This research paper explains how to predict the next arab spring and cyber attacks
Ira Sager

Photograph by Khaled Desouki/AFP via Getty Images
An Egyptian protester holds a sign which reads in Arabic "My age is 21 years of emergency" as riot policemen stand guard outside the parliament.

"Specific triggers for how and when instability would lead to the collapse of various regimes cannot always be known and predicted … We are not clairvoyant."

—James Clapper, director of national intelligence, explaining to a congressional committee in February 2011 that he believed U.S. intelligence agencies had done the best they could to track the Arab Spring protests.

Here's what we do know: Some incidents will incite violent protest, political and social upheaval, or set off a barrage of cyber attacks. Other, seemingly similar situations will fade quietly without whipping the masses into frenzied action. We just can't tell which events will turn ugly.

What if you could predict the dangerous incidents well in advance? Researchers at Sandia National Laboratories have developed an early warning system that will alert officials to politically motivated cyber attacks or other threatening activities around the world.

In a paper (PDF) released late last year, "Proactive Defense for Evolving Cyber Threats," Sandia researchers Richard Colbaugh and Kristin Glass outline a computer model that they claim can monitor the Internet to identify volatile situations weeks before they go south—with "perfect accuracy."

The husband-and-wife research team has been studying since 2009 how information spreading through social networks influences behavior. The pair built its model using the latest predictive analytics techniques, with a twist: Colbaugh and Glass map how widespread conversational rage is on the Internet.
Most attempts at digital precognition rely on volume. If a phrase or word is mentioned very often, it signals an emerging trend—and perhaps an opportunity. While that information may be enough for a retailer to bet that the "steampunk" look will be the next hipster fashion, it's what spymasters call "non-actionable intel." Translation: not enough detail to act.

The Sandia researchers solve that problem with software that traces the convoluted path of Internet conversations. They start by tracking how many times a specific phrase turns up, using a website that tracks memes daily—sort of an early early warning system. Their

algorithm then takes that data and analyzes the connections among social and information networks and the influence members have over one another. Their approach works, Colbaugh says, because it's a blend of social science (the power people have to influence others) and computer science (the power of Big Data).

Studying past events—34 were analyzed—the duo discovered their model unfailingly picked the situations where virtual vitriol exploded into action. "We pay attention not only to the chatter, but also the way that chatter is dispersed over a network," says Colbaugh.

The model doesn't require a big investment. The researchers typically run the program over a weekend on a $10,000 workstation.

U.S. Intelligence agencies, embarrassed by the unforeseen events that lead to the Arab Spring and historic changes in the region, have been working on open source tools (PDF) that will make them more prescient about world events. "If I'm in DOD, I'd want to be best friends with these researchers," says Marc Maiffret, Chief Technology Officer of security provider BeyondTrust.

The Sandia research is generating interest as a way to detect and track emerging social and political events. "Think Arab Spring sorts of things," writes Colbaugh, in a follow-up e-mail. There's ongoing work at Sandia on "hardening" the algorithms so the program can operate without much human supervision.

For now, there appears to be no effort to use the model to develop a defensive weapon against cyber attacks. The research, Colbaugh points out, is in the public domain and it wouldn't be difficult for a large corporation concerned about cyber attacks, say in financial services, to modify the model for its use.

The Department of Defense, Homeland Security, and Boeing (BA) are listed in the paper as sponsors of the Sandia research. The DOD and the National Security Agency did not respond to several requests to discuss the paper. Boeing, the only corporate sponsor listed in the paper, did not respond to an e-mail request for an interview.

Encouraging as the research appears, it is not designed to replace existing cyber security tools or traditional methods of intelligence gathering. It is best used to zero in on public chatter on the Web—not the modus operandi of your lone cyber criminal or a state-sponsored pro because, as John Pescatore, director of emerging security technologies for SANS Institute, points out: "They're not going to yak about it on social media."

True, but other cyber weapons do require a fair amount of yakking to launch. A favored weapon of hacktivists is the distributed denial-of-service (DDoS) attack, which is a type of attack the Sandia research tested. A DDoS attack requires coordination since it involves incapacitating a website by having lots of computers send mountains of data — effectively crashing servers, hence denying service to others. But, cautions computer security expert and author, Bruce Schneier, the Sandia model should be considered "one tool among many."

At least the research is the moving in the right direction, say security experts. "Threat intelligence can no longer be a lagging indicator," says Christopher Ling, a senior vice president at Booz Allen Hamilton, who leads the firm's military intelligence unit. Inside Booz, he says, they've been working on a similar approach. "This is a first step," he says of the Sandia work. "We need much more sophisticated analysis."

Fonte: Bloomberg Businessweek. Disponível em: <http://www.businessweek.com/articles/2013-03-04/this-research-paper-explains-how-to-predict-the-next-arab-spring-and-cyber-attacks#r=tec-s>. Acesso em: 4 Mar. 2013.