How technology could help predict terrorist attacks

June 22 2016, by Sheryl Prentice

Credit: The Conversation

The internet has become a weapon for terrorists, who use social media and other technologies to organise, recruit and spread propaganda. So is it possible to turn technology around and use it to not only catch

terrorists but predict and potentially stop terror attacks before they happen?

One thing we can do is use technology to search for patterns in the activity and language of terrorists and their supporters online. If we can spot trends that typically occur in the run up to an attack, it may be possible to automatically identify when future acts of violence are being planned. In a new study, researchers from Harvard University attempted to do just this. They used computer simulations to show how unofficial groups of online Islamic State (IS) supporters spread and grow through social networking sites and how this relates to the timing of violent attacks.

This follows research into how messages on Twitter can be classified to predict whether someone will support or oppose IS. Other researchers have used data-mining techniques on social media data to try to work out when supporters "begin to adopt pro-IS behaviour".

And others have used text analysis software to show that language patterns used by certain extremist groups differ in the months leading up to a violent attack. For example, the language may show less cognitive complexity – a more simplistic way of viewing the word – if it uses less complex structures, with more short words or sentences.

My own research with Paul J Taylor and Paul Rayson at Lancaster University has used linguistic software to detect patterns in the language used by various Islamic extremist groups and narrow down potential clues in a message. Using the method of collocation, which measures the strength of association between words or between a word and a concept, we showed you could automatically establish whether extremists' messages were portraying people or places positively or negatively. For example, some personal names were significantly associated with the negative term "agentry" (referring to people acting as enemy agents),

while others were significantly associated with the positive term "heroic".

This method could indicate potential terrorist targets by highlighting people or places to which violence or contempt is felt. For example, we might find that the terms "target", "targeting", "attack" or "kill" were strongly associated with the name of a particular place, person, or organisation. We could then look at the context of where and how these words were used in the text to work out if they suggested that person, place, or organisation may be in danger.

Other technologies

However, the limitation of this sort of approach is that it excludes attacks that may have happened without this kind of online build up. Each of these studies focuses only on a small aspect of the wider ecosystem of terrorism. So unless we can show that these patterns occur in all types of terror-related situations, we have to be careful not to exaggerate their importance and remember that other factors including political and personal situations can drive acts of violence.

Terrorists' online communications are only part of the picture. We also have ways of studying terrorists' offline communicative behaviours by measuring levels of stress or anxiety, or detecting patterns associated with deceit. For example, we can use sensors, infrared scanners and brain imaging technologies such as fMRI to monitor changes in the body or track people's face, body or eye movements. Some argue that if we deployed this kind of technology in airport security, it might alert us to those intending to carry out an attack.

In 2002, researchers at Honeywell Laboratories in the US showed how thermal imaging technology could identify a heat pattern that occurs around the eyes when people try to deceive someone. They suggested

this technique could be used to rapidly screen air travellers during pre-flight interviews "without the need for skilled staff".

Human factor

But such a system wouldn't be foolproof. There are a number of reasons why an individual may be anxious at an airport, which may have nothing to do with attempts to deceive airline staff. Perhaps they have a fear of flying. These technologies are not 100% accurate. They tend to be tested in lab-based environments and trained on fake attempts to deceive rather than in real-life situations.

Some argue that technology does not have three vital qualities that humans possess: experience, values and judgement. This means that machines may miss something that only a human could detect.

So while technology offers exciting possibilities for tracking terrorist communications and predicting attacks, it isn't a replacement for human judgement and should be used with caution.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation

Citation: How technology could help predict terrorist attacks (2016, June 22) retrieved 2 May 2024 from https://phys.org/news/2016-06-technology-terrorist.html