that anyone advocating a one-size-fits-all approach to fighting terrorism (or any other strategic problem) is not too bright. So it makes sense that math should join military might in the antiterror arsenal, both as an additional weapon and as a way of choosing which weapons to use. (And it implies that keeping magazines around is a good idea, too.) — *Tom Siegfried, Editor in Chief*



Safety in Numbers

Mathematics offers innovative weapons for fighting terrorism

By Laura Sanders

Mathematicians don't wear capes and tights. They are not more powerful than a locomotive and they can't leap tall buildings in a single bound. But when it comes to protecting people from evildoers, these calculating crusaders could turn out to be super.

On the surface, fighting terrorists with mathematics sounds absurd. Yet some mathematicians and computer scientists are devising equations and algorithms that show real promise as terrorism countermeasures. From simple formulas that focus on mathematical properties underlying terrorist behavior to immense mega-analyses incorporating billions of information bits, mathematics is becoming an increasingly important weapon in the antiterror arsenal.

"The area has exploded, in terms of the types of techniques and technologies," says computer scientist Kathleen Carley of Carnegie Mellon University in Pittsburgh. "There are huge, rapid advances in this area with, of course, some very interesting challenges."

Some researchers, including Carley, are formulating powerful new algorithms that comb through mountains of data and uncover hidden "rules" that govern terrorism behavior. Each tiny electronic crumb — from among billions of cell phone calls, web-browsing records, e-mail messages, credit card receipts and airline manifests — could serve as a microclue to help create a complete picture of a terrorist's life.

Other researchers, instead of using mountains of data, begin with a molehill, seeking simple, pared-down mathematical formulas that might describe the optimal arrangement of a secret terrorist cell, for instance, and provide hints on how to destroy it.

Already, terror-crushing algorithms are proving their mettle. New techniques are untangling the covert organizational structure of terrorist networks. By modeling the internal tugs-of-war between secrecy and the need to communicate, researchers can predict patterns of terror cells' organization. Other mathematical methods may help identify the members of a terrorist cell who are actually calling the shots. And still other numerical techniques can pinpoint concealed weapons caches — a method now being used by two U.S. Army groups to find improvised explosive device stockpiles in Baghdad.

Putting hard numbers to something as nebulous and secretive as terrorism "transforms the science from being kind of a case study, expert-opinion sort of field into a quantitative area," says Alexander Gutfraind, a mathematician at Los Alamos National Laboratory in New Mexico. "If you have a mathematical model that can describe the structure of a terror network — and the model works — then you can predict the future."

V.S. SUBRAHMANIAN, P. SHAKARIAN, M. SAPINO

A new algorithm uses the location of blasts (red) from improvised explosive devices to deduce the hiding places of weapons caches (yellow) in Baghdad.

Some researchers are convinced of math's merits but face roadblocks in persuading other people that calculations can aid the fight. "These days, the impression I get is that people who ought to support this kind of research don't fully believe that mathematics can be useful," says mathematician Jonathan Farley of Johannes Kepler University Linz in Austria. "And their belief is so extreme that they're not even willing to check it out."

But some of the new methods are beginning to attract attention. Farley, Gutfraind and others belong to the Consortium for Mathematical Methods in Counterterrorism, which promotes math's role in tackling counterterrorism and global security problems. Consortium members share methods and papers, and meet annually to talk about emerging problems in their field, such as how to quantify threats of violence, how to disrupt terror cells and how terrorists arrange themselves into groups.

Connecting the right dots

In the aftermath of the September 11 attacks, a technique called social network analysis was touted as the best way to find terrorist kingpins. Connecting the dots between people called attention to those who were most highly linked — presumably, the most important members of the network. "The idea was to disconnect those social networks, and if you did this, you could inhibit, prevent or moderate the impact of these events — and maybe actually save lives," Carley says. "What we found in the ensuing time is that taking an approach that focuses only on social networks will not work."

Such simple maps can miss crucial features of terrorist networks. "The person with the most links is not necessarily the most important person," Farley says.

Carley's research group and others have begun to find that people who have roles in multiple groups — called interstitial members — are some of the most important. Interstitial members communicate between groups and relay information, a position critical to operations going as planned. A new technique called fuzzy grouping, which allows people to be assigned to multiple groups simultaneously, better describes how these people fit into networks, Carley says.

Another important attribute is exclusivity. Some members of a network have specialized training and so are in high demand for certain jobs. People who know how to launder money or fly an airplane, for instance, have a high exclusivity measure. Accounting for exclusivity measures and adopting fuzzy grouping techniques can lead to more nuanced descriptions of covert networks.

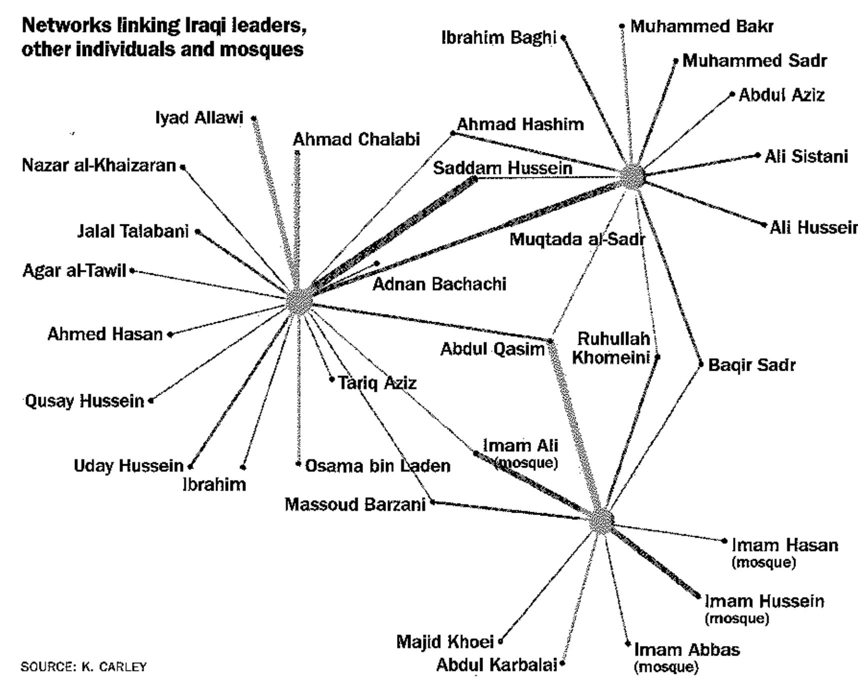
Putting terrorists into groups or assigning exclusivity measures is a matter of collecting and assessing the right pieces of data. "The data is coming from a wide variety of sources, things like open-source text, crowd-sourced information off the Web, anything you can basically imagine," says Carley. "The million dollar question is, can we drill down and find the network relevant to the problem?"

Ideally, drilling down through this aggregation of data will reveal trails. "We link together the who, the what, the where, the why, the how, and we use all of these things in a dynamic complex configuration," Carley says. Once specific trails are identified, complex grouping algorithms may be able to decipher unexpected locations for groups to meet, for instance.

Piecing together trails and anticipating behaviors of any single person is a challenge, and guessing the next move of clandestine groups such as Al Qaeda seems nearly impossible. But because terrorists rarely work in isolation, they are susceptible to what computer scientist V.S. Subrahmanian of the University of Maryland in College Park calls the "bureaucracy effect." Because of sluggish coordination, terrorist

Linked up A type of network arrangement called fuzzy group clustering pinpoints people who belong to two distinct groups simultaneously, such as Saddam Hussein. Models suggest that such "interstitial" members are likely to be the key coordinators of a terrorist mission.

Networks linking Iraqi leaders, other individuals and mosques



SOURCE: K. CARLEY

organizations' behavior is constrained, he says. "Large organizations, even if they are terrorist organizations, may not have the ability to make radical changes in their behavior without taking time to do so, and that makes them a little more predictable," he says.

A particularly rich source for data on behavioral patterns is news articles, Subrahmanian says. He and colleagues have begun testing a new algorithm that identifies and extracts keywords, such as "abduction," "suicide bombing" and "hostage" from news databases. The team aims to have the program ultimately extract over 700 variables accurately and automatically. These word frequencies could then be combined with other data to form "rules" about groups' behaviors. One such rule is that Lebanon-based Hezbollah, regarded by many, including the U.S. government, as a terrorist group, attacks Israel less often during Lebanon's election years, the team found, probably in an effort to garner public support at home.

Subrahmanian is exploring how to not just predict terrorist group behavior but to actually change it. With a grant from the Air Force Office of Scientific Research, he and his colleagues have developed a tool called the policy analytics generation engine. "The goal is to take the same kinds of data and turn it backwards," he says. "Rather than saying, 'Here's my data and here are the behaviors I've learned and here are my forecasts for what this group will do in the third quarter of 2010,' can we go the other way?"

Changing one key factor might make a big impact, Subrahmanian says. For instance, the rule about Hezbollah suggests that the political pressure of an election year keeps attacks low. Finding ways to dial up Hezbollah's political involvement in Lebanon might lead to fewer attacks on Israel. The idea is to identify the critical factors, and then figure out the constellation of forces that influence those factors, Subrahmanian says.

Calculated risks

In a more concrete example of counterterrorism, Subrahmanian and his team have devised a new algorithm that predicts where caches of improvised explosive devices might be hidden. The algorithm was designed to discern a fine line: Stockpiled weapons kept too close to attack locations run a high risk of being blown up or targeted in military sweeps. The weapons also couldn't be too far away, because transporting explosives long distances heightens the risk of being caught. These dueling considerations push weapons caches into doughnut-shaped rings of ideal locales.

Researchers fed the program the locations of seven months of attack data and weapons caches found in Baghdad. Then the program was asked to find the best cache locations for the next 14 months of attack data. The algorithm pinpointed the weapons caches' locations to within about 0.7 kilometers — less than half a mile — of actual caches discovered by U.S. forces. The work, done with graduate student (and U.S. Army Captain) Paulo Shakarian and Maria Luisa Sapino of the University of Turin in Italy, will appear in an upcoming *ACM Transactions on Intelligent Systems and Technology*.

"We view this as not being a predictor of where attacks will occur," Subrahmanian says, "but rather, preventing those attacks from occurring." U.S. Army officials have begun using Subrahmanian's program in Baghdad.

Since these results will soon be published for everyone — including terrorists — to see, the researchers also figured out how the ideal cache location would change if terrorists know that computer scientists can predict their hiding places. In an unpublished follow-up study, Subrahmanian and colleagues found that this situation would probably push the caches outside of the doughnut-shaped comfort zone, both farther from and closer to the attack sites.

Building the perfect cell

Applying principles from game theory — the mathematical study of strategic interactions — is also useful for studying the structure of terrorist cells. Using a version called cooperative game theory, Roy Lindelauf of Tilburg University in the Netherlands and his colleagues have come up with a description of a resilient cell.

"We imagined we were the terrorists and we wanted to set up our organization," Lindelauf says. "How do these guys operate? What kinds of organizational structures do they use? How do they prevent being destroyed by governmental organizations?"

It turns out that like choosing a good spot for a weapons cache, setting up an effective terrorist cell requires compromises. The desire to remain secret prompts organizations to let as few people as possible in on the important details. If everyone knows everything, each person is a walking security risk. If just one person were captured and spilled the beans, he or she would be able to take down the entire organization single-handedly. "In a criminal organization, the people you know represent a threat," Lindelauf says.

On the other hand, the fewer people involved, the harder it is to get anything accomplished. "These kinds of organizations are bargaining with themselves," Lindelauf says. "We combine this bargaining model with network analysis, and then use that to create new mathematical techniques to predict the structure of terror organizations."

Lindelauf and colleagues analyzed graphs in which each person was a dot, or node, with links from node to node representing communication between people. This communication could be anything from smuggling weapons or fake documents to selecting targets to something as simple as a telephone call. The team found that the ideal organizational structure changes as the threat of being discovered increases. Diagrams of the structures can range from stars and reinforced rings to reinforced wheels and even reinforced windmill shapes.

"We can predict structures that resemble organization structures that we observe in reality," Lindelauf says. In the study, which appeared in *Social Networks* in May 2009, the authors acknowledge that their analysis omits some complexities, but say that even a basic understanding of network-shaping forces is important.

In a paper currently under review, the Lindelauf team has extended the network analysis to figure out what happens to the optimum network shapes when cell members are attacked. "The surprising result," Lindelauf says, "is that organizations that adopt such a structure are pretty good at withstanding attacks." These organizations will be destroyed only if massive attacks bring down most of the key players, he says. "And that's clearly not what we're doing right now."

Farley is taking a different approach to the same question of defining a perfect terrorist cell. Like Lindelauf, Farley begins with a pared-down, tidy version of reality — a small number of variables that he can work with. "I'm coming up with simple models with few assumptions and I'm openly admitting that they could be wrong," he says. "I'm not saying forget about data. I'm just saying that our assumptions are all laid out. They're simple and they're clear."

Using a branch of mathematics called lattice theory, Farley relies on the basic hierarchical nature of terrorist networks to figure out the most stable arrangement of leaders and followers. By assuming that the leaders and followers are spread out in a particular arrangement, Farley has come up with several structures for terror cells that can't be easily destroyed. In certain cases, destroying links in the network would result in the network splitting into two smaller — and still functional — networks, rather than a complete collapse, Farley's studies show.

It remains to be seen whether the models and algorithms that work so well in the lab will also work in the messy, complex real world. Subrahmanian is quick to point out that the best way to get at these hard problems will be an amalgam of many different approaches.

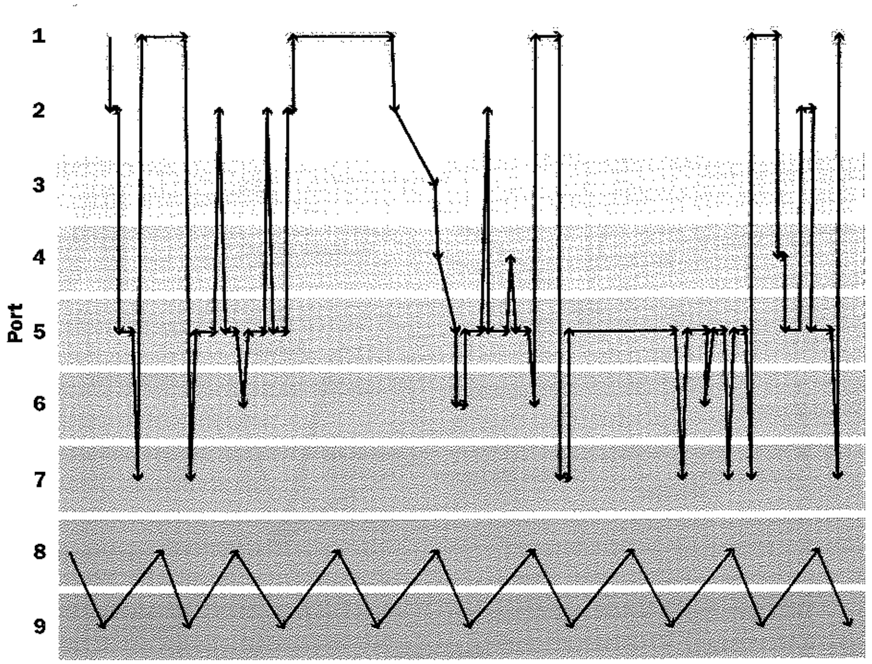
"There's got to be a collaboration between multiple disciplines — computer science, social scientists, mathematicians — in jointly trying to address this," he says. "There's still a long way to go here in translating the behaviors that are being learned to policy," he cautions. "But we believe this stuff is going to be useful." ■

Explore more

- The Consortium for Mathematical Methods in Counterterrorism website: www.rit.edu/cos/math/cmmc
- University of Maryland LCCD group: www.umiacs.umd.edu/research/LCCD

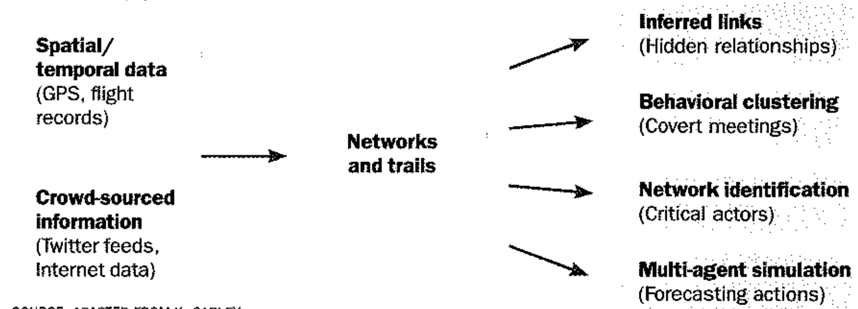
Terrorist trails Two suspicious ships sail between ports (numbered), forming trails that can be analyzed for insight into terrorist activities. One ship's trail (red line) has a very predictable pattern. The other ship's trail (black line) isn't as tidy, but still offers some useful clues. Every time the ship leaves Port 1, it goes somewhere for a quick trip and eventually ends up at Port 5.

Ship travel between ports



SOURCE: JON STORRICK AND K. CARLEY

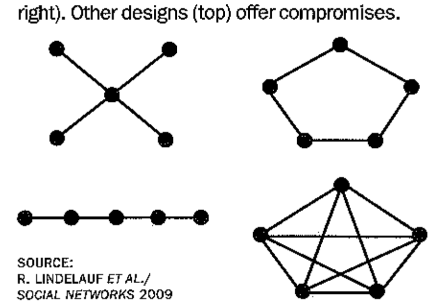
Information pipeline, from sources to uses



SOURCE: ADAPTED FROM K. CARLEY

Putting the pieces together Mathematicians are using bits of data (left) to assemble trails and networks, which ultimately can be used to forecast the behavior of terrorists (right).

Terror cell trade-off Dots representing terrorists and their relationships (lines) show how terrorist cells can be structured to balance the need for communication with the risk of betrayal. In the bottom left network, secrecy comes at the expense of information flow. When members can easily coordinate, secrecy is lessened (bottom right). Other designs (top) offer compromises.



SOURCE: R. LINDELAUF *ET AL.*/ *SOCIAL NETWORKS* 2009