Risk Assessment and the Terrorist

By Karl Roberts, John Horgan

Introduction

Given the scale of challenges posed by the threat of terrorism and the perpetually limited resources available to counter terrorism, there is widespread agreement – if on nothing else - on the fact that there is an urgent need to find ways to prioritise the use of those resources. In this research note we argue that a greater consideration of the role of psychology in the development of risk assessment procedures may well be a useful tool to enable such prioritisation in a number of critical areas. It ought to be noted at the outset that there are many obvious challenges facing efforts to design risk assessment tools. Questions necessarily emerge about who needs to be assessed for risk and additionally - stemming from the conceptual confusion over what is meant by terrorism, and by extension, *extremism* - we might also wonder what is being risk-assessed? And finally then, we might ask what factors are related to the level of risk posed, and how we might identify these. At present we do not have complete answers to all of these questions, but this research note aims to explore some of these issues as a first step in the design of risk assessment tools for development in counter-terrorism.

Definitions

The term *risk* is generally associated with the likelihood of danger or harm. In the context of offense, harm may incorporate physical, sexual and psychological damage inflicted upon an individual or group of individuals by a particular event or events. It therefore follows that a *risk assessment* is a projection of the likelihood that a hazard, i.e. a harmful behaviour, or event, will occur. Additionally, other terms such as "dangerousness" have also been used in discussions of risk and refer to particular individuals or even groups of individuals who present a high risk of harm to others. While the goals of risk assessment may reveal different functions depending on the specific settings in which they are used, in general risk assessments are tools adopted to make the best possible predictions about future events in order to minimise the harm to others.

Hazard Identification

In discussing what risk assessment entails, a number of important factors need to be considered. The first is referred to as *hazard identification*. This involves a clear and unambiguous specification of the nature of the hazard. Within the field of psychology, the hazard is usually the behaviour that is likely to cause harm. For example hazards might include a physical or sexual assault, the use of firearms, verbal insults etc. It is important to clearly identify the hazard so that the end users (e.g. security analysts) of the risk assessment clearly understand the predictions (or hypothesis) stated.

In the case of terrorism, proper hazard identification is critical as there are many potential hazards to consider. As with defining what is meant by "crime", there are multiple behaviours and activities that could reliably constitute "terrorism." Terrorism can encompass extortion, bombing, activities associated with the preparation of bombs, shooting, arson, and a variety of other diverse behaviour. Given this, a wide range of risk assessment may be possible, and as such we might for example seek to examine factors that increase or decrease the likelihood of terror group *membership*. At another level we might also be interested in the hazard a terrorist group or an individual member of a terror group presents in terms of the likelihood of a terrorist *attack*. At another level still, we might be concerned about the risk of occurrence of *particular* expressions of terrorist violence, for example, whether we are likely to see shootings or suicide bombings by a particular group.

Doubtless, for each of these hazards there are a number of shared and specific risk factors that may raise or lower the risk of the particular hazard. Moghaddam has identified a metaphor of terrorist engagement that suggests the presence of various levels of involvement. [1] The factors he describes as being associated with different levels of involvement can be considered as risk factors for progression into and through terrorist organisations and this may well form a useful starting point in specifying risk factors associated with particular types of hazard in this context. Similarly, Horgan presents a model of involvement in terrorism that is based upon the identification of risk factors for initial involvement, but develops Moghaddam's metaphor by distinguishing

between the factors that govern involvement and those factors that govern engagement in terrorist activities. [2] The factors that predict involvement, and the qualities that govern the progression to deeper and deeper levels of commitment, may not necessarily have a bearing on the ways in which individuals come to engage in terrorist activity. The significance of this issue in understanding how risk (broadly speaking) may be conceptualized, is critical. In criminological terms, these distinctions are not new (e.g. Clarke and Cornish)[3] but they have rarely been applied to thinking about terrorists (with some exceptions, e.g. Taylor)[4].

Frequency of a Hazard

Another important issue in risk assessment is the predicted frequency of a given hazard within a specified time frame. This essentially refers to how often a hazard is likely to occur within a period of time. It is important to clearly specify the time frame under consideration because different durations of time are likely to be related to different levels of opportunity to commit offenses. For example, a forensic psychologist compiling a risk offense report for a parole hearing would typically be interested in the likelihood of the individual committing another offence within, say, six months, two or even ten years of release from prison. All other things equal, the longer the time frame, the greater the opportunity the offender may have to offend, so six months may offer fewer opportunities for re-offense than, say, two years. Furthermore, when considering the time frame it is important that the predicted frequency of the hazard is set within a time frame that is practically useful. Over a large time frame the hazard may be unmanageable. For example, a prediction that an individual is likely to carry out an offense, say, a bombing, some time in the future is likely to be less useful in managing a risk and in prioritising resources than a prediction that there is a high likelihood of a bombing within a clearly specified time frame, like six months. In the context of terrorism the time frame may be of additional importance given that terrorist groups on occasion may work towards specific dates, e.g. specific anniversaries. Although the date may be several years in the future, the risk of offense does not diminish with time but increases as the key date approaches.

Similarly, the terrorist group may engage in other activities in support of the future event, e.g. activities designed to obtain required funding, collection of weapons, identification and training of recruits to carry out the attack, surveillance of target sites etc. Each of these supporting activities in themselves could be a hazard that may be subject to additional risk assessment.

Problem of Low Base Rates

One of the difficulties in violence risk assessment in general is the problem of low base rates. Essentially what this means is that the hazard in question is not very common relative to other forms of behaviour. For example, the base rate for homicide in the United States in 2005 was 6.1 cases per 100,000 people. In comparison, the rate for major cardiovascular diseases was 277.3 cases per 100,000 people and an overall premature death rate by all causes was 798.8 cases per 100,000 people. [5] Homicide then is relatively unlikely compared with other risks to life. In a similar vein, terrorist acts have a low base rate. For example in 2005, 56 US civilians were killed as a result of terrorism which leads to an estimated death rate due to terrorism of 0.019 cases per 100,000 people (assuming a United States population of 295,500,000 in 2005). [6] Terrorist violence may therefore be considered to be a relatively rare event, despite the potentially enormous consequences it may bring. With a low base rate hazard, a statement that it is unlikely to occur is likely to be an accurate reflection of its likelihood; however such a prediction may not be very useful as it does nothing to allay public fear and is of little use in attempting to manage what risk there might be.

In addition, and related to the point above, the risk management issue only becomes meaningful when we accept that terrorist events only represent the tip of the iceberg. The successful terrorist event - for example, a bombing - will only happen because it is sustained and enabled through a series of informal but related activities.
Risk assessments therefore need to be mindful of their usefulness and specificity in the light of unlikely events. A rare event may be of low frequency but being able to suggest those factors that increase or decrease its likelihood and ultimately how likely it is, may enable law enforcement to plan more effectively. In any event, this also highlights how a narrow focus of what constitutes “terrorism” may in itself be one of the most obvious obstacles to risk management.

Dynamic Risk Assessment

Hazards are part of the social world and are not separate from it; as such there may be risk factors that serve to

raise or reduce the likelihood of a hazard occurring that may change over time. There are two broad classes of these risk factors - *static* risk factors and *dynamic* risk factors. Static risk factors are factors that do not change over time. These are typically historical or categorical factors, for example, the gender of an individual, features of their childhood, e.g. family discord, periods spent in local authority care, nationality, date of birth, experience of abuse during childhood, etc. Dynamic factors, on the other hand, do change over time and these can be under or outside the control of individuals. For example, the availability of weapons and explosives, changes in social support for an individual and/or a particular group, activities of security forces etc. A risk assessment therefore needs to consider both static and dynamic factors. To illustrate, in the context of violence risk assessment, a commonly used risk assessment tool is the HCR20 Violence Risk Assessment Scheme.[7] This was designed to assess risk of violence for individuals with a mental or personality disorder. The HCR20 assesses an individual's propensity for violence across a range of ten static (historical) and ten dynamic (clinical and risk management) factors. **Table 1** lists the relevant risk factors.

Table 1: HCR20 Risk factors for violence (Webster, Douglas, Eaves, & Hart, 1997).

Historical Factors	Clinical Risk and risk management
Previous violence.	Lack of insight.
Young age at first violence.	Negative attitudes.
Relationship instability.	Active symptoms of major mental illness.
Employment problems.	Impulsivity.
Substance use problems.	Unresponsive to treatment.
Major mental illness.	Plans lack feasibility.
Psychopathy.	Exposure to destabilizers.
Early maladjustment.	Lack of personal support.
Personality disorder.	Noncompliance with remediation attempts.
Prior supervision failure.	Experiencing stress.

As may be seen, the static or historical factors are unchangeable as they are events and characteristics that are in the past, whereas the dynamic, clinical and risk management factors, may change, e.g. the individual may find social support by starting a new relationship or may no longer be experiencing the symptoms of major mental illness. Risk management strategies may also serve to change these dynamic factors; for example, an individual may be placed in an environment where they are unable to experience destabilizers such as drugs or alcohol thus reducing risk of violence.

Specific Risk Factors

In addition, for any given hazard there are risk factors that will increase and others that will decrease the likelihood of a hazard occurring. A risk assessment therefore needs to be sensitive to both types of risk factors and the degree to which they impact the likelihood of the hazard occurring. All too often in risk assessment the focus is upon factors that raise a hazard's risk whilst neglecting factors that reduce risk. This is illustrated by reference to the HCR20. For example, a previous diagnosis of Psychopathy significantly raises the likelihood of an individual to be violent in the future. In contrast, should the individual become involved in a close relationship with someone whom they develop a close and mutual affectionate attachment with, the risk of violence is likely to be reduced because the individual may now have some form of social support (a lack of social support being a risk factor for violence). To appreciate how this may be relevant to understand risk as it applies to the

terrorist, the availability of weapons and explosives may increase the risk but a change in the public image of the terrorist group, dwindling membership and reduced community support may all serve to reduce it. Further research is likely to be able to further illuminate the relationship between differing factors and types of terrorist risk.

Repeated Risk Assessment

Dynamic risk factors, by nature, change over time. This means that that the risk may rise or fall with changes in an individual's behaviour, circumstances and the specific risk management strategies being employed. Therefore it is desirable that risk assessments are carried out on a regular basis to reflect these changes. As a very simple example, a terrorist group may present a lower risk of carrying out an attack in the absence of explosives; however the risk that they pose will change should they somehow acquire them. It is important to acknowledge here also the possibility that the absence of certain types of weapons may be influential in the development of other forms of threat by the terrorist group. The need to obtain funds with which to purchase explosives or weapons, for example, may increase the risk of the group carrying out the supporting criminal activity. Risk assessment thus needs to be an on-going process that is sensitive to the emergence of new forms of threat. The difficulty with on-going risk assessment is of course identifying when to carry out each assessment - should this be hourly, daily, weekly, monthly etc? Unmistakeably, the regularity of a risk assessment needs to be determined by the particular circumstances of the group or individual of interest. For instance, terror groups evolve over time. Sometimes they may be very active in response to events, at other times - due to changes in membership, the attitude of the greater society, and the particular expressions their activities take – their level of activity may be reduced or change in nature, frequency or scope. More regular risk assessment should be made for groups or individuals that are known to be particularly active at any given time. It may be that for certain individuals, the risk assessment may need to be done on a daily basis due to identified intentions to act. Essentially, it follows that any risk assessment should be flexible and related to the demands of the particular circumstances.

Modelling Risk

A part of the development of risk assessment tools is the production and testing of models of a specific hazard risk. A risk model will specify the precise relationship between risk factors and the occurrence of the risk. Usually different risk factors will have different types of relationship with the specified hazard. Some risk factors may have a positive relationship with the hazard such that identifying the presence of that risk factor increases the likelihood of the hazard occurring. Sometimes the relationship will be negative, indicating that the occurrence of the risk factor serves to reduce the likelihood of the hazard occurring. Also, risk factors are likely to have different strengths of relationship with the particular hazard so that the presence of some factors will have a greater effect upon the hazard occurrence than others. By way of an example, regular drug use is positively correlated with risk of violence, serving therefore to *increase* the risk of violence whereas the existence of an extended social network of friends is negatively correlated with risk of violence, serving to *reduce* the risk of future violence. Drug use has a stronger association with risk of violence than does an extended social network so that where regular drug use is identified, even when an individual has an extended social network, the risk of violence will increase but not by as much as if the individual had no social network. Hence the risk model can help identify not only which factors impact a hazard risk, but in which ways they impact it and how they collectively combine to change risk.

A risk assessment based upon a particular risk model may be helpful in counter terrorism activities by identifying which risk factors are most influential in changing the level of risk. This could be useful in prioritising resources relevant to the specific risk factors. By way of a simple example, a risk assessment model may specify that increasing the number of members of a group increases the likelihood of a terrorist attack and that this has a greater contribution to increasing risk than, say, the amount of money the group has access to. In prioritising resources it might therefore be opportune to target recruitment activities as opposed to financial activities. The challenge of course is to generate and test appropriate risk models for the various hazards relevant to counter-terrorism.

Risk Assessment Tools for Terrorism

The creation of empirically valid risk assessment models for aspects of terrorism that can form the basis for risk assessment tools is likely to be a useful enterprise. Risk assessment tools such as HCR20 have shown promise and proved their worth in a range of fields related to harm reduction. For example, the police in the United

Kingdom have made use of risk assessment tools for the prediction of domestic violence and have identified reductions in the number of cases of domestic murder since the introduction of such tools. In prison settings, risk assessment tools are being used to predict harmful behaviour such as sexual violence, stalking and physical violence and have had a significant impact upon decision-making at parole hearings and in creating risk management strategies for offenders on release from prison. The most successful (in assessing the risk of the hazard) of these risk assessment tools are evidence-based, derived from empirical research that has identified significant risk factors and the relationship that they have with the particular hazard. However, in the case of terrorism although some researchers have produced models that implicitly suggest potential terrorism risk factors, to date there has been little systematic study of the specific relationship between these risk factors and aspects of terrorism. Such research is vital as a prelude to any attempt to create useful risk assessment tools for terrorism.

Of course one of the underlying problems in attempts to conceptualize and devise such tools is in the identification of the hazard – what would a terrorism risk assessment tool seek to predict? Depending on our ability to conceptualize the relationships between the core factors outlined in this research note, this could be in a number of areas, including the risk of a given individual seeking involvement in a terror group, the risk of a group engaging in violence, the particular risk of violence an individual poses or even the risk of particular types of violence (bombings, suicide attacks, WMDs etc.) posed by an individual or group.

Context of Risk Assessment

In devising risk assessment tools for terrorism another important issue relates to the context in which the risk assessment tool is to be used. An understanding of the importance of context places particular requirements and constraints upon risk assessments. This applies especially in terms of the purpose of the risk assessment, in the types of information that are available to influence the risk assessment and in the capacity of individuals to those charged with carrying out the risk assessment. For example, in prisons, risk assessments might be required to aid parole decision-making and might seek to identify the risk an individual poses on release over some specified time frame. In the context of law enforcement the need may well be different, for example, to identify the risk of specific types of violence in the immediate future.

In different contexts, different types of information may be available. In prisons, reports from mental health professionals and prison staff might be available, and would typically be expected to include reports from interviews and psychometric assessments of the individual. Supporting these would sometimes be accounts by prison staff detailing their observations of an individual's behaviour over a significant period of time. Other information on the nature of the offenses an individual has committed and details of an individual's background and lifestyle would also be expected to be available. Together these amount to a significant collection of behavioural information. In contrast, law enforcement personnel are unlikely to have at their disposal such a rich source of behavioural information about a given suspect. They may have details of behaviour from observations and details of the individual's interests and activities from surveillance and reports of informers, but this is likely to be relatively narrow and limited. Given this, risk assessment tools need to be mindful of the sorts of information that is likely to be available to those doing the assessment, and their ability to ascertain significance in and out of all apparent contexts.

Additionally, the capacity of individuals in a particular context to carry out the risk assessment needs to be considered. In prison a risk assessment could legitimately require the assessor to interview an individual as part of the assessment. In the law enforcement arena this might prove difficult if not impossible – some jurisdictions would certainly not allow law enforcement interviews with individuals who were not under arrest not to mention the risk of compromising intelligence operations by carrying out such interviews. Therefore, it is likely that very different kinds of tools will need to be designed for use in different contexts.

Risk Management

While the identification of risk factors and their relationship to a hazard might be an important step towards conceptualizing the hazard, a risk assessment in itself is of limited use in reducing the likelihood of a hazard occurring. For this reason it is generally expected that risk assessment and risk management would be closely related. Therefore risk assessment needs to be the first stage in the development of risk management strategies. In essence a risk management strategy involves a plan for implementing actions that may be taken to minimise the likelihood of the hazard occurring. In managing risk it should not be forgotten that there are risk factors that serve to *increase,* i.e. factors positively related to, the likelihood of the hazard occurring, and factors that *de-*

crease, i.e. factors negatively related to, the likelihood of a hazard occurring. A risk management strategy may therefore attempt to mitigate those factors increasing the risk and perhaps encourage those factors that reduce the risk. In the context of terrorism, mitigating factors that may increase risk might include attempts to actively disrupt a terror group's ability to recruit new members, infiltration of the group by security forces, disruption of its capacity to obtain weapons, capture of group members and strengthening defenses against terrorist activity. Encouraging factors that serve to reduce risk may include, for example, encouraging the wider society to report suspicious activity, attempt to persuade members of society not to join terror groups, and increasing the rewards of non-participation in terror groups. It is therefore desirable, and sensible, that risk assessment be couched within an approach to risk management where risk assessment specifies the hazard and factors related to its occurrence and a strategy is devised to mitigate or protect against it.

Conclusion

This research note has considered a variety of issues relevant to thinking about how risk assessment as conceptualized in forensic settings might relate to the development of tools to assess and ultimately manage terror risk. In considering the relevance of these issues for terrorism, it is important not to be distracted by the feature differences of the contexts driving the current examples (e.g. forensic settings), but to see how the consideration of which risk issues are conceptualized provides us with the basis of a framework for developing risk assessment tools that may have similar positive impacts in the context of terrorism. Certainly if tools could identify risk factors for involvement in terrorism, on varying levels, this may aid counter-terrorism work in designing strategies that impact those risk factors and contribute to the prioritisation of resource allocation in planning exercises. Similarly, identifying those factors that make attacks more or less likely could aid in targeted counter-terrorism strategies. Risk assessment of those convicted of terrorist acts whilst in prison could certainly inform parole decisions and may inform methods of risk management should they be released.

Taking the points raised within this research note together, an agenda for research in terrorism risk assessment begins to emerge. In designing risk assessment tools an important first step is conceptualising the risk - exactly what hazard is being assessed? Once this important question has been answered, the next phase is to develop empirically valid risk assessment models linking risk factors to the hazard. Once generated, risk models will specify which factors need to be considered in designing risk management strategies and how the degree of risk will be altered by changes in specific risk factors. The design of risk assessment tools in counter-terrorism will need to be informed by relevant theory and empirical research. The research will necessarily require the collection and consideration of data describing various risk factors so that relevant factors and their precise relationship to the hazard in question can be derived. This is an area in which collaboration between psychologists skilled in forensic risk assessment and practitioners working within counter-terrorism can collaborate towards mutual benefit with the sharing of ideas, data and research methodology. Potential benefits for the researcher include an opportunity to study factors relevant to the aetiology of different terrorist behaviour; for the practitioner: empirically valid tools to be used in countering terrorist activity. Certainly, there does appear to be a need for psychologically informed risk assessment tools as part of counter-terrorism strategy. The experience from other spheres of criminal justice indicate that evidence-based, empirically valid risk assessment tools not only aid resource prioritisation but can aid attempts to manage a variety of diverse hazards.

Karl Roberts *is Director of the Centre for Investigative Skills at the University of Sunderland, a Chartered Forensic Psychologist of the British Psychological Society, and is accredited by the United Kingdom Association of Chief Police Officers as a Behavioural Investigative Advisor. He has considerable operational experience working with the police as a Forensic Psychologist.*

John Horgan *is Director of the International Center for the Study of Terrorism at Penn State. His forthcoming book Walking Away from Terrorism: Accounts of Disengagement from Radical and Extremist Movements will be published by Routledge at the end of 2008.*

NOTES:

[1] Moghaddam, Fathali, "The Staircase to Terrorism, A Psychological Exploration," *American Psychologist*, 60 (2) 2005.
[2] Horgan, John (2005). *The Psychology of Terrorism* (London: Routledge).
[3] Clarke, R.V.G., and Cornish, D.B. (1985). 'Modeling offenders' decisions: A framework for research and policy', in M. Tonry and N. Morris (eds.), *Crime and Justice: An Annual Review of Research, Volume 6* (Chicago: University of Chicago Press).
[4] Taylor, Maxwell (1988). *The Terrorist* (London: Brasseys).
[5] National Center for Injury Prevention and Control (2008), *WISQARS Injury Mortality Reports*.

[6] United States Bureau of Justice Statistics (2006).
[7] Webster, C., Douglas, K., Eaves, D., & Hart, S. (1997). *HCR-20 Assessing Risk for Violence: Version II*. Burnaby, British Columbia: Mental Health, Law & Policy Institute, Simon Frazier University.