UA effort sifting Web for terror-threat data

New $1.5M grant to help track how IED info conveyed
By Eric Swedlund
arizona daily star
Tucson, Arizona | Published: 09.24.2007

Terrorists use the Web as a virtual university of how-to videos for making bombs, enticing recruits and plotting attacks — but UA researchers are zeroing in on them.

UA's Dark Web project scours the Internet to listen in on terrorist chat rooms, untangle the vast network of extremist links and spot threats emerging daily.

That gives Tucson the world's largest database of terrorist-generated Web sites, a collection of more than a half billion pages, postings, images and videos — a new tool for the military and U.S. agencies to use in assessing threats.

And now the UA will use a $1.5 million federal grant to look deeper into one pressing danger: how the Web teaches extremists to set up improvised explosive devices, or IEDs, the roadside bombs often used against U.S. soldiers in Iraq.

"Our young soldiers, before they're being deployed, will know the IEDs through the enemies' eyes," said Hsinchun Chen, director of the University of Arizona's Artificial Intelligence Lab, which is three years into its Dark Web work.

UA will now get even "closer to the action," Chen said.

The Army's military intelligence school at Fort Huachuca is also working to gather intelligence on IEDs.

Officials there can't comment specifically on Dark Web, but fort spokeswoman Tanja Linton noted that the Internet makes the job of intelligence officers more challenging.

"As a rule, obviously, having a better understanding of the enemy is always a goal of military intelligence," Linton said. "The better we are at identifying terrorists, the better off we are.

"Now we're fighting people who don't wear uniforms," making it especially tough to root them out, she added.

Sophisticated analysis

The UA is collaborating with various federal intelligence agencies and essentially taking orders for what Dark Web will focus on. "The possibilities are endless," Chen said.

In cyber-terms, Dark Web is now about at version 2.5 and moving toward version 3.0, Chen said, growing savvier along with its prey.

Its success lies in the sophistication it brings to analyzing social linkages between groups and the ability to identify and track individual authors by their writing styles, Chen said.

That component, called Writeprint, helps combat the Web's anonymity by studying thousands of lingual, structural and semantic features in online postings. With 95 percent certainty, it can attribute multiple postings to a single author.

From there, Dark Web has the ability to track a single person over time as his views become radicalized.

The project analyzes which types of individuals might be more susceptible to recruitment by extremist groups, and which messages or rhetoric are more effective in radicalizing people.

In one study, Chen found terrorist Web sites and U.S. government sites are equally sophisticated on the technical level. But terrorist Web sites are about 10 times richer in multi-media content like pictures and video and also about 10 times more effective in creating a community. Terrorist sites are quick to provide answers and instruction when their users ask questions, he said.

50,000 terror sites on Web

Chen estimates there are now more than 50,000 terrorist-led or terrorism-related Web sites, with new ones cropping up every day, especially in Arabic, but also in many other languages.

At its start, Dark Web had the capability to collect and analyze Internet activity in English, Spanish and Arabic.

It's now branching out into other languages, with German and French already incorporated into the system, and Chinese, Farsi and Dutch among about 10 others in the works.

"We have to increase the sophistication of our language recognition," Chen said.

In the future, Chen envisions Dark Web moving from a research prototype into a tool agencies can use independently.

The various agencies he works with on Dark Web have their own unique uses for the data. One group is looking at which ideas are most effective in recruiting, while another is analyzing the spread of training information.

Deception-detection research

The Dark Web team, made up of about five professors and eight graduate students, isn't the only group of UA researchers bringing computer expertise to the national security effort.

Led by Jay Nunamaker, UA's Center for the Management of Information is using subtle indicators in language use, vocal qualities like pitch or pauses, and an analysis of gestures and motions to build a complex model of how people behave when they're being deceptive.

"We take those three cues and fuse them to get a signal of truth or deception," said Nunamaker, whose team, like Chen's, is within the Management Information Systems Department of UA's Eller College of Management.

The next step is to refine the project so it can adjust for different situations and cultures, Nunamaker said.

"Everybody wants a silver bullet, one super cue that will identify truth or deception, but the problem is far too complex for that," he said. "You have to identify the context you're dealing with."

The UA is expanding on the deception-detection research with three recent grants, starting with $823,000 from the Defense Academy for Credibility Analysis. Researchers also are teaming with three other universities on a $1.2 million grant to study human and social dynamics, and are working with West Virginia University on a $350,000 project to pair biometric indicators with the deception techniques.

"There's no single technique that's going to identify a terrorist," Nunamaker said. "It's with all the technologies taken together that you're going to be able to make some progress."

● *Contact reporter Eric Swedlund at 573-4115 or at eswedlund@azstarnet.com.*