

Press Release 07-118

Scientists Use the "Dark Web" to Snag Extremists and Terrorists Online

Team from the University of Arizona identifies and tracks terrorists on the Web



The Dark Web project team catalogues and studies places online where terrorists operate.

[Credit and Larger Version](#)

September 10, 2007

Terrorists and extremists have set up shop on the Internet, using it to recruit new members, spread propaganda and plan attacks across the world. The size and scope of these dark corners of the Web are vast and disturbing. But in a non-descript building in Tucson, a team of computational scientists are using the cutting-edge technology and novel new approaches to track their moves online, providing an invaluable tool in the global war on terror.

Funded by the National Science Foundation and other federal agencies, Hsinchun Chen and his Artificial Intelligence Lab at the University of Arizona have created the Dark Web project, which aims to systematically collect and analyze *all* terrorist-generated content on the Web.

This is no small undertaking. The speed, ubiquity, and potential anonymity of Internet media--email, web sites, and Internet forums--make them ideal communication channels for militant groups and terrorist organizations. As a result, terrorists groups and their followers have created a vast presence on the Internet. A recent report estimates that there are more than 5,000 Web sites created and maintained by known international terrorist groups, including Al-Qaeda, the Iraqi insurgencies, and many home-grown terrorist cells in Europe. Many of these sites are produced in multiple languages and can be hidden within innocuous-looking Web sites.

Because of its vital role in coordinating terror activities, analyzing Web content has become increasingly important to the intelligence agencies and research communities that monitor these groups, yet the sheer amount of material to be analyzed is so great that it can quickly overwhelm

traditional methods of monitoring and surveillance.

This is where the Dark Web project comes in. Using advanced techniques such as Web spidering, link analysis, content analysis, authorship analysis, sentiment analysis and multimedia analysis, Chen and his team can find, catalogue and analyze extremist activities online. According to Chen, scenarios involving vast amounts of information and data points are ideal challenges for computational scientists, who use the power of advanced computers and applications to find patterns and connections where humans can not.

One of the tools developed by Dark Web is a technique called Writeprint, which automatically extracts thousands of multilingual, structural, and semantic features to determine who is creating 'anonymous' content online. Writeprint can look at a posting on an online bulletin board, for example, and compare it with writings found elsewhere on the Internet. By analyzing these certain features, it can determine with more than 95 percent accuracy if the author has produced other content in the past. The system can then alert analysts when the same author produces new content, as well as where on the Internet the content is being copied, linked to or discussed.

Dark Web also uses complex tracking software called Web spiders to search discussion threads and other content to find the corners of the Internet where terrorist activities are taking place. But according to Chen, sometimes the terrorists fight back.

"They can put booby-traps in their Web forums," Chen explains, "and the spider can bring back viruses to our machines." This online cat-and-mouse game means Dark Web must be constantly vigilant against these and other counter-measures deployed by the terrorists.

Despite the risks, Dark Web is producing tangible results in the global war on terror. The project team recently completed a study of online stories and videos designed to help train terrorists in how to build improvised explosive devices (IEDs). Understanding what information is being spread about IED methods and where in the world it is being downloaded can improve countermeasures that are developed to thwart them.

Dark Web is also a major research testbed for understanding the propaganda, ideology, communication, fundraising, command and control, and recruitment and training of terrorist groups. The Dark Web team has used the tools at their disposal to explore the content and impact of materials relating to "virtual imams" on the Internet, as well as terrorist training and weapons manuals.

Dark Web's capabilities are also being used to study the online presence of extremist groups and other social movement organizations. Chen sees applications for this Web mining approach for other academic fields.

"What we are doing is using this to study societal change," Chen says. "Evidence of this change is appearing online, and computational science can help other disciplines better understand this change."

-NSF-

Media Contacts

Dana W. Cruikshank, NSF (703) 292-8070 dcruiksh@nsf.gov

Program Contacts

Maria Zemankova, NSF (703) 292-8930 mzemanko@nsf.gov

Principal Investigators

Hsinchun Chen, Artificial Intelligence Lab, University of Arizona (520) 621-6219
hchen@eller.arizona.edu

Related Websites

Dark Web Project Web Site: <http://ai.arizona.edu/research/terror/index.htm>

NSF's Division of Information & Intelligent Systems (IIS):

<http://www.nsf.gov/div/index.jsp?div=IIS>
