

AT THE END OF A LONG HALLWAY IN A GRAY AND CAVERNOUS BLOCK at the University of Arizona in Tucson sits a closet-size room secured by complex access codes and bulletproof-glass windows. The room is chilled to a steady 60 degrees and crammed with rack-mounted monitors, blinking red lights, a squat supercomputer, and three “spidering machines” that crawl through the Internet, quietly spooling data from the shadowy digital realm inhabited by terrorists, hackers, and cybercriminals. Welcome to the Dark Web.

These machines store Web data from roughly 1,500 terrorist and extremist organizations, including 500 groups with roots in the Middle East, explains University of Arizona computer scientist Hsinchun Chen, who designed this digital sleuthing tool. Accessible only to those who pass fingerprinting and extensive background checks, the Dark Web project constitutes the largest collection of online terrorist data on the planet and may be key to cracking future plots. It is, literally and metaphorically, a portal to the underworld.

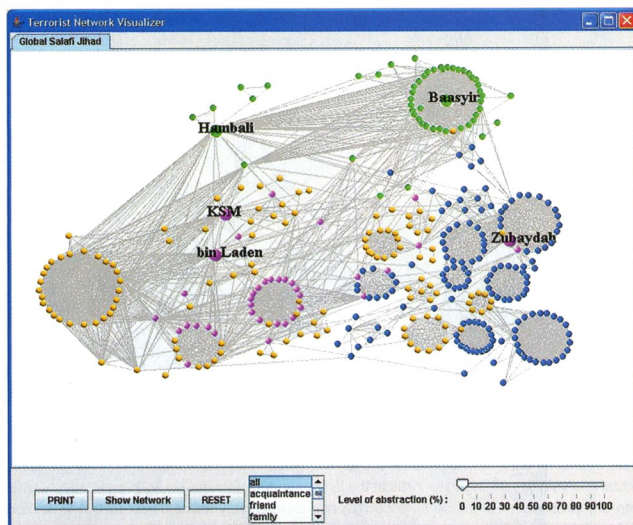
Tall and affable, Chen is just one among thousands of scientists and government agents working doggedly to infiltrate terrorist networks around the world and to disrupt their actions. The expansion of the Web and wireless technology, open-source coding, and free online storage have been a boon to terrorist organizations. More than simply a communication tool, the Web serves as a platform for e-jihad:

planning, recruitment, fund-raising, training, and indoctrination. The number of jihadist Web sites has grown from a dozen in 1998 to 4,800 today. “They know how to use the Internet in an intelligent way,” says a member of Chen’s team. “They’re hiding in the shadows,” adds Chen.

The Dark Web Project has developed algorithms for assessing the threats associated with various Web sites and forums. One is a mathematical formula that measures the “infectiousness” of ideas on a Web forum. An infectious idea is one that spreads rapidly, like a highly contagious cold. The formula takes into account such parameters as the number of postings, the volume and duration of a conversational thread, and the number of members participating. It then generates a “thread score” that is tracked over time. Some ideas peter out, while others hit a tipping point. The system also uses keyword and textual analysis to quantify and track the level of violence and racial hatred expressed on a Web site or forum—a measure that can be used to determine which groups might be most threatening and to alert investigators to follow up.

Chen’s group has also developed techniques to decipher social interactions among terrorists online. One method, called link analysis, studies the connections between Web sites and online forums to create a two-dimensional map that reveals at a glance the relationships between terrorist clusters. On a monitor, Chen calls one up. It somewhat resembles a map of airport hubs. Small circles represent individuals, some of whom are grouped into rings of teams. Lines radiate from each ring, connecting to other circles with which they are affiliated. A group’s importance can be inferred quickly from the number of lines connected to it. One ring is shaded nearly black with connections. “This was the 9/11 group,” Chen says. “In the middle here, this is Bin Laden.”

July 2006
pg. 32-42,
76



TERROR FAMILY TREE Web communications tracked by computer scientists reveal a clear network of relationships among members of terrorist groups (left). Meanwhile, videos of Osama bin Laden (right) appear on the Arabic television station Al Jazeera—a reminder that the terrorists remain one step ahead.