AAAS
ADVANCING SCIENCE, SERVING SOCIETY

http://www.aaas.org//news/releases/2009/0324math_terrorism.shtml

News: News Archives

In Conference at AAAS, Experts Detail How Mathematics Can Shed Light on Terrorism


Roy Lindelauf

Mathematicians and computer specialists have enlisted in the effort against terrorism, using tools of their trade on such problems as modeling the behavior of terrorist cells, finding common patterns in insurgencies, sifting huge amounts of data for tell-tale connections between individuals, and assessing how communities might respond to terror attacks.

Even as scientists have used computational techniques to help policy makers understand the shadowy world of terrorism, much of their work remains theoretical—constrained by a lack of data on the targets of interest.

Learn more about the AAAS Center for Science, Technology and Security Policy.

That is perhaps understandable, given the secrecy surrounding both the terrorists and the intelligence agencies that track them. But participants at the 5th Conference on Mathematical Methods in Counterterrorism, hosted 12-13 March at AAAS, urged more sharing of information by federal agencies to help improve the computer models and analytical tools being developed by academic specialists.

"It's very hard to find good, open-source data sets," said Roy Lindelauf of the Netherlands Defense Academy. He has been using network theory to assess the tradeoffs between secrecy and operational efficiency in covert groups.

Jennifer O'Connor

The conference participants did receive a bit of a pep talk from Jennifer O'Connor of the human factors and behavioral sciences division of the Department of Homeland Security's Science and Technology Directorate. "You're working in an area right now that is huge," O'Connor said. "DHS is very interested in moving from ideas in the mathematical community" to practical applications in the real world of counterterrorism, she said.

Her division's wish-list of projects includes more research on how to detect change, whether in the structure of a terrorist network over time or changes in a person's facial expression and behavior at a security checkpoint; tools to better understand geospatial patterns in information sets; multi-camera tracking of objects; and better methods to visualize and accurately represent huge amounts of data.

DHS has been using various mathematical tools to try to model human behavior and outbreaks of violence. "It's been a useful area for us to try to pursue," O'Connor said. "What would lead a group or push a group toward violence?" The models allow analysts to simulate events over time and look for points where violence could occur.

Any effort to model the behavior of individuals must start with some underlying assumptions, said William Burns of the Center for Risk and Economic Analysis of Terrorism Events. For one thing, he said, "You have to assume terrorists are rational. We don't like their values, but they're not crazy." From such assumptions, experts can begin to craft models that might offer insight on how terror cells form, evolve and take action.

Lindelauf and others have been depicting terror cells schematically with structures called graphs. These are not the graphs of high school algebra. They are collections of dots, or nodes, that represent individuals. Lines between nodes (called edges) represent communication links or other relationships that individuals may share. Analysts look for ways to identify the network's key players, those whose capture would cause the most disruption.

Lindelauf and his colleagues tested their network model by applying it to the 2002 bombing in Bali by the Indonesian terror group Jemaah Islamiyah. The theoretical framework did well in explaining most aspects of the actual network structure that the group adopted to carry out its attack, according to an April 2008 paper by Lindelauf and his colleagues.

Alexander Gutfraind of Cornell University's Center for Applied Mathematics has been working on a simple mathematical model of terrorism that focuses on three variables: the leaders, the foot soldiers, and the overall strength of a terror group. In his analysis, he asks: What is the most effective disruption strategy? Do you go after the leaders or the followers? What happens if the organization's strength declines?

"Creating maximum short-term damage might not be the best strategy," Gutfraind said. A simultaneous decline in the group's strength and in its pool of leaders is often insufficient and effective only for the short-term. On the other hand, he said, if the pool of foot soldiers declines at the same time as the group's overall strength, the organization is likely to collapse.

While such modeling can suggest counterterrorism strategies for particular networks, Gutfraind said there is a need for real-world data on terror networks as a way to test the validity of theoretical work.

Still, specialists are finding ways to exploit the available data, both historical and contemporary. Gordon Woo, author of The Mathematics of Natural Catastrophes, has looked at efforts to interdict terrorist plots since the 9/11 attacks of 2001 in the United States. Woo said there have been more than 50 terror attacks planned in Europe since 9/11. All but two—the Madrid train bombings in 2004 and the attack on the London transit system in 2005—have been foiled, said Woo, who is with Risk Management Solutions in the United Kingdom. "That is a success story," he said. "It is hard to keep a plot secret."

Gordon Woo

Woo has used mathematical analysis to argue that "too many terrorists spoil the plot." But how many are too many? Using a method of analysis called clique percolation, Woo concluded that about 50 is the maximum number of operatives who can be actively involved in attack planning and avoid disclosure. He assumes a 10 percent chance of some linkage being discovered between any two jihadi suspects. While insider betrayal is less likely in close-knit Muslim social networks, Woo says, such networks are susceptible to data mining by security agencies looking for ostensible links between individuals who maintain close social ties.

Daniel Myers of the University of Notre Dame also has looked at some publicly available data sets. He argues that the frequency of collective violence—whether lynching episodes in the United States, urban rioting between 1964 and 1971, airplane hijackings in the 1970s or terrorist incidents more recently—can be predicted using a technique called diffusion modeling that weighs the competing forces of ideological provocation and repression in a society. "Terrorism is just another form of political violence, in my view," Myers said. "It is similar to other forms of collective violence."

George Markowsky, a lattice theorist from the University of Maine, has used order theory to take a critical look at a risk assessment tool called CARVER that is being used in the real world by 35 states and more than 100 local jurisdictions to assess the vulnerability of key resources and infrastructure facilities. Using the tool's six assessment categories, security officials can assign point scores to various assets, with the most vulnerable receiving the highest numbers. While the CARVER tool is helpful, Markowsky said, it can produce peculiar outcomes. In one case, a small monument was assigned more points than a chemical factory. The problem of comparing apples and oranges is a real one, he said. "Security is a dynamic process," Markowsky said. "I worry when people say this target is worth 390 points and it gets engraved in stone."

A common tool for risk analysis is the decision tree, a visual representation of all the events which can occur in a system. As the number of events increases, the picture fans out like the branches of a tree. The odds of a final event occurring—such as a terrorist attack on a building—will depend on the probabilities assigned to earlier events in the sequence, such as the success in penetrating a border crossing, acquiring explosives, eluding security guards and so on. Downstream events are conditioned on what happens in the preceding events. Decision trees and other types of logic trees have been widely used to assess risks in the nuclear power industry and in NASA's space program.

Barry Charles Ezell, a specialist on risk analysis at Old Dominion University's Virginia Modeling, Analysis and Simulation Center, cautioned: "If we are to represent the terrorists in the form of a decision tree, we have to understand their preferences." An analyst must make intelligent estimates on what choices a terror group might make at different junctures.

Barry Charles Ezell
[© Innovative Decisions, Inc; used with permission]

It may be a faulty to assume, for example, that a terror group wants to maximize the consequences of every action. It may prefer to pursue a lower level but more persistent level of attack. Decision trees can have value even when there is a scarcity of data, experts say, as long as the analyst's insights on likely alternatives and probabilities are sound.

Ezell said it is important for specialists to figure out the gaps in their modeling of terrorist activities. "I think the academic community can do better," he said. Ezell also cautioned that no single model can represent all of the risks of terrorism.

Beyond risk analysis and modeling, are there larger, more structural patterns in terrorism that are amenable to mathematical analysis? Neil Johnson, a physicist from the University of Miami, has used the math of complex systems to find some surprising uniformity in ongoing wars and terrorism. From the jungles of Colombia to the deserts of Iraq, Johnson and his colleagues have found that, regardless of origins and locations of modern conflicts, the insurgent groups are operating in much the same way.

Their attacks followed a power law, a mathematical relationship like those that describe natural phenomena such as gravity and the electrostatic force between electrical charges. In Johnson's model, attacks are classified according to the number of people killed. The number of attacks in any given year is proportional to the number of deaths raised to a constant power.

Johnson proposes that the insurgent force operates as a dynamically evolving population of fairly self-contained units, which he and his colleagues call "attack units." Each unit has a particular "attack strength," based on the number of casualties that typically are caused when the unit attacks. Over time, attack units either join forces with other attack units or break up. The ongoing process of coalescence and fragmentation eventually reaches a steady-state which is solvable analytically. It yields a power law with coefficient of 2.5 that holds true for conflicts in such diverse locales as Colombia, Iraq, Senegal, Peru, and Afghanistan.

"We do observe a complicated pattern that has to do with the way humans do violence in some collective way," Johnson said. He said the patterns of formation and breakup can be discerned also in the behavior of financial markets. In addition, he is interested in finding power law relationships in the behavior of street gangs and even virtual guilds that form in the Internet realm of the massive, multi-player game called "World of Warcraft."

The conference on mathematical methods in counterterrorism was organized by Jonathan Farley of Phoenix Mathematics, Inc., Anthony Harkin of the Rochester Institute of Technology, and Benn Tannenbaum of the AAAS Center for Science, Technology and Security Policy.

Earl Lane

24 March 2009