CNET News
Military Tech
August 24, 2009 6:23 AM PDT

Social networks--the new front in war on terror

by Mark Rutherford

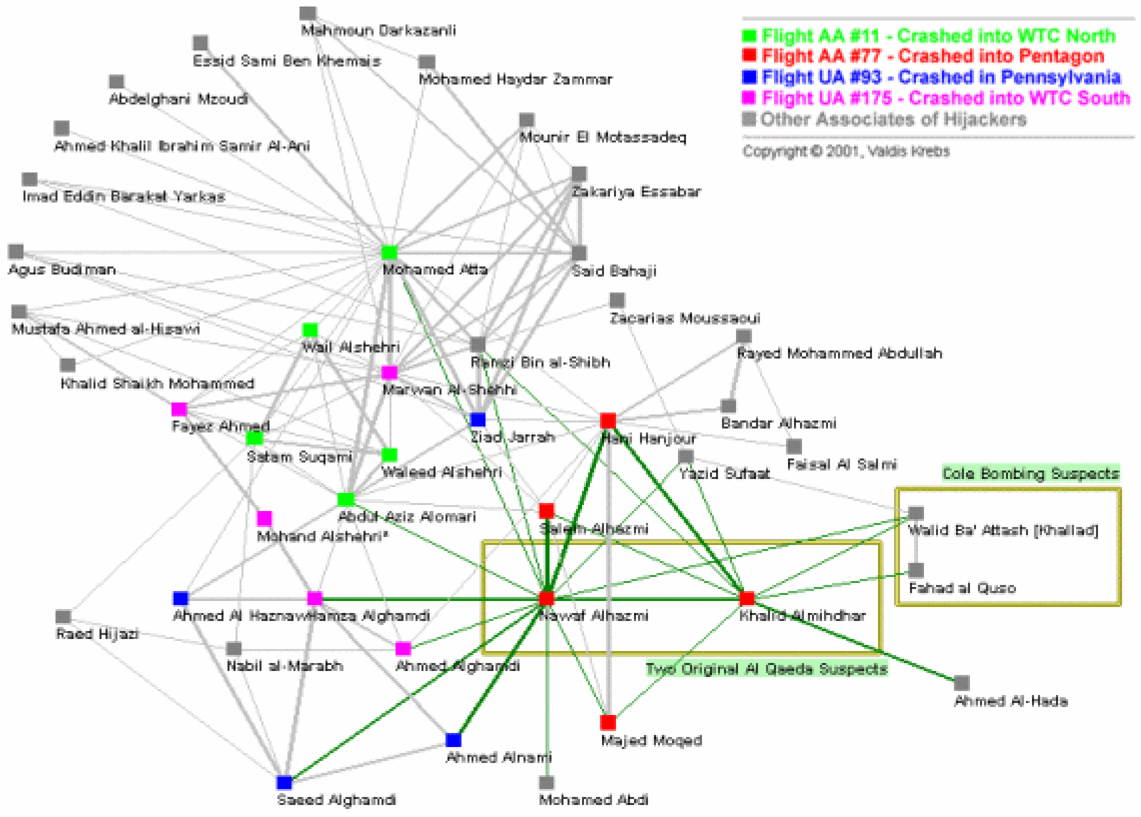

Figure 3 - All Nodes within 2 steps / degrees of original suspects

Management consultant Valdis Krebs used newspaper clippings to build a visual and mathematical picture of the September 11 terrorists' social network.
(Credit: Orgnet.com)

Unnamed intelligence agencies and certain academics have yet to give up on data mining to identify terrorists and predict attacks, despite a 352-page tome published last year pronouncing the **practice a waste of time**.

The U.S. is spending "hundreds of millions of dollars" to develop techniques to mine the mountains of information gleaned from e-mails, telephone calls, interviews with suspects, and now social networks to build-up Facebook-style databanks on international terrorists, according to a recent piece in the British newspaper, **The Independent**.

The result has been the arrest and interrogation of "many thousands of innocent people" in Iraq and Afghanistan in the hope of extracting any tidbits of intelligence that could be fed into computers programmed with social-network algorithms, The Independent's Steve Connor wrote, quoting unnamed critics.

Once compiled, analysts can sift through the data banks at their leisure using complex computer programs in hopes of identifying terror honchos and predict their moves. But this approach leads to false positives and the flagging of "ordinary, law-abiding citizens and businesses" as suspects, according to the National Research Council report titled "Protecting Individual Privacy in the Struggle Against Terrorists." Data mining is "neither feasible as an objective nor desirable as a goal of technology development efforts," the report concluded.

Despite this, "military intelligence chiefs" hope data mining will prove a new front in their war on terror, Connor wrote. And they'll do this "By analyzing the social networks that exist between known terrorists, suspects and even innocent bystanders arrested for being in the wrong place at the wrong time."

But while critics condemn the practice as being everything from wasteful and counterproductive to a gross violation of human rights, there is evidence that data mining social networks could payoff.

For instance, hackers who perpetrated many of the **cyberattacks on Georgian** government Web sites during the five-day Russian-Georgian war in 2008 were recruited by Russian language social networking sites, according to a recent study reported on here.

"Social network analysis is analysing information about who knows who or who talks to whom," professor **Kathleen Carley** of Carnegie Mellon told Connor. "What social network analysis is about is giving me the whole of the 'Facebook-style' data and saying that I'm going to analyze it mathematically to tell you who the critical people are."

In another case, a **U.S. Army major** at West Point Military Academy used social network analysis to tease out relationships between hundreds of videos of American deaths filmed in Iraq.

"The rationale for how they were related is classified so I can't give away methods (but) the interpretation was that the cluster of videos were likely to have been done by the same group," the officer told Connor. "It allowed us to look at the structure between terrorist groups and actual attacks."

Mark Rutherford is a West Coast-based freelance writer. He is a member of the CNET Blog Network, and is not an employee of CNET. Email him at markr@milapp.com. Disclosure.