Assessing Terrorist Risks: Developing an Algorithm - Based Model for Law Enforcement

Frederic Lemieux, James L. Regens

Abstract

Assessing the risk posed by terrorist groups has always been a challenge for national security intelligence analysts. The most noticeable obstacles are, on one side, the limited availability of reliable information about violent groups and, on the other side, the absence of objective as well as rigorous assessment methods. This paper aim to outline the basic principles of a risk-based approach to terrorism threat assessment, which integrates algorithm models in order to provide more accurate situational awareness and orient strategic decision-making process. This paper is divided in three sections: first we introduce the readers to the objectives of strategic terrorism risk assessment. Second, we provide a comprehensive critic of existing terrorism threat assessment. Third, we develop an alternative logic model based on several factors related to the threat, vulnerability and uncertainty (error term). Finally, the paper suggest a methodology that takes in account the integration of risk factors drawn from theoretical and "real life" law enforcement perspectives.

Keywords

Terrorism, Risk Assessment, Law Enforcement, Strategic Analysis

Introduction

The U.S. Department of Homeland Security (DHS) has implemented numerous anti-terror countermeasures in response to perceived threats over the past decade, and efforts are underway to develop others. Unlike natural or accidental man-made disasters, terrorists are adaptive and may shift their tactics, techniques and procedures (e.g., attack strategy) when countermeasures are employed. Moreover, when confronting adaptive adversaries, defenders also often have to operate under resource constraints including limited information for modeling terrorism risk. For example, understanding and assessing adversarial behaviors requires insights into motivations, intentions, and capabilities, but garnering those insights is difficult because we rarely can collect information directly from terrorists. As a result, assessing the risk posed by domestic and international terrorist groups and 'lone wolf' actors operating outside the context of formal groups is a daunting challenge for law enforcement intelligence analysts. Currently referred to as the "intelligent adversary" problem, the ability to estimate reasonable and defensible occurrences (or at least relative probabilities) for terrorism events is an important focus for research.

There are two critical obstacles that must be overcome to derive credible estimates to guide homeland security and law enforcement agencies: (1) the limited availability of reliable information about threatening groups or individuals; and (2) the need for rigorous objective and practical assessment methods. This paper proposes to surmount these barriers by identifying key metrics to design an algorithm-based model that facilitates integrating risk-based terrorism threat assessment into situational awareness and strategic decision-making for counter-terrorism (CT) strategies at the law enforcement level. The paper focuses on combining rigorous scientific research with law enforcement experience to design and calibrate the algorithm-based model. The proposed model can enhance intelligence sharing from the tactical/operational level to the strategic level by generating a common operating picture (COP) of the threat environment. Finally, a risk-based assessment using robust algorithm model can accelerate and validate decision-making to identify, assess, and implement CT strategic priorities by law enforcement agencies.

The long-term goal of this model is to develop effective intelligence-driven CT strategies that can help law enforcement to prevent attacks though identification of key variables related to engagement in terrorist activities, thereby enhancing the capability of analysts to 'connect the dots'. This application's objective is to assess the utility of algorithm-based models by integrating risk-based terrorism threat assessment into situational awareness and strategic CT decision-making by drawing on parameters outlined by law enforcement. Our central assumption is that a mathematical model that incorporates key variables identified through a combination of expert judgment grounded in field experience and empirical data can aid intelligence analysts in assessing the risk, prevalence, and trends of terrorist activity.

The relevance of this paper is rooted in the importance of analytical frameworks to generate strategic intelligence. Because formal or informal threat assessment techniques frame judgments about risk, the 'lenses' that analysts employ play decisive roles in developing actionable intelligence, making them the key to identification and disruption of terrorist planning (George and Bruce, 2008; Heuer, 1999). This underscores the inherent centrality of the analytical tools with which indicators and warnings are identified, interpreted, and placed into context.

Background

Ten years after the tragic attacks of September 11, 2001, the United States still remains at risk of being targeted by political violence at home and abroad. The past decade has revealed important lessons learned about deterring and/or preventing our adversaries from initiating successful terrorist actions. Retrospective analyses

underscore the effectiveness of the US intelligence community's CT activities as critical components in achieving success thus far. Since 9 / 11, most of those CT efforts have been focused on thwarting al-Qa'ida's (AQ) strategic reach at the international level; diminishing its operational capacity at the regional level (i.e., Afghanistan, Iraq, the Maghreb, Somalia, Yemen); preventing successful attacks at the domestic level; and, ultimately strategically defeating al-Qa'ida as a terrorist threat. The killing of a number of senior operatives including its leader, Osama bin Laden, provides a hopeful indication that the threat posed by AQ Central (the core al-Qa'ida group concentrated in Afghanistan/Pakistan) may be weakening. However, despite the elimination of many key al-Qa'ida members, its adaptive nature and ability to launch operations – including Afghanistan, Pakistan, and al-Qa'ida 'franchises' in countries like Yemen– has lead the Office of the Director of National Intelligence (ODNI) to categorize this violent group as an unacceptable risk to national security. Additionally, the risks posed by self-radicalizing groups and individuals including right-wing terrorists have become more apparent, further boosting the need for more accurate and reliable assessment.

Governments have responded to these challenges by applying techniques grounded in the intelligence-led policing model (ILP) to assess terrorism threats (Lemieux, 2006; Lemieux, 2008a; Lemieux, 2008b; Verfaille and Beken, 2008). Threat assessment is intelligence-driven, aims to provide a comprehensive understanding of the nature of a given threat, to communicate the level of seriousness of that threat to decision-makers and, in the case of open source releases, to the general public. The ultimate purpose of a threat assessment is to identify warning signs, generate potential perpetrator profiles, and have preventive measures in place to deter potential threats from becoming operational. The most notable open source documents released by the US are assessments published by the ODNI, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), and DHS. Foreign government agencies including the RCMP, BFP, and the United Kingdom's Security Service (commonly known as MI5) also have generated terrorism threat assessments that are publicly available. Similarly, think tanks such as the Rand Corporation have published reports on risks and threats related to terrorist groups or activities (Jackson et al., 2005; Willis et al., 2005). Reliance on these tools for CT domestically and internationally raises important concerns about the conceptual reliability of terrorism threat assessment methodologies to accurately generate situational awareness and to be effectively integrated into strategic decision-making from the perspective of law enforcement.

Published data and our own experience strongly indicates that intelligence-driven strategies require consolidating the physical, informational, and behavioral sciences into logical, cohesive overlays or patterns that can be applied to human

terrain data (e.g., individuals and groups in an operational environment). That is, situational awareness of real world phenomena within specified temporal and spatial domains (e.g., perception of environmental elements) forms a common intelligence picture of potential adversarial threats to be used by law enforcement agencies (Smith, Demphousse and Roberts, 2011). It provides the 'what to report' as well as the 'what if' and 'so what' for intelligence data, and is a foundational component of counterterrorism that is grounded in actionable and credible subject matter knowledge. Such analysis inevitably is based on the fusion of a large accumulation of data and experience. To meet the precipitating challenges of transforming first responders into first preventers, the 9/11 Commission recommended developing fusion centers to adapt the ILP concept to counterterrorism (National Commission on Terrorist Attacks Upon the United States, 2010). Drawing on its prior experience with ILP to identify chronic high-rate criminal offenders and other recurring problems, the UK similarly has endorsed an intelligence-driven model for law enforcement engagement in counterterrorism, particularly integrating ILP with community-oriented policing to thwart homegrown terrorists (Riley et al., 2005; Clark and Newman, 2007).

Not surprisingly, generating valid and reliable risk assessments that are actionable to counter adversarial behaviors is a challenging endeavor. Terrorists are not homogeneous. They differ widely in terms of capabilities; motivations; decision-making information, skills, and processes; and organizational or personal psychology. Because political violence in general, and terrorism in particular, is not the exclusive domain of a single academic discipline, building actionable knowledge and understanding requires an interdisciplinary approach to overcome existing conceptual and methodological limitations. This is particularly true when it comes to integrating mathematical formulas and using risk theory. Table 1 presents current methodological approaches used in assessing terrorist risk and their associated shortcomings.

Table 1: Current methods use in Terrorism threat/risk assessments and their limitations

Methods	Limitations
Qualitative methods that provide descriptive analysis for tactical/operational and/or strategic decision-making	These methods lack rigor and provide only loose conceptualization/operationalization
The Delphi method to weigh terrorist attributes and rank order them for prioritization purposes	Method results provide subjective appraisals that does not account for error or uncertainty
Probability models to quantify estimated risk based on some combination of threat, vulnerability, and consequence	Approaches result in partial model parameterization and deficient data quality

Unfortunately, there is no 'gold standard' (i.e., best practice) that has achieved universal acceptance despite some crossover of common elements for risk assessment. For instance, the U.S. General Accountability Office (GAO) published a report in the aftermath of 9/11 events asserting that a "good risk management approach" should include three main elements: (1) a threat assessment; (2) a vulnerability assessment; and (3) a criticality assessment (U.S. Government Accountability Office, 2001). According to the GAO, a threat assessment identifies and evaluates threats based on various factors including capability and intentions, as well as the potential lethality of an attack. A vulnerability assessment refers to a process that identifies weaknesses that may be exploited by terrorists and suggests options to eliminate or mitigate those weaknesses. A criticality assessment identifies and evaluates an organization's assets based on the importance of its mission, the group of people at risk, or the significance of a structure.

Similarly, a Rand Corporation report asserted that a terrorist risk assessment should be based on an analytic process (e.g., quantitative) relying on three central factors to determine terrorism risk: (1) *threat* measured as the probability that a specific target is attacked in a specific way during a specified period; (2) *vulnerability* measured as the probability that damage [i.e., fatalities, injuries, property damage, etc.] could occur according to a given a threat; and (3) *consequences* measured as the magnitude and type of damage resulting given a successful terrorist attack. Using the Rand approach, risk is a function of threat, vulnerability, and consequences (Willis et al., 2005). The report describes two approaches for estimating terrorism risk: (1) simple risk indicators that explore the link between population-based indicators and terrorism risk and (2) event-based models built upon relatively detailed analysis of consequences from specific attack scenarios.

Homeland Security Presidential Directives (HSPD) -10, - 18, and -22, recognize the need for systematic, science-based, terrorism risk assessments that inform strategic planning and resource prioritization. To address this need, DHS S&T developed a set of Terrorism Risk Assessments: Bioterrorism Risk Assessment [BTRA], Chemical Terrorism Risk Assessment [CTRA], and Integrated Chemical, Biological, Radiological and Nuclear Terrorism Risk Assessment [ITRA]. In addition, the Risk Assessment Process to Inform Decision-making (RAPID), in support of the DHS Policy for Integrated Risk Management (May 27, 2010), provides an all-hazards risk analysis by incorporating the information from all of these TRAs and addresses additional risks such as those from natural disasters and other threats. The TRAs mirror aspects of the Rand approach described above and are help prioritize protecting critical infrastructure against terrorist attacks. The TRAs are probabilistic risk assessments that integrate the expert judgments of the

intelligence and law enforcement communities with those from the scientific, medical, and public health communities. This approach is based on the following formula:

$$\text{Risk} = f(\text{Threat} \times \text{Vulnerability} \times \text{Consequences}) \quad \text{[Eq. 1]}$$

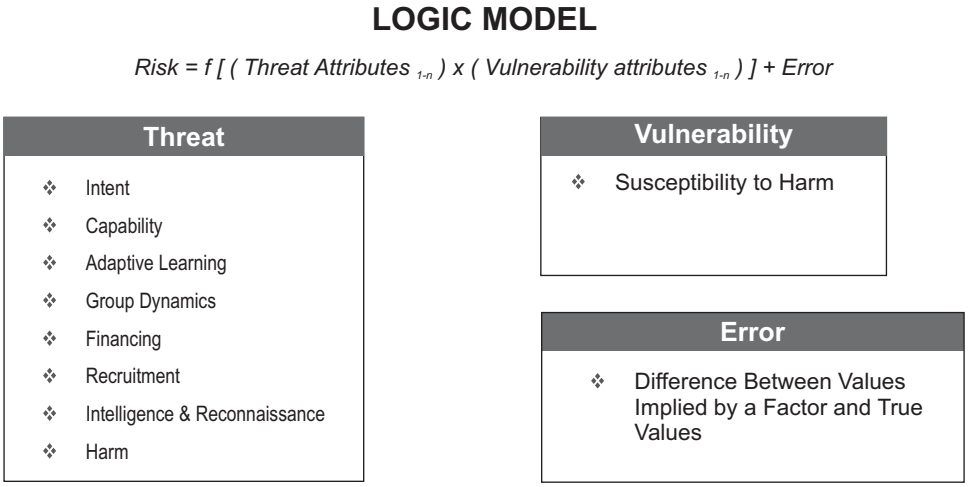
As Cox notes, several conceptual and methodological challenges arise when one attempts to directly assess threat probabilities for the actions of intelligent antagonists versus modeling how they adaptively pursue their goals in light of available information and experience (Cox, 2008). First, estimates have a very high degree of unavoidable uncertainty due to the relatively rare nature of terrorism threats and/or the scarcity of data. A number of studies have demonstrated that estimating the probabilities of high-impact, low-frequency events is extremely difficult and often produces highly subjective assessments (Krimsky and Golding, 1992; Weber, Blais, and Betz, 2002). Illustrating the imprecision of such subjective appraisals, a study concluded that assuming an annual worldwide death rate from international terrorism of approximately 1,000 victims/year (based on U.S. Department of State estimates), the lifetime probability that a person will be killed by terrorists is about 1:75,000 which, he points out, is about the same likelihood that one would die from the impact of an asteroid colliding with the Earth (Mueller, 2007). In other words, risk models based on probability produce an excessive level of uncertainty. Second, methodological issues are associated with the structure of the formula and its conceptual articulation. These include: (1) the failure to adjust for correlations among components (e.g. measures of damages and consequences); and (2) potential non-additivity of estimated risks. Third, there are inherent uncertainties and randomness associated with terrorism threats due to several factors: (1) terrorist entities are clandestine, closed systems making credible and timely acquisition of information problematic (Willis et al., 2005; Aust, 2009; Giorgio, 2003); (2) terrorism campaigns are dynamic (i.e., they occur over time with corresponding shifts in counterterrorism efforts and adversarial behaviors) (Cronin, 2009; Bjorgo and Horgan, 2009); and (3) law enforcement officials, especially at the state and local levels (due to the structure of the justice system), play a significant role in countering terrorism within the US which makes the situational awareness of those individuals critical in preventing and mitigating attacks (Riley et al. 2005; Carter and Carter, 2009).

Alternative Approach in Conceptualizing and Developing Logic Model of Terrorist Risk Assessment

When one takes these methodological and conceptual considerations into account, three factors must be addressed in order to design, parameterize, and interpret a new evidence-based assessment of terrorism risks: *threat, vulnerability* and *error/randomness*. On the threat dimension, the assessment must measure the *intent*, *capability*, and *harm* of a given terrorist group or 'lone wolf' actor within the context of a terrorist campaign. On the vulnerability dimension, the analysis must measure the *reliability and effectiveness of existing counter-measures*. Finally, it is essential to provide an *estimation of errors*. This last element is crucial because it quantifies and bounds the randomness of errors and information about the stability of predictions as well as the level of uncertainty attributable to the model. The following equation illustrates the conceptualization we propose:

$$Risk = f\left[\left(Threat\ attributes_{1\text{-}n} \right) x \left(Vulnerability\ attributes_{1\text{-}n} \right) \right] + Error \qquad [\text{Eq. 2}]$$

The threat attributes component or dimension that 'drives' risk requires specification and operationalization of multiple indicators in order to quantify threats to be linked through mathematical equations. Similarly, the vulnerability dimension of Eq.2 requires explicit metrics for inclusion in the equation. The error term quantifies the difference between values implied by a factor and the true values of the quantity being calculated. In the next section, we present the logic model that underlies our proposed algorithm-based this second equation.



Historically, groups (as opposed to 'lone wolf' actors) predominate in conducting terrorist campaigns. As a result, we opt to focus on group-centric modeling of adversarial behavior and our logic model is grounded in the following general premises:

- Risk assessment should seek robust risk estimators that account for uncertainty about terrorism risk;
- Algorithm-based assessments can serve both operational and strategic purposes by providing realistic threat and vulnerability measures;
- Analyzing these complex dynamic interactions, many of which are not well understood, requires simplification; and
- Too much simplification produces results, which may be useless or misleading.

Given these premises, we turn to describing how the key components of the model are conceptualized.

Threat represents the first of the two dimensions included in Eq. 2 that determine risk. It can be conceptualized as encompassing intent, capability; adaptive learning; group dynamics; financing; recruitment; intelligence and reconnaissance; and harm. For example, the underlying capability and intent as well as adaptive learning ability of a group can affect the persistence of terrorist campaigns, especially adaptation to CT measures (Cronin, 2009; Bjorgo and Horgan, 2009). As a result, when the components of the logic model are taken as a whole, the elements of threat component represent necessary but not sufficient conditions for terrorism to pose a risk. Each element of threat is defined below.

Intent refers to an opponent's ideology, motivations and desire to engage in adversarial behaviors and is a necessary but not sufficient condition for threat materialization (Schmid and Jongman, 2005; Crenshaw, 2000). Ideology refers to the underlying belief system (i.e., attitude structure for interpreting phenomena) that can explain and/or motivate action. Two paradigms, *prophetic* and *dialectic*, serve as proxies for motivation for terrorism. Religious and white supremacist groups commonly are categorized into the prophetic paradigm; the Aum Shinrikyo sect provides an example of prophetic terrorism. Left-wing and nationalist terrorist groups tend to be categorized into the dialectic paradigm; the Irish Republican Army (IRA) and the Quebec Liberation Front (FLQ) are examples. In parallel, radicalization processes – both religiously and non-religiously inspired – shape the dynamics of domestic and international terrorism (Jones, 2008; Horgan, 2005). A number of recent studies find individuals must progress sufficiently through a process of radicalization to acquire both the motivation and ability to support and, ultimately, to commit acts of goal - directed political violence. Finally, a terrorist

group must express directly or indirectly its intention to carry out violent actions against an entity. Each of these components of intent needs to be represented formally in an objectives hierarchy.

155*Capability* refers to the scientific/technical expertise, organization structure, and operation financing (e.g., tactics, weaponry) that a terrorist group possesses. Since 1968, terrorists have employed a wide range of weapons, from knives to assault rifles to toxic chemicals. Weapons in a general sense, constitute a logical and straightforward requirement, access to external weapon sources and/or unconventional weapons add another degree of complexity to this requirement. Indeed, it appears that as groups expand their activities, the reliability of weapon supplies becomes a more important operational requirement than simply having access to large weapons stockpiles. The array of potential threats encompasses chemical, biological, radiological, and nuclear terrorism, as well as conventional explosives, which remain the most common weapons used by terrorist groups.

Examples of possible attack scenarios include release of chemical warfare agents or toxic industrial chemicals in confined spaces; aerosol releases of bacterial, viral, or toxin agents in a building environment; the deliberate release of non-fissile nuclear material using a radiological dispersion device (RDD), commonly called 'dirty bombs', to contaminate a major port facility; the detonation of an improvised nuclear device (IND); or the use of conventional explosives to produce mass casualties and/or infrastructure destruction. Each scenario has different scientific and engineering barriers, especially acquisition of sufficient materials and delivery/use at a target, which affect an adversary's capabilities to execute the scenario. Those factors that influence the ability to attack are impacted by the choice of weapons, delivery technologies, time frame, and feasible target set. For example, although most microorganisms that cause disease or produce toxins (i.e., viruses, bacteria, fungal spores, and toxins) can be used as biological weapons, some are more likely candidates for use because they are extremely infectious and exhibit high mortality or debilitating mortality rates (Lane, Montagne and Fauci, 2001; Reshetin, and Regens, 2003). Similarly, an IND, unlike a RDD, requires sufficient fissile material (^{235}U or ^{239}Pu) and the proper design configuration to achieve criticality (Regens and Gunter, 2010; Regens, Gunter and Beebe, 2007). Comparable technical constraints apply to chemical terrorism (Regens et al., in press) or, for that matter, in the case of conventional explosives (Peleg et al. 2011). The increased likelihood, and perhaps inevitability, that terrorists will attempt to use weapons of mass destruction (WMDs) or weapons of mass effect (WMEs) is a core assumption of current assessments of the threat posed to homeland security by terrorism (Lane, Montagne and Fauci, 2001; Hoffman, 2006). The employment of Improvised Explosive Devices (IEDs) and other more common modes of attack further complicate the threat environment. However, the use of complex weaponry requires some level of sophistication and expertise.

Adaptive learning refers to the ability to hone expertise through learning from experience and emulating the successful behavior of others. Terrorist groups embody this attribute because they need to provide their members with the technical skills to conduct attacks successfully (e.g., bomb making, weapon handling, and even operational security techniques). Addressing adversary adaptation requires understanding the ways terrorist groups can respond to new defensive or other changes. They have a variety of options, each with distinct direct and indirect risk effects. For example, al-Qa'ida operatives are known to be highly adaptive in learning from past successes and failures (Springer, Regens and Edger, 2009). Relationships with other like-minded groups, possibly as an investment for future cooperation or help, also can be a way to gain "supplemental" expertise and/or training (Jackson et al., 2005). In addition to formal camps that require a secure operational base, the Internet and social media technology have become critical mechanisms for adaptive learning.

Group dynamics refers to the structural and leadership characteristics of social organizations. Command and control is the group dynamic mechanism that terrorist groups use to plan, coordinate, and execute their attacks. Command and control is a relatively consistent requirement across all terrorist groups, despite varying degrees of capabilities. The effectiveness of the attacks that a terrorist group might be capable of launching depends much on the structure of its organization. The less centralized and hierarchical, the more resilient the organization will be to CT action. A more elusive and resilient type of network architecture has no hub, but consists simply of a set of terrorist cells, which may comprise one or more individuals. For an emergent network under constant pressure from international CT forces, the types of attacks that can be attempted will be constrained by available resources (Jackson et al., 2005). For example, high loss scenarios may be attractive to AQ, but they may also be especially hard to execute under pressure. Also, the IRA campaign provides illustrations of the effectiveness of heightening security and cutting off supplies of armaments in reducing the options for terrorist action. Terrorist groups tend to coalesce around charismatic individuals who attract and inspire supporters. Therefore, leadership in this context plays a more cohesive than operational role, and we would expect that the most adversarial terrorists groups have fairly charismatic leaders like bin Laden (Springer, Regens and Edger, 2009).

Financing refers to the ways terrorist groups acquire financial resources. As such, money is best considered an operational and strategic tool; financing activities can be categorized as being (1) operational or (2) strategic (Ehrenfeld 2003; Warde, 2008). Short-term funding sources are usually exploited for operational purposes and represent a flexible "means-end financing". Operational financing is largely task-oriented and does not require sophisticated funding sources to support disorganized local entities or decentralized structures. Strategic financing aims to

support the long-term activities. According to Hoffman (2006), financing is a key element in ensuring the endurance of terrorist groups in part because they successfully acquire the loyalty of community members. Moreover, recent studies emphasize the function of voluntary organizations (i.e., 'club' model) as efficient providers of local public goods in the face of government failure to do so (Berman and Laitin, 2008). These "violent clubs" act as social movements and possess sufficient financial resources and a base of supporters within the community to function as alternatives to formal governmental institutions (e.g., Hamas, Hezbollah).

Recruitment refers to the processes for attracting new members both to grow in strength and to replenish losses and defections. Recruitment can be so important that one study of left-wing terrorism in Italy from 1970 to 1983 found that groups conducted increasingly lethal attacks, in part, to gain more recruits (Della Porta, 1995a, 1995b).

Intelligence and reconnaissance/casing refers to the basic skills in information collection and analysis that terrorists need to identify a potential target and plan/execute a method of attack, which engenders a desired response from its intended audience. Logically, we expect that the degree to which terrorist groups need intelligence will be directly related to the sophistication of the planned attack. Intelligence and reconnaissance includes activities designed to establish an accurate understanding of the local operating environment and the effect of an attack on their adversaries.

Harm refers to the severity of the event (e.g., deaths, injuries, psychological damage, level of critical infrastructure destruction, etc.) and its potential societal impacts (e.g., economic costs, impact on trust in government, etc.). That is, harm is a measure of a terrorism event's consequences.

Vulnerability represents the second of the two dimensions included in Eq. 2 that determines risk. Assessment of vulnerability is mainly related to the evaluation of the counter-measures. Most studies have looked at situational prevention and physical protection focusing on deterrence, preparedness, and response to mitigate consequences. The Department of Homeland Security defines vulnerability as a "physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard". For the purpose of this study, the vulnerability characteristics of a target will be drawn from the information contained in the database for each incident (if available). Factors such as location, accessibility, and the nature of the target (hard or soft) can explain the fluctuation of terrorist attacks.

Error is the third component that our logic model incorporates. Estimates of risk generated using indicators of threat and vulnerability are inevitability uncertain. For example, we know terrorists may build IEDs and vulnerabilities to IEDs exist under some scenarios. That is, each dimension is necessary and some combination of the two dimensions is a sufficient condition for risk. However, because we lack perfect information, some error in likelihood estimates is inherent in our predictions. Moreover, even 'known' information is subject to uncertainty, thereby introducing error into our estimates of risk.

The ***error term*** in Eq. 2 refers to a statistical estimator that quantifies the difference between values implied by a factor and the true values of the quantity being calculated. Mean Squared Error (MSE) plays a role of "risk estimator" within the equation, corresponding to the expected value of the squared error loss. In the formula to assess terrorism risk, the MSE is used to determine whether the risk model does not fit the data well and/or whether removing or modifying factors can simplify the model.

Suggested Methodology

Modeling adversarial threats has the potential to inform probabilistic estimates of adaptive attack behavior and aid law enforcement in the design and selection of anti-terrorism countermeasures. The overall strategy for applying the Logic Model outlined in the preceding section involves building on the broader literature, existing models, and our own prior work to: (1) parameterize the "theoretical model" based on open source data supplemented by indicators from the broader literature as well as our prior studies; (2) parameterize existing law enforcement practical models; (3) estimate threats using historical data to compare models' output; (4) specify an integrated theoretical model that captures key parameters with the greatest predictive power in the practical models used by the law enforcement existing models; (5) verify the predictive power of the integrated algorithm-based model; and (6) interpret the findings and develop desktop application that captures structured, encryptable data on terrorist events. The methodology must follow a series of step in order to produce a robust modelization

First, database architecture should be designed to include data entry protocols providing randomized checks of data integrity to review values entered and correct invalid information prior to and subsequent to populating the database, in order to ensure quality control data entry. The database management architecture should also include procedures for data archiving. Completion of this task, which includes a protocol for ongoing database management, is necessary for modeling and advanced data analysis. In parallel to designing the database, it is also crucial to design data entry protocols for all data to populate the relational databases. Protocols should be developed and implemented to provide randomized checks of

data integrity to review values entered and correct invalid information prior and subsequent to populating the database. This task is critical because standardized procedures are necessary to ensure consistent, replicable techniques are used for database construction.

Second, a data set should be created. This task is crucial because it leads to the development of the theoretical terrorism risk assessment model. Task 3 involves four sub-tasks: (1) collecting data from public sources; (2) applying geographic identifiers (x, y coordinates) to those data; (3) populating the geo-referenced database; and (4) analyzing the data set with regression techniques and other statistical tools. As main source of data, the Global Terrorism Database can be used. GTD is an open-source database including information on terrorist events around the world from 1970 through 2010, with additional annual updates planned for the future. Unlike many other event databases, the GTD includes systematic data on domestic as well as transnational and international terrorist incidents that have occurred during this time period and now includes more than 98,000 incidents. For each GTD incident, information is available on the date and location of the incident, the weapons used and nature of the target, the number of casualties, and – when identifiable – the group or individual responsible. The National Consortium for the Study of Terrorism and Responses to Terrorism (START, a DHS academic center of excellence) maintains this database.

Another database that include open source data available from the New America Foundation and Syracuse University's Maxwell School of Public Policy database of post-9/11 Americans or U.S. residents convicted or charged of some form of jihadist terrorist activity, as well as the cases of those American citizens who have traveled overseas to join a terrorist group along with details of the alleged plots. The New America Foundation/Syracuse University data can be used to supplement the GTD.

All data should be linked to geographic identifiers and geo-referenced to support modeling the spatial component of terrorist threat. Geo coded data on terrorist attacks can be useful to assess the geographical scopes of terrorism activities. It can also help identifying concentration areas where some terrorist activity takes place. Data will also be analyzed using time-referenced data in order to better understand the relation between fluctuation of attacks (dependent variable) and threat/vulnerability characteristics (independent variables) over the time. Both spatial and temporal analyses will provide critical results regarding the specificities of some groups or target characteristics that are more susceptible to fluctuation according to time or space.

Finally, a first round of analysis must be conducted to estimate the specification of the theoretical model in order to analyze the influence of the indicators outlined in

the logic model summarized above. This procedure provide an opportunity to estimate the reliability of the theoretical model, test for autocorrelation and multicolinearity problems, and identify variables that need to be removed from the model.

Third, the accuracy and reliability of existing threat assessment models should be tested against the database described in this section. Testing these "practical models" from law enforcement can help to identify additional relevant concepts/variables to be included in Eq. 2. This stage consists of: (1) populate models using GTD values; (2) estimate terrorist threat predictions; and (3) interpret model results. For example, threat assessment models developed by the Royal Canadian Mounted Police and the Belgian Federal Police can represents an excellent source of data for comparisons.[1] This third phase involves estimating terrorism risk using the law enforcement models. Each of the models selected for evaluation can be used separately to generate terrorism threat predictions using historical data. Finally, this phase involves interpreting the law enforcement model results. Qualitative appraisals and statistical analysis procedures should be used to identify key predictors from both models. Potential measures may include residual errors, coefficient estimates, coefficient standard errors, and goodness of fit measures. In essence, which parameters from which models are most accurate in predicting those historical events?

The fourth phase requires the elaboration of an integrated algorithm-based risk model, based on a system of mathematical equations, which incorporates the key parameters identified above combined with subject matter expert judgments and input from the law enforcement community. It is crucial that the model's system of equations integrates and weights appropriately each of the three elements described in the logic model (e.g., *threat*, *vulnerability*, and *error*).

Finally, the last phase is about populating the Integrated Algorithm-based Model and Estimate Terrorism Risk. More precisely populating the parameters for the algorithm-based model specified before, drawing on the GTD and supplemented by the law enforcement information for initial parameterization. The model can then be re-specified and calibrate by utilizing a random sample of terrorism incidents from the database developed. Finally , the performance of this new terrorism risk

[1]The RCMP developed a model called "*Sleipnir*" for national threat assessments on terrorism and criminal extremism. The *Sleipnir* model allowed the RCMP to set priorities in its fight against terrorist groups. To date, the BFP's Integrated Police Operation Directorate and its Strategic Analysis Service have identified more than 30 recurrent or emerging security problems against which police must take action, including terrorism. However, only certain elements of terrorists' capacity were included in the threat assessment model.

model (Equation 2) must be compared to the existing risk model developed by Department of Homeland Security (Equation1) to understand and underscore the conceptual contribution to the field as well as its application to situational awareness and strategic decision-making for law enforcement agencies.

Conclusion

The application of algorithm model to terrorism risk assessment can help to understand better pattern of violent groups over a period of time. This approach can serve both operational and strategic purpose by (1) providing realistic measures to investigators and intelligence officers on threat and vulnerability characteristics and (2) using individual terrorism group risk factors to help decision-makers to identify strategic priorities as wells as appropriate tactics to reduce vulnerabilities and mitigate threats. However, this model does not predict terrorism attacks neither it provides a crystal ball to analysts. Another limitation related to algorithm-based approach is the availability of significant amount of data in order to generate reliable models. The application of robust risk analysis can help law enforcement agencies to prioritize groups that present the most serious security risks, allocate resource efficiently, elaborate more effective counter-terrorism strategies and tactics thereby increasing safety for communities.

Reference

Aust, S. (2009). *Baader-Meinhoff.* Translated by A. Bell. New York: Oxford University Press.

Berman, E. and D. D. Laitin (2008). *Religion, Terrorism and Public Goods: Testing the Club Model*. NBER Working Papers. 13725, National Bureau of Economic Research.

Bjorgo, T. and J. Horgan (Eds) (2009). *Leaving Terrorism Behind*. London: Routledge.

Carter, D.L. and J.G. Carter (2005). Intelligence-led policing. *Criminal Justice Policy Review* 20: 310-325.

Clarke, R.V. and G.R. Newman (2007). Police and Prevention of Terrorism. *Policing* 1 (1): 9-20.

Cox, L. A. Jr, (2008). Some Limitations of Risk = Threat × Vulnerability × Consequence for Risk Analysis of Terrorist Attacks. *Risk Analysis*, 28: 1749–1761.

Crenshaw, M. (2000). The psychology of terrorism. *Political Psychology* 21: 405-420.

Cronin, A.K. (2009). *How Terrorism Ends*. Princeton, NJ: Princeton University Press.

Della Porta, D. (1995a) *Social Movements and the State: Thoughts on the Policing of Protest*. European University Institute.

Della Porta, D. (1995b). Left-Wing Terrorism in Italy, in Martha Crenshaw (ed.) *Terrorism in Context,* pp. 134-157. State College, Pa.: Pennsylvania State University Press.

Ehrenfeld, R. (2003). *Funding Evil: How Terrorism is Financed and How to Stop it*. Santa Monica: Bonus Books.

George R.Z. and J.B. Bruce (eds.) (2008). *Analyzing Intelligence.* Washington: Georgetown University Press.

Giorgio (2003). *Memoirs of an Italian Terrorist.* translator A. Shugaar. New York: Carroll & Graf.

Heuer, R.J. Jr. (1999). *Psychology of Intelligence Analysis*. McLean, VA: Central Intelligence Agency, Center for Study of Intelligence.

Hoffman, B. (2006). *Inside Terrorism.* New York: Columbia University Press.

Horgan, J. (2005). *The Psychology of Terrorism*. London: Routledge.

Jackson, B. et al. (2005). *Aptitude for destruction: organizational learning in terrorist groups and its implications for combating terrorism.* Santa Monica: Rand Corporation.

Jones, J.W. (2008). *Blood That Cries Out From the Earth*. New York: Oxford University Press.

Krimsky, S. and D. Golding (1992). *Social theories of risk*. Westport, CT: Praeger-Greenwood.

Lane, H.C., J. L. Montagne and A. S. Fauci (2001). Bioterrorism. *National Medicine* 7:1271-1273.

Lemieux, F. (2006). *Norms and Practices in Criminal Intelligence: An International Comparison*. Ste-Foy: Laval University Press.

Lemieux, F. (2008a). Information Technology in Criminal Intelligence Services: A Comparative Perspective. in Leman-Langlois, S. (Ed.) *Technocrime*, pp. 139-168. Columpton, UK, Willan Publishing.

Lemieux, F. (2008b). A Cross Cultural Comparison of Intelligence Led Policing, in Williamson, T. (Ed.) The Handbook of Knowledge Based Policing: Current Conceptions and Future Directions, pp. 221-240. Chichester, U.K., Wiley & Sons.

Mueller, J. (2007). Reacting to Terrorism: Probabilities, Consequences, and the Persistence of Fear. *Paper presented at the annual meeting of the International Studies Association 48th Annual Convention, Hilton Chicago* Chicago, IL, USA, Feb. 28.

National Commission on Terrorist Attacks Upon the United States (2010). *The 9/11 Commission Report*. Washington: U.S. Government Printing Office.

Peleg, K., J.L. Regens, J.T. Gunter and D.H. Jaffe (2011). The normalization of terror. *Disasters* 35: 268-283.

Regens, J.L. and J.T. Gunter (2010). Predicting the magnitude and spatial distribution of potentially exposed populations during IND and RDD terrorism incidents. *Human & Ecological Risk Assessment* 16: 236-250.

Regens, J.L., J.T. Gunter and C.E. Beebe (2007). Estimating total effective dose equivalents from terrorist use of radiological dispersion devices. *Human & Ecological Risk Assessment* 13: 929-945.

Regens, J.L., J.T. Gunter, M. Amin, A. Nowakowski & H. Navaz (in press). Parameterizing potential exposure to HD using mixed model regression" *Human & Eco Risk Assess*.

Reshetin, V.P. and J.L. Regens (2003). Simulation modeling of Anthrax spore dispersion in a bioterrorism incident. *Risk Analysis* 23: 1135-1145.

Riley, K.J., G.F. Treverton, J.M. Wilson and L.M. Davis (2005). *State and Local Intelligence in the War on Terrorism*. Santa Monica: RAND.

Schmid, A.P. and A.J. Jongman (2005). *Political Terrorism.* Amsterdam: North Holland Publishing.

Smith, B., K. Demphousse, and P. Roberts (2011). *Pre-Incident Indicators of Terrorist Incidents: The Identification of Behavioral, Geographic and Temporal Patterns of Preparatory Conduct.* Washington D.C.: U.S. Department of Justice.

Springer, D.S., J.L. Regens and D.N. Edger (2009). *Islamic Radicalism and Global Jihad*. Washington: Georgetown University Press.

U.S. Government Accountability Office (2001). *Homeland Security. Key Elements of Risk Management Approach*.

Verfaille, K. and T. V. Beken (2008). Proactive policing and the assessment of organized crime. *Policing: An International Journal of Police Strategies & Management*, 31(4): 534 – 552.

Warde, I. (2008). *The Price of Fear.* Los Angeles: University of California Press.

Weber, E. U., A. R. Blais, and N. Betz (2002). A domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors. *Journal of Behavioral Decision Making* 15: 1-28.

Willis, H. et al. (2005). *Estimating Terrorism Risk*. Santa Monica, Rand Corporation.

The author Frederic Lemieux is Professor and Program Director of the bachelor's degree in Police Science and master's degree in Security and Safety Leadership at The George Washington University. Dr. Lemieux has numerous publications in English and French on terrorism financing, best practices in strategic intelligence, militarization of the intelligence community, and international police cooperation. He spearheaded several international research projects on intelligence-led policing in collaboration with the Royal Canadian Mounted Police; Serious Organized Crime Agency (United Kingdom); Drug Enforcement Administration; Belgium Federal Police; Europol (Netherlands); Interpol (France); OCTRIS (France); Colombian National Police and Department of Administrative Security (DAS); Venezuela National Police; Singapore Police Force; Australian Federal Police and Australian Crime Commission; NATO (Europe); and Geneva and Lausanne canton police forces (Switzerland). Prof. Lemieux can be reached at flemieux@gwu.edu.

The author James L. Regens holds the Edward E. and Helen T. Bartlett Foundation Chair and is founding Director of the Center for Biosecurity Research at the University of Oklahoma Health Sciences Center. Dr. Regens has served in policy and analytical positions in government and national laboratories and is a member of the Council on Foreign Relations. He has authored or co-authored over 200 scientific and technical publications including articles in journals such as Proceedings of the National Academy of Sciences, Risk Analysis, and Human & Ecological Risk Assessment as well as eight books. Dr. Regens can be reached at Larry-Regens@ouhsc.edu.