Modernising Risk Assessments and Building Community Resilience

Nazli Hocaoglu & Zoe Miles

Abstract:

This paper highlights the imminent enactment of Martyn's Law in the UK, which will set a global standard for counter-terrorism measures in crowded places. It underscores the need for Australia to consider similar regulations in safeguarding its crowded venues, given the global nature of terrorism. The paper introduces the concept of quantitative risk assessments using technology-based engines like the Terrorism Risk Assessor (TeRA), emphasizing their real-time, unbiased, and scalable approach to assessing terrorism risks. It also discus ses the importance of historical data, obtained from the Global Terrorism Database, in providing an objective basis for risk assessment. The paper concludes that such quantitative risk assessments can enhance security consciousness, improve preparedness, and ultimately contribute to a safer society. Incorporating these advanced risk assessment tools and embracing global best practices will empower communities to proactively strengthen their security measures and enhance their resilience against emerging threats.

The legislating of Martyn's Law that is due to be passed in the United Kingdom parliament shortly, will set a global precedent of national counter-terrorism standards for owners and operators of crowded places. This new anti-terrorism law- which will require publicly accessible locations with a capacity of or greater than 800 people to complete a compliant annual risk assessment which includes the assessment of terrorism as a viable risk – encourages consideration of the significance of regulating and enforcing the protection of people in crowded places within Australia. Six years ago, on the 22nd of May, 2017, a shrapnel-filled bomb detonated at the Manchester Arena in England, killing 22 people. Although the attack occurred in the United Kingdom, the attack was widely publicised and condolences for the victims and the victims' families was felt internationally. Recent inquiries into the terrorist attack and the security of the targeted venue found that not only did the responsible company have an inadequate general written risk assessment, but the risk assessment failed to identify terrorism as a potential hazard and to adopt the necessary security measures to reduce those vulnerabilities. The lethal, unpredictable and global nature of terrorism is an issue that is felt internationally, and with increasing amounts of people susceptible to becoming radicalised, the likelihood of a terrorist attack occurring in Australia is possible.

Traditionally, qualitative and semi-quantitative risk assessments have been conducted using the subjective descriptors of the assessor, general tick-box methods, reliant upon the knowledge of the assessor and completed according to human schedules. Although largely unenforced within

Australia, liability for the protection of users of a crowded place, be it visitors or employees alike, from a terrorist attack lies on the owners and operators of the venue. The purpose of this paper is to contribute to crowd safety within Australia by presenting the value of using quantitative technology-based engines to create quantitative risk assessments. The development of risk assessments using quantitative data to provide a mathematically accurate, real-time, and objective analysis of the risks that may impact on a location is a modern innovation which gives a new meaning to the phrase 'anytime, anywhere'. Engines, like the Terrorism Risk Assessor or TeRA for short developed by Assess Threat, uses accurate information in its analysis of a site that also allows for risk assessments to be conducted on a greater scale without necessitating the need for knowledge of the risk management process that is required of traditional risk assessment formats. By making available scalable risk assessments that can be used by anyone, anywhere at any time, it generates greater security consciousness and resilience to terrorist attacks that allows for a safer society. In depiction, this paper will discuss the conventional format of traditional risk assessments and the value in using the Global Terrorism Database as a source of quantitative data for quantitative modelling. The paper will then share the technical workings of a quantitative risk assessment and how mathematically accurate results are produced based on real-time risks that offers quantitative stability without bias. Finally, an examination will ensue about how using quantitative risk assessments increases community resilience and makes life safer and easier.

Security risk management is a structured and disciplined endeavour, which is founded on process and education in order to raise awareness of the circumstances that can cause losses. The current method of developing a risk assessment requires researching, investigating, and consulting with internal and external stakeholders. When conducted thoroughly this produces a solid background to raise risk concerns and prioritise risks for mitigation and defences to be developed and implemented. This method relies on risk practitioners to develop bespoke and customised reports. However, like all solutions, each process has its strengths and weaknesses, and this traditional method both takes time and introduces bias to the risk assessment. Bias can be easily incorporated into the assessment and just as easily undetected, such as the author of the risk assessment report may not have full knowledge of the current situation or may focus on a particular area of specific knowledge. This may be unintentional, due to time constraints, or to cutting and pasting writing techniques.

Risk assessments can also prioritise the likelihood and consequence of the risk using a range of qualitative or semi quantitative scores. Each of these methods have strengths to help the human cognitive process keep the risk in the front of their mind. Many risk practitioners accept that this is the best outcome of the risk management process as a known risk is a risk considered.

Majority of risk assessments use subjective descriptors to categorise risk likelihood and consequence typically formatted into a 4x4 or 5x5 risk matrix. However, these are subjective and oversimplified forms of assessing risks.

While risk management is good practice its regulation is not policed as an everyday law, meaning its mainly the compliance orientated organisations that apply strong risk management culture.

The direct focus of a risk assessment, whilst hopeful, presents several problems for the Risk profession. An immediate issue is the ability of the risk management industry to scale up to produce risk assessments for each event and venue with a greater visitor capacity rather than the typical yearly, or never, assessment. There are also issues regarding the quality and consistency of the risk assessments as well as the matter of who will store, check, and review the risk assessments. Next comes the consideration of how critical information in risk management plans may be provided to the authorities so that they may focus their efforts to policing the highly vulnerable and exposed publicly accessible locations whilst instigating an increase in resilience. The need for risk assessments to be produced in a timely, cost-effective, and accurate standard calls for a rethink of how technology can support such an enormous task.

The solution is quantitative risk assessments. Or, more specifically, the solution is TERA.

Terrorism presents a unique threat consisting of an active, mobile risk that maintains the ability to increase its awareness of an asset's security and target vulnerabilities in security to cause as much devastation as possible. Although terrorism in the west has declined, the threat is very real. The Global Terrorism Index report for 2023 and 2022 not only found that terrorist attacks were becoming more lethal, but in the west terrorist attacks were five times more likely to be politically motivated rather than religiously. From 2010 to 2021, domestic terrorism had increased by 357% in the United States, caused by a resurgence in, amongst others, covid-19 and 5G conspiracy theorists, and far-left and far-right extremist ideologies. However, to protect a crowded space, a site must be prepared for the idea of an attack occurring. Because the risk of terrorism is conducted by a conscious, living, breathing human, they will attack when least expected but when they have the most to gain. And so, terrorism must not be looked at as only those attacks which did occur, but also those attacks which failed, that were planned, and those individuals who could become terrorists. In 2021, ASIO stated that monitoring of far right-wing extremists accounted for 50% of their caseload, and with the rise of Neo-Nazi groups making public their existence, scope and ideologies at rallies, the depiction that although there are not many attacks in Australia or the West there is always the potential for many more is a realistic warning.

However, the more complex an attack, greater number of people killed, or atrocious manner of death leads to more widespread publishing in the media. As noted by the European Council, “the dramatic and spectacular aspect of [extreme] terrorism fascinates the general public”. The downside to this is that is does not represent the real risk that terrorism poses, but merely gives a brief glimpse of the reality. This is where historical data is important to the assessment of terrorism as a possible threat and where its use in risk assessments is valuable.

The historical data collected and used by Assess Threat in its TeRA risk assessments is of past terrorist attacks and is obtained from the Global Terrorism Database. The Global Terrorism Database, the GTD, is an open-source record of terrorist events that have been conducted around the world from 1970 and has documented over 200,000 cases of terrorism.

In situations like assessing risks, the inability to remember all current and past threats increases the likelihood of assumptions being used to bridge the gaps in knowledge. The entire process and results become subjective judgements rather than objective facts. Risks then may become underrated or ignored altogether, as was the case with Manchester Arena, the assessor did not identify terrorism as a risk in the assessment and security procedures were not updated to suit the risk. And unfortunately, the ignored risk became a reality. Because of the absence of accuracy and objectivity in concise and numerical statistics, and presence of gaps in knowledge, assumptions, and subjective biases, uncertainty arises, and when it comes to security and the safety of the masses, it does not bode well to be uncertain.

The GTD provides a concise and comprehensive record of terrorist incidents that have occurred globally. With information available regarding the date, location, type of attack and casualties inflicted, analysis of terrorism trends makes it possible to determine the threat that terrorism poses to an asset. The distance between a site being assessed and the location of previous terrorist events is merely one factor, another factor to consider is the type of target and whether this target type will result in extremists being influenced to attack a similar target type. With the use of historical data in quantitative risk assessment, the analysis of the risk that terrorism poses to an asset is based upon realistic and measurable data of events that has occurred in order to calculate the probability of occurrence at the asset.

Assess Threat provides a terrorism risk assessment known as the Terrorism Risk Assessor, or TeRA for short. The way that TeRA works is that it calculates the safety of an asset using an algorithm which requires a user to answer a set of standardised questions relevant to their asset being assessed, such as the size and location of the asset, and the safety procedures and policies that exist. The questions are developed according to recommended actions provided in the Department of Homeland

Security FEMA 452 Checklist, the United Kingdom's CPNI, the UK's Crowded Places Guidance, and the Crowded Places Security Audit developed by the Australia New Zealand Counter Terrorism Committee. The answers provided along with the location of the asset being assessed and historical data help to calculate the threat and vulnerability scores.

The threat of terrorism to an asset is mathematically defined through a threat score, which is based on a weighted average algorithm that has two components, a background risk component and site-specific risk component. The threat score is determined by applying a contra-harmonic mean to the background and site score, that is, the threat score is equal to the maximum value between the site score and background score, and the calculation of this logic starts by understanding the weights and values used in the formula. The site-specific score is determined through an informational analysis of its online presence and a web scraping process which identifies the number of results from a google custom search and the importance of the asset according to Open Street Maps. A background score is determined through analysis of historical data on the number of attacks in a local area based on the given latitude and longitude, the number of attacks in the country, and the number of attacks in the region, for instance, the number of terrorist attacks conducted in Sydney, Australia, and Asia-Pacific. The threat score is a measurement of the risk that an asset will be targeted or attacked.

The vulnerability score is used to determine an assets resilience to an attack and takes into consideration the aforementioned size, location, and security policies and procedures in place according to the answers provided by the user. Each question in the report is assigned to a pre-attack, attack or post-attack category: these are planning, deterrence, detection, prevention, protection, response and recovery. The vulnerability score is calculated according to the total number of questions answered for all the categories divided by the number of categories.

The responses collected from the questions about the asset are compared and analysed with the overall threat and attacks mentioned in the historical data which acts as the information analytics in the TERA report, and workflow automation then uses the output to create a standardised but detailed report. The use of real-time data through web scraping and historical data in TERA is significant as it recognises that terrorism target selection is an evolving and complex situation and what was an accurate threat environment then may not be correct now.

As shown in the explanation of the technical side of TERA as a quantitative risk assessment, the process itself is standardised, with predetermined question sets, values according to scores, data collected from the same sources and recommendations according to current guidance's'. The differences between each assessment depends upon the location and the answers to the assessment. This creates consistency; a stability in the assessment and report that eliminates the discrepancies that can be seen in other risk assessment formats. As previously discussed, bias is an issue that can

occur in traditional risk assessment formats, and unlike as easily as it can be incorporated int0 the assessment, it cannot be as easily detected.

Perhaps the assessor may not have extensive knowledge of particular risks or the threat environment, maybe they focus on certain risks and eliminate others, they may recall terrorist attacks inaccurately or omit details, or perhaps they act with great knowledge of all risks and as objectively as possible. The problem is that there is no way for someone, besides the assessor, to know for certain. Perhaps the results were intentional, caused by time restraints, cutting and pasting techniques or lack of extensive knowledge on specific risk topics. However intentional or unintentional, it doesn't change the fact that these techniques influence the results provided in a report to the business owners, their understanding of the risks and the security policies and procedures adopted to protect against these risks. The quantitative data obtained based on frequency and location of terrorist attacks in the local, national and regional vicinity of an asset being assessed, the public profile of the asset, and the type of asset are used to assess the risk of terrorism to the asset from which TeRA provides objective and recommended risk improvement actions to improve the preparedness, response and recovery of an asset to and from a terrorist incident. The risk that is assessed is the risk itself, not the human perception of what the risk is, or what the risk could be.

The use of quantitative data in the assessment of risk to a particular asset shows the true risk environment for that asset at that point in time. The ability to properly protect an asset is dependent upon knowing the risks and this requires complete, accurate and objective information rather than a reliance upon knowledge. The ability of any person in a company with the knowledge to answer questions on the assets size, insurance, and existing security procedures and policies to conduct a self-assessment of the asset and read the generated report without the assistance of risk management industry professionals, increases the amount of people who can be educated on risks and develop risk awareness. The TeRA report is communicated clearly and concisely, explaining the way the results were deciphered, what the results are and the meaning of those results, and what a company can do to improve. Intricate knowledge of the risk environment is no longer a necessity. The scalability of TeRA means greater availability to businesses, companies, governments, to assess sites more than the common yearly risk assessment. There is the possibility for each publicly accessible event to be assessed against possible terrorist threats and for security procedures and policies to be modified to suit the threat at that time. Greater use of TeRA will enable people at the asset, be it owners and employees alike, to learn about security, security procedures and devices which can be adopted and installed to reduce the impact if an emergent risk were to become a reality; if a radicalised person was looking for a target to attack.

To be risk aware is to understand the risks that exist, what impacts those risk can have, what security measures can minimise or prevent those risk from occurring, and looking for new risks which may arise. Quantitative risk assessments, like TeRA, provide any person the ability to become risk aware. This is vital as it is not only within crowded venues that terrorist attacks occur, and the knowledge acquired by users of TeRA can be implemented in not only professional environments, but also social environments and merely walking down the footpath in town. The greater the amount of people who are risk aware means a greater community-oriented security consciousness. A terrorist is a risk that has the capacity to be more security conscious than its target and will identify and act on vulnerabilities in security measures of a site to conduct as devastating an attack as possible. Salman Abedi, the terrorist who detonated his bomb in the lobby of Manchester Arena was found by MI5 to demonstrate some degree of security consciousness, and this, paired with the lack of necessary security measures to detect and prevent a terrorist attack, and the lack of considering terrorism as even a viable risk, was a recipe for disaster that unfortunately came true.

In honour of the 22 victims of the Manchester Arena attack, Martyn's Law will ensure the safety of the public so that loved ones can return home safely after attending a gathering. Traditional risk assessments provide an option for assessing a site and recommending risk mitigation strategies; however, it includes subjectivity, bias, gaps in knowledge and assumptions. It produces uncertainty in the risk assessment process, the report, the identified risks, and the security strategies recommended. Historical data removes this subjectivity, bias, gaps in knowledge and assumptions as it uses only that which is true, mathematically accurate and objective. Adopting technology into the risk management process eliminates the need for humans as assessors which allows for risk assessments to be conducted on a greater scale than ever before. With an estimated 650,000 incoming requests for risk assessments, we have a solution that will allow these assessments to be conducted realistically without compromising accuracy and objectivity. The solution is quantitative risk assessments, and the solution is TeRA. By taking away the need to have risk management knowledge to conduct a risk assessment, and by increasing the capacity of the risk management industry to conduct risk assessments more often, the education of risks will spread. More and more people can learn and identify what risks exist, how best to respond to those risks and how to identify new risks. This awareness of risk is not solely professional, and this is vital because it isn't only in venues who conduct risk assessments where terrorist attacks occur. As a mobile risk capable of being security conscious and using this knowledge to target vulnerable assets, terrorism is not an issue to be disregarded, because they won't forget about their target if it suits their agenda.