The Bulletin of Military Operations Research

MORS PHALANX

VOL. 44, No. 2 JUNE 2011 ISSN 0195-1920 • http://www.mors.org

Inside

Plenary Speaker, The Honorable John Scott Redd, Vice Admiral, United States Navy (Ret.)

Military Operations Research Society
1703 North Beauregard Street, Suite 450
Alexandria, VA 22311
(703) 933-9070; FAX (703) 933-9066
e-mail: morsoffice@mors.org
http://www.mors.org

The *Phalanx* (ISSN 0195-1920) is published quarterly, $40.00 for one year or $70.00 for two years (US Rates) by the Military Operations Research Society in cooperation with the Military Applications Society (MAS) of the Institute for Operations Research and Management Science (INFORMS). Principal office: 1703 N. Beauregard Street, Suite 450, Alexandria, Virginia 22311. Periodicals postage paid at Alexandria, and at additional mailing offices. POSTMASTER: Send address changes to *Phalanx*, 1703 N. Beauregard Street, Suite 450, Alexandria, Virginia 22311. Please allow 4-6 weeks for address change activation.

INFORMS
7240 Parkway Drive, Suite 310
Hanover, MD 21076
800-4INFORMS
FAX (443) 757-3515
e-mail: informs@informs.org

Subscriptions to *Phalanx* are included in the annual dues of both INFORMS/MAS and MORS members.

IN THIS ISSUE

Phalanx STAFF

Printed On Recycled Paper

New Models of Interdiction in Networked Systems

Alexander Gutfraind, Los Alamos National Laboratory, agutfraind.research@gmail.com

Fifty-six years ago, in 1955, General Frank Ross, formerly in charge of the U.S. Army's Transportation Corps in Europe, commissioned RAND analyst Ted Harris to solve a problem. General Ross wanted a plan for cutting the Warsaw Pact rail network in case of a hot war in Europe (Schrijver 2002). In that network, which rail nodes would need to be bombed in order to disrupt Soviet supply routes? Every possible route from the origin in the east to the battlefront in the west would have to be disrupted. Obviously, some railway lines have more capacity than others and traffic can be rerouted from damaged lines to functioning ones. Which one of the many target sets is best?

In network language, this problem is now called the "minimum cut problem": a railroad hub is represented by a node which is connected to nearby nodes using edges of some specified carrying capacities (Figure 1). The capacities correspond to the amount of cargo they can ship and also roughly to the difficulty of destroying them. The objective is to destroy some of those links so as to fully disconnect the supply nodes of the adversary from his targets. So, it was a monumental scientific achievement when Ford and Fulkerson pioneered methods for solving this problem optimally even on very large networks.

Ross' minimal cut problem was unusual in 1955, but is typical of today's battlefield. Whereas traditional battles were fought on land, sea, and air, increasingly the conflicts are set in networks: road and air transportation systems, clandestine networks, and most recently cybernetworks. Although in the past the objective was to protect your own territory or take the enemy's, today's objective is to protect your own networks while unwiring the enemy's. In the past, commanders relied on cartographers and logistics specialists, but today's strategists must also rely on network scientists. In this article, I survey recent developments in this field, or to be specific, the research presented at a session of the 2010 INFORMS annual meeting.

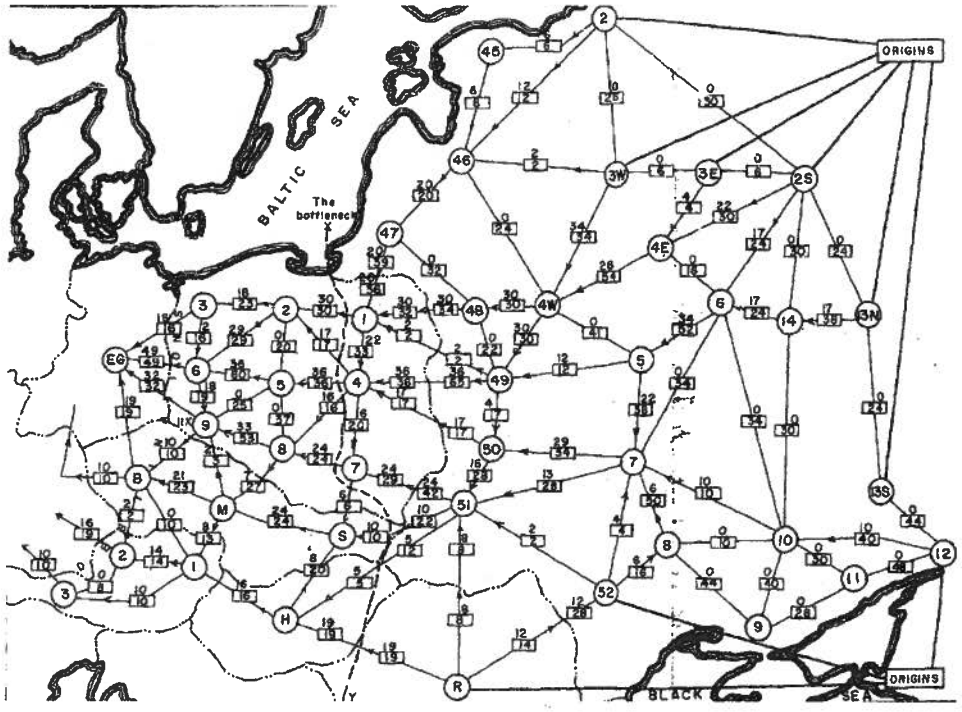

Figure 1. The East European railway network and its bottleneck, the minimal cut. From Harris and Ross (1955). Circles are labeled nodes and boxes give edge capacities (number of 1,000-ton trains per day). Numbers over boxes give the flow when the network is fully utilized as during a war.

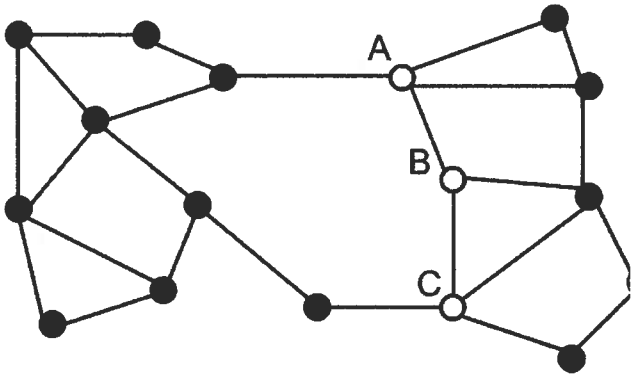

Figure 2. A connected cut is formed by nodes A, B, and C. The network could be infiltrated at A and C, then disrupted at B. When the three are removed, the left part of the network is separated from the right. Adapted from Banerjee et al. (2011).

The Connected Minimal Cut

Not every network disruption problem is like Ross' minimal cut. In a minimal cut, the disrupted edges can be far removed from each other, creating a cut through a subtle synergy. In practice, such distributed attacks might be infeasible and it is necessary for the disrupted edges to be close to each other. For example, in the case of air strikes, to make any arbitrary cut one might need to penetrate enemy air defense systems in multiple locations far from each other. Far more practical is to suppress those defenses in part of the airspace and then disrupt the network in that area. A similar penetration problem is also relevant to cyberattacks. Finally, one can consider the social terrain: in disrupting clandestine networks such as terrorist groups, it is very difficult to cut the network by arresting enough individuals because many of the actors are difficult to access. A more realistic disruption plan is

See ***SYSTEMS*** on following page...

SYSTEMS from previous page...

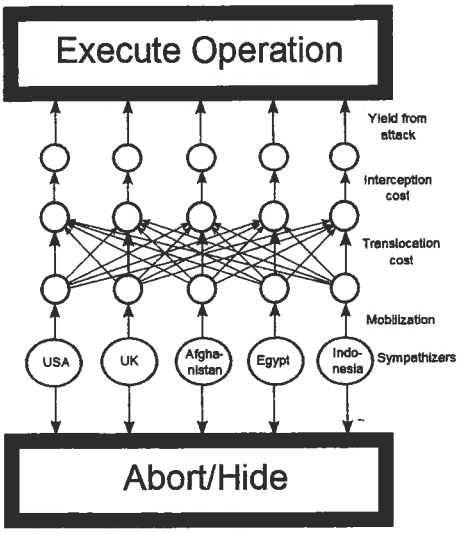

Figure 3. A small operational graph for transnational terrorists. Rows represent stages while columns represent countries. Every attack corresponds to a path from a sympathizer node in some country to the column of the country being attacked, and then to the "Execute Operation" node. The full model contains many more source and target nations.

to infiltrate the network and then disrupt or even recruit other nodes *connected* to the initial infiltration set (Figure 2).

The work of Banerjee and collaborators considers the *minimal connected cut* problem (MCC), where the network G is to be cut with minimal effort while requiring that the removed set forms a connected subgraph of G. Can such a subgraph always be found? Sadly, no. MCC is shown by the authors to be computationally hard, NP-hard (for the enthusiasts, MCC could be related to the Steiner Tree problem—the problem of building with the least cost, a spanning network between a specified set of nodes.) NP-hardness indicates that it would be computationally difficult to find the MCC on *arbitrary networks*. Fortunately, it is often possible to quickly find solutions that are good enough, if not quite optimal, even on large networks. Moreover, real-life networks are not truly arbitrary and often have a special structure. Indeed Banerjee et al. found an important special case: networks that sit on a plane (without crossing edges). In those planar networks, MCC is easy to find. This is great news because many infrastructure networks are planar or nearly so. Cybernetworks as well as social networks are usually not planar: if 5 nodes are mutually connected, the graph is no longer planar. Therefore, an obvious future project is to develop algorithms that find high-quality solutions to MCC even on nonplanar networks.

Tactical Network Interdiction

The problems considered by General Ross and Ted Harris are sensible for a total war: all the enemy's supply lines must be cut whatever the cost or collateral damage. In a limited war (or with a smaller attack force), a full network cut is not possible, and one might instead try to disrupt some of the network. Such a poor man's cut is the *network interdiction* (NI) problem (Israeli and Wood 2002). In NI, success is measured by how much more difficult it becomes to cross the network.

To give a concrete example of recent interest, imagine that the enemy is a nuclear-armed terrorist who starts somewhere on the network and wishes to reach a destination. One might be able deploy radiation sensors that detect the materials inside such a weapon, but the sensors are only feasible in some parts of the network such as border crossings. Those sensors increase the risk to the adversary and can force him to find long risky routes that bypass the sensors (see Morton et al. 2007).

Recently, Mehmet Ertem and Vicki M. Bier from the University of Wisconsin-Madison applied NI ideas to defending against cyberattacks. In their model, the network represents the "attack graph"—the set of all possible attack scenarios against the system. An attack scenario is just a path on the network that reaches from an entry point to another node—for example, secure data stored deep in the network. Each of the edges in the network has an associated success probability when traversed by the attacker. At this point, the defender deploys sensors that further reduce the probability of success. He might also install systems such as firewalls, which fully block suspected malicious traffic. The attacker and defender play a multistep game where the defender can learn from past attacks to add new sensors to the network. This problem could be represented as a multistage stochastic program. Because programs of this type are hard to solve optimally, Ertem and Bier propose a number of heuristics that help find effective interdiction solutions.

Network Interdiction of Transnational Terrorist Networks

Much of the recent work in network interdiction was motivated by problems in counterterrorism. Indeed, terrorist operations rely on networks of many kinds: the internal organization of the terrorist group is a network, and a network can represent the travel routes toward the target.

A terrorist operation can itself be represented as a network with interdependent steps: the recruitment of operatives, the procurement of weapons, training with the weapons, and so forth. An important additional problem for a transnational terrorist organization like Al-Qaida or Hizbullah is the risk of crossing international borders: getting the travel documents, learning the language, and the logistics at the remote target. They must also consider the efficiency of law enforcement agencies and the value of different targets—countries.

One could reconstruct the calculus of the terrorists, that is, rebuild their operational network (Figure 3). In that network, much of the relevant information could be estimated from public sources (if only roughly). For example, the costs of crossing international borders are indirectly expressed in the amount of tourism or immigration between the relevant countries (properly adjusting for populations and distance).

After collecting such data, one can estimate the risk to different countries—that is, the likelihood of an attack—as follows. To be more specific, suppose T_{ij} represents the risk (that is, the probablility of failure) when moving a cell from country i to country j. Also, let I_j be the risk of interception once at j, and Y_j the yield from a successful attack. Note that risks or probabilities can be converted to costs by the function $f(x) = -\log x$, which makes them comparable to the yield(note that costs are positive numbers, while yield is negative). Then "Bin Laden's" problem is to find which country j to target:

$$\min_j \{T_{ij} + I_j + Y_j\}$$

To find the total risk to any country one must also consider the supply of cells in various source countries (which could be estimated from public opinion surveys and other data). The final estimate is as follows. The United States has the highest risk of any country from international terrorism. This is simply because by attacking the U.S., a terrorist organization hopes to affect the policy of the biggest player in the international arena. Of course, in the last decade the U.S. did not stand idle and made it much more difficult for terrorists to reach its shores. So, a possible scenario in the network is one where all edges entering the US are interdicted. In response, smart terrorist groups can be expected to shift to less protected but still valuable targets. Under the assumptions of the model, such a U.S. move would not measurably decrease the volume of attacks but would deflect them, greatly increasing the risk from terrorism to every other country.

The model is consistent with the increase in terrorism in Europe following the security measures implemented over the last decade: Islamist radicals based in Europe or going through Europe just could no longer reach the US! This effect points to the need for international security arrangements, because in the current environment much of the security effort merely fuels a competition over which country is hardest to reach or has the most fortified embassies. In principle, a more effective strategy is to focus resources on stopping terrorists at their source nodes. In practice, such interdiction strategies might have unwanted effects of their own.

Weighing the costs and benefits of interdiction strategies and computing the vulnerabilities and resiliencies of networks is the task of network science. It is certain that this research area will only increase in significance as the world grows to become more and more a cake of overlapping networks.

Acknowledgements
In addition to the featured projects, Carol Meyers also contributed to the mini-symposium research related to the U.S. nuclear arsenal. Statements and opinions do not necessarily reflect policies or positions of the Department of Energy or the U.S. Government. Released as LA-UR-11-02114.

References

Banerjee, S., Davulcu, H., Ghosh, P., Sen, A. and Suomela, J. (2011), On the Minimum Connected Cut Problem and its Application in Destabilizing Networks. To appear.

Gutfraind, A., Targeting by transnational terrorist groups, in *Counterterrorism and Open Source Intelligence* (U. K. Wiil, ed.), Lecture Notes in Social Networks, Springer, 2011.

Harris, T.E., and Ross, F.S. (1955), Fundamentals of a Method for Evaluating Rail Net Capacities. Research Memorandum RM-1573, The RAND Corporation, Santa Monica, California.

Israeli, E., and Wood, R.K. (2002) Shortest-Path Network Interdiction. Networks 40(2), 97–111.

Morton, D.P., Pan, F., and Saeger, K.J. (2007), Models for nuclear smuggling interdiction. IIE Transactions 39(1), 3–14.

Schrijver, A. (2002), On the history of the transportation and maximum flow problems. Mathematical Programming, Ser. B 91, 437–445.

Author Biography

Dr. Alexander Gutfraind received a PhD from Cornell University and is currently a postdoctoral researcher at the Los Alamos National Laboratory. He develops mathematical models to illuminate problems in complex systems and counterterrorism using methods from the theories of complex networks, discrete optimization and dynamical systems.

International/Cross-Cultural Effects in Organizational Decision Making

Rafael E. Matos, Whitney, Bradley & Brown Consulting, RMatos@WBBINC.COM

There is an increased interest in the U.S. Department of Defense (DoD) in the application of cognitive psychology in decision making. The DoD fiscal year 2011 budget (Department of Defense 2010) requests that efforts seeking to understand cognitive effects of heightened sensory input continue. Research interest within the department would leverage advances in mathematics, biology, psychology, and other relevant sciences to improve informational and decision-making tools. The complexity of decisions ranges from the strategic to the tactical level—from budgetary decisions to troop employment strategies. My personal experience with DoD personnel and individuals from other agencies is that they bring certain organizational/cultural factors to decision support events that influence the manner in which the decisions are made.

For example, let us take the analysis of a notational next joint helicopter that would be used by the Army, the Navy, and the Marine Corps. The experiences of the individuals from these organizations are unique to their cultures. When placed together to decide on the capabilities the common platform (helicopter) would have, there would be some disagreement and healthy debate. Each member of the decision team would bring their own experiences and organizational objectives to satisfy service-specific goals. Depending on the manner in which the decision support event is facilitated, all inputs would be considered and would contribute to the final output.

Similarly, the backgrounds, experiences, and cultural foundations of the individuals that make up the decision team might affect the decisions made by international and multicultural teams. In tandem with the interest of the military services, the Military Operations Research Society (MORS) has dedicated additional efforts in the last few years to explore social science applications to decision analysis and the enhancement of computational social sciences. In their annual symposium, MORS has expanded topics in computational social sciences, as well as human

See ***DECISION*** on following page...