# The social science of cyberattacks

November 8 2013, by Eric Swedlund

Thwarting cyberattacks could be as much a task for social scientists as it is for computer engineers.

A unique research collaboration at the University of Arizona is working on a special NSF exploratory grant to test exactly that notion, hoping that cooperation between social and computational scientists can yield a

breakthrough.

Cybersecurity is essential for protecting national interests in terms of defense and finance, but those security needs are increasingly found in other sectors as well.

However, current defenses have limited capabilities in predicting cyberattacks or determining their sources. Brint Milward, lead investigaor of the UA's grant, says the typical understanding of cyberattacks is along the lines of studying symptoms instead of a disease.

Milward, the Providence Service Corporation Chair in the School of Government and Public Policy, is teaming with sociology professor Ronald Breiger and two colleagues from electrical and computer engineering – Loukas Lazos and Jerzy W. Rozenblit, University Distinguished Professor and Raymond J. Oglethorpe Endowed Chair – to develop models of cyberattack characteristics, classify adversarial groups according to similar features and analyze those groups using social network science.

"What we're saying from the social science perspective is don't focus on the attack. Focus on the attackers," Milward said. "Tracing where these attacks come from when they're bounced off computers all over the world is extraordinarily difficult and the best you can do is trace them back to a country. The ideal would be to move beyond that to identify the groups and their motives. A second best solution may be to identify the attackers by the kind of attack they carry out."

The researchers are integrating cyber data forensics with human-centric social network analysis, a novel approach that Milward hopes will contribute to counter-strategies down the road.

"One of the things we've done initially is classified attacks according to

the purpose, like recreation, where people just want to create trouble, ideology, revenge and profit. All those things could be the motive and if you could attach a signature, based on the techniques a group uses to any of those motives, it tells you about the kinds of people who are engaging in this," Milward said.

"What the computer scientists are able to do is analyze enormous amounts of data and from that we can look at the smaller set of data associated with these attacks. In looking at the attacks, we can infer from the nature what the strategy or motive would be and find a signature and over time we can hopefully attach that signature to specific groups."

The proof-of-concept grant will also test whether the research team's interdisciplinary approach can yield answers that have eluded individual researchers in a single academic discipline.

"Can we bring people from very different fields with very different skill sets to attack a very hard problem and are they going to be able to tell us things that other people can't?"

Provided by University of Arizona