

Return to  
~~XXXXXXXXXX~~

**Document 1 of 1.**

Copyright 2001 The Washington Post  
The Washington Post  
September 17, 2001, Monday, Final Edition  
SECTION: STYLE; Pg. C01

LOOK  
@ Karen Stephenson & Kathleen Lanley elsewhere

**LENGTH:** 2604 words

**HEADLINE:** Disconnect the Dots; Maybe We Can't Cut Off Terror's Head, but We Can Take Out Its Nodes

**BYLINE:** Joel Garreau, Washington Post Staff Writer

**BODY:**

The essence of this first war of the 21st century is that it's not like the old ones.

That's why, as \$ 40 billion is voted for the new war on **terrorism**, 35,000 reservists are called up and two aircraft carrier battle groups hover near Afghanistan, some warriors and analysts have questions:

In the Information Age, they ask, how do you attack, degrade or destroy a small, shadowy, globally distributed, stateless **network** of intensely loyal partisans with few fixed assets or addresses?

If bombers are not the right hammer for this nail, what is? ✓

Bombers worked well in wars in which one Industrial Age military threw steel at another. World War II, for instance, was a matchup of roughly symmetrical forces. This is not true today.

That's why people who think about these things call this new conflict "asymmetric warfare." The terrorist side is different: different organization, different methods of attack -- and of defense.

"It takes a tank to fight a tank. It takes a network to fight a network," says John Arquilla, senior consultant to the international security group Rand and co-author of the forthcoming "Networks and Netwars: The Future of Terror, Crime and Militancy." **GET THIS**

He asks: "How do you attack a trust structure -- which is what a network is? You're not going to do this with Tomahawk missiles or strategic bombardment."

"It's a whole new playing field. You're not attacking a nation, but a network," says Karen Stephenson, who studies everything from corporations to the U.S. Navy as if they were tribes. Trained as a chemist and anthropologist, she now teaches at Harvard and the University of London. "You have to understand what holds those networks in place, what makes them strong and where the leverage points are. They're not random connections," she says.



Human networks are distinct from electronic ones. They are not the Internet. They are political and emotional connections among people who must trust each other in order to function, like Colombian drug cartels and Basque separatists and the Irish Republican Army. Not to mention high-seas pirates, smugglers of illegal immigrants, and rogue brokers of weapons of mass destruction.

But how to establish a target list in a network?

The good news is that in the last decade we have developed a whole new set of weapons to figure that out.

An industry has arisen to help corporations build new networks and junk old hierarchical bureaucracies in the age of merging and emerging companies, says Kathleen Carley, director of the Center for Computational Analysis of Social and Organizational Systems at Carnegie Mellon University. New tools have been developed that analyze how an organization interacts, yielding a kind of X-ray that shows where the key links are.

There is a general set of principles to any network, says Stephenson, whose company, NetForm, has developed software that mathematically analyzes networks. ✓

She points out that typically a network is made up of different kinds of nodes -- pivotal people.

The critical ones are "hubs," "gatekeepers" and "pulsetakers," she believes. Hubs are the people who are directly connected to the most people; they know where the best resources are and they act as clearinghouses of information and ideas, although they often are not aware of their own importance. Gatekeepers are those connected to the "right" people. They are the powers around the throne, and often they know their own importance. Pulsetakers are indirectly connected to a lot of people who know the right people. They are "friends of a friend" to vast numbers of people across widely divergent groups and interests.

How does this relate to Tipping Pt?

The classic example of how to use this analysis is "finding the critical employee in the company -- the lone expert who knows how to fix the machine," Carley says. Ironically, without network analysis, managers frequently don't recognize who that is and the nature of his importance.

"But there's no reason it can't be turned around in the opposite way," she says. There's no reason organizational glitches, screw-ups, jealousies and distrust that slow and degrade performance can't be intentionally introduced. A network's ability to adapt to new challenges can be degraded.

Carley says: "One of the things that leads to the ability to adapt is who knows who and who knows what. The higher that is, the better the group's flexibility. But you can reduce the number of times the group can communicate or congregate. Or you can rotate personnel rapidly." And in war, this may have to be done by capturing or killing them. You can also segregate the things people are doing, so they learn only on a need-to-know basis. The more isolated the tasks are, the more you inhibit their ability to function as a team.

? → # @ Q  
DOES this

software agents. When the activists check in, they can't leave without taking with them a piece of software that allows you to backtrack, getting into at least one part of the enemy network. "That likely gives you his/her all-channel connections, and maybe even some hints about hubs or the direction of some links," says Arquilla.

There are other possibilities.

"You know those little cameras that some people have on top of their monitors? Let me just say that it is entirely possible to activate those and operate them and look through them without the machine being turned on," he says.

Software also exists that "allows you to reconstruct every single keystroke. One after the other. Why is that important? If you do find the right machine, you can reconstruct everything that happens. Even with unbreakable encryption, you have all the keystrokes."

Much of this is hardly new, of course. Divide and conquer has worked for a long time. Whenever the police got a Mafia wiseguy -- Joe Valachi, for instance -- to betray the others, no Mafiosi could trust another one as much anymore. Machiavelli, in "The Prince" of 1505, wrote about the strategic deployment of betrayal to undermine trust.

What's different is our technological ability to track groups in real time and see patterns that may be invisible on the surface. "Our technology is sufficient that you can now handle realistic-sized groups. We can deal with 30 to several thousand," says Carley. "You couldn't do that before."

In 1996, Arquilla and Ronfeldt wrote a slim but highly prescient volume called "The Advent of Netwar" for the National Defense Research Institute, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Chiefs of Staff and the defense agencies.

 It predicts that in a war between human networks, the side with superior intelligence wins. It also makes some tactical suggestions about countering human networks with counter-networks that actually have been used to combat computer hackers.

They include:

\* Find a member of the enemy group who is clearly a harmless idiot; treat him as if he were the most important figure and the only one worthy of being taken seriously.

\* Single out competent and genuinely dangerous figures; write them off or call their loyalty to the cause into question.

\* Control the stories people tell each other to define their reason for living and acting as they do. The terrorist story, says Ronfeldt, "gives these people common cause -- us versus them. Right now the U.S. would seem to have the edge at the worldwide level. But within the region, there was the dancing in the streets in Palestine. Part of the story is that America's evil, and that America's presence is to blame for so many of the problems in the Middle East. We have to

attack that part."

✓ \* Find the list of demands extorted by the network; grant some that make no sense and/or disturb and divide their political aims.

\* Paint the enemy with PR ugly paint so that they seem beyond the pale, ridiculous, alien, maniacal, inexplicable.

\* Destroy their social support networks by using "helpful" but differently valued groups that are not perceived as aggressive.

✓ \* Divide and conquer; identify parts of the network that can be pacified and play them against former allies.

\* Intensify the human counter-networks in one's own civil society.

Adds Manuel Castells: "We should be organizing our own networks, posing as Islamic terrorist networks. We should then demand to join one of these networks and then destroy the trust structures. Only way to infiltrate. Oldest technique in the world."

Few of these ideas involve flattening Kabul, all of these analysts note.

Stephenson worries that massing the Navy near Afghanistan is "a symbolic show of old-fashioned strength. It's not about that anymore. This whole playing ground has shifted."

"In order to do anything, you cannot be blind," says Castells. "The most extraordinary vulnerability of the American military is it looks like they do not have many informants inside Afghanistan. It also looks like the majority of the components of this network do not relate directly or essentially to nation-states. That is new. Unless we have a fundamental rethinking of strategic matters, it's going to be literally, literally exhausting and impossible. It will be desperate missile attacks at the wrong targets with a lot of suffering. Massive bombardments turn around the opinion in many ways."

"Basically," says Ronfeldt, "you have to find somebody to wipe out."