This website requires certain cookies to work and uses other cookies to help you have the best experience. By visiting this website, certain cookies have already been set, which you may delete and block. By closing this message or continuing to use our site, you agree to the use of cookies. Visit our updated privacy and cookie policy to learn more.

SECURITY

Disrupting the status quo: Data-driven analysis of terrorism

September 14, 2021

Aaron Tran

As any effective manager knows, you can't manage what you can't measure. Since September 11, 2001, how best to measure – and therefore manage – terrorism risk has been an ongoing quest.

Protecting people, property and information from security threats at an operational level requires reliable measurement methods as a solid foundation for security precautions, plans, policies and other responses.

Current terrorism risk assessment measurement methods rely on subjective and intuitive judgments and have questionable accuracy and reliability. Structured forms of risk assessments, like risk matrixes, create standard scores or ranks from the information input by human users. While they produce consistent and reliable results, they are only as good as the information entered into them. In other words, quality inputs produce quality outputs. The inputs to these risk assessments are subject to bias and fallacies, like all human interactions. They are, essentially, qualitative judgments translated into quantitative values.

Human flaws undermine most existing forms of measurement. Individuals tend to be overconfident in their ability to intuitively and subjectively assess risks. What's more, individual judgment is inconsistent – even when presented with the exact same situation, no two people's reactions are identical. Even experienced risk managers are likely to rely on a common human trait, that is, making judgments on the last, most easily retrievable and vivid memory or image of a particular subject. Such risk assessments are a source of risk in themselves.

Every successful terrorist attack is a failure of terrorism risk management. To maximize our chances of success, we need assessment methods driven by systematic data-driven analysis. There have been rapid advances in technological approaches to risk assessment, but to date, developments in data-driven analysis of terrorism have been largely academic.

They are also fairly high-level, looking at terrorism risk at a national or regional level rather than the very localized level required by risk managers and security professionals who are focused on risk across and within specific buildings and sites.

Academic research is helpful in identifying the root causes of terrorism at a national and regional level, typically focusing on distribution and frequency, such as how many terrorist attacks might occur in one country compared to another. This information is valuable for policymaking but has limited application for operational decision-making regarding terrorism risk.

What is needed for managers is terrorism risk assessments that establish the likelihood of an attack, its chances of success, and the extent of damage, cost, or losses. This information has very specific and significant implications for operational decision-making and management of terrorism risk, such as what additional security measures, plans and policies should be implemented.

Data-driven methods can provide these kinds of risk assessments. But absolutely crucial, they must also be *accessible* and *practical* enough to be used by a range of different organizations to inform their operational risk management decisions.

A barrier, to date, has been not only the lack of practicality in data-driven approaches but also the cost. Statistical modeling of risk is more resource-intensive than existing methods due to the need to gather and maintain databases, select appropriate modeling methods, train and test algorithms, and then interpret the results.

While the cost of developing these data-driven risk assessment systems may be relatively high, once the system is established, the per-unit cost of conducting risk assessments using data-driven methods is significantly less, while potentially providing far superior results and information.

Statistical modeling of risk is complex and requires specialist knowledge that is outside the skill set of most security and risk practitioners. However, this can be addressed by developing software that conducts the statistical analysis, with the user simply providing the required inputs.

This article originally ran in *Security*, a twice-monthly security-focused eNewsletter for security end users, brought to you by *Security* Magazine. Subscribe here.

Aaron Tran is the Co-Founder of Vardogyir. Tran has worked as a consultant and terrorism researcher on projects across critical infrastructure, energy, and government. He has worked on strategic reviews of current security policies and procedures for critical infrastructure assets. Tran graduated from the University of New South Wales where his work was recognized through several industry awards and scholarships for his research on terrorism and national security.

Get our new eMagazine delivered to your inbox every month.

Stay in the know on the latest enterprise risk and security industry trends.

SUBSCRIBE TODAY!

Copyright ©2021. All Rights Reserved BNP Media.

Design, CMS, Hosting & Web Development :: ePublishing