2008-06

Threat-Based Approach to Risk, Case Study: The Strategic Homeland Infrastructure Risk Assessment (SHIRA)

French, Geoffrey S.

Threat-Based Approach to Risk
Case Study: The Strategic Homeland Infrastructure Risk Assessment (SHIRA)

Geoffrey S. French
Jin Kim
Pasha Vasilev
CENTRA Technology, Inc.
4121 Wilson Blvd, Suite 800
Arlington, VA 22203
frenchg@centratechnology.com
kimj@centratechnology.com
vasilevp@centratechnology.com

Introduction

The culture of risk management is beginning to grow at the Department of Homeland Security (DHS). Created in response to the attacks of September 2001, the Department has as one of its primary missions to protect the nation from terrorism.[1] Five years after its creation, and through several reorganizations, DHS still struggles to master risk management with respect to terrorism. Although DHS realized the need for the collaboration of intelligence and security professionals to jointly assess risk at its inception,[2] it was not until the formation of the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) that DHS had a truly integrated approach to terrorism risk analysis.

Risk, defined in the National Infrastructure Protection Plan (NIPP) as a "measure of potential harm that encompasses threat, vulnerability, and consequence,"[3] guides the DHS infrastructure protection community in its analyses and assessments to better inform decision-making. Although the NIPP also includes natural disasters or other incidents in its definition of risk,[4] this paper will focus on terrorism risk, describing the organizational development and convergence of DHS' intelligence and infrastructure protection areas – changes designed to bring forth a cultural change of collaboration. In addition, the paper will identify current problems and hurdles with regard to a terrorism risk culture. The case study will focus on a successful current threat based approach to risk, the Strategic Homeland Infrastructure Risk Assessment (SHIRA). Finally, this paper will propose a path forward in leveraging the success of the SHIRA to better meet the needs of terrorism risk analysis and assessments that inform strategic planning to enhance the protection and preparedness of the nation's CIKR.

Recognizing the Need for a Threat-Based Strategy

CIKR is at the heart of the nation's economy and way of life. From the Banking and Finance Sector to the Food and Agriculture Sector, the 18 CIKR sectors form the backbone of the United States.[5] The preponderance of CIKR in the United States is owned privately, making the federal government's duties with respect to its protection challenging. Homeland Security Presidential Directive 7 (HSPD-7) established the need

---

[1] DHS website, http://www.dhs.gov/xabout/strategicplan/index.shtm, accessed 10 April 2008.
[2] *Homeland Security Act 2002*, http://www.whitehouse.gov/deptofhomeland/bill/, accessed 11 April 2008.
[3] *National Infrastructure Protection Plan*. Department of Homeland Security, 2006, 105, http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm, accessed 11 April 2008.
[4] Ibid.
[5] The eighteen CIKR sectors are: Agriculture and Food, Banking and Finance, Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy: Electric, Energy: Oil and Gas, Government Facilities, Information Technology, Monuments and Icons, Commercial Nuclear Reactors, Materials, and Waste, Postal and Shipping, Public Health and Healthcare, Transportation: Aviation, Transportation: Highways, Transportation: Maritime, Transportation: Mass Transit, Transportation: Pipelines, Transportation: Rail (Freight), Water: Drinking Water, Water: Wastewater.

to create roles and responsibilities "for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks."[6] The NIPP, developed by the Office of Infrastructure Protection, outlines the overarching structure to blend together current infrastructure protection programs with future requirements under a single program.[7]

This blending requires a strategic risk analysis that informs the prioritization of federal government resources for CIKR protection. Risk, a function of the likelihood of an unwanted event and its impact or effects, translates into a function of threat, vulnerability, and consequences in terrorism risk analysis; threat and vulnerability constitute the likelihood.[8] There are many techniques and approaches to the risk calculus; but at the core of sound risk analysis are the requirements that it be: objective, transparent, repeatable, accurate, and discriminating. Because risk models come in various forms (quantitative, semi-quantitative, and qualitative) there are competing ideas for what constitutes an effective risk model. Quantitative proponents may argue a strict adherence to probability theory; however, in situations where data are sparse – as is with intelligence and infrastructure – the precision that quantitative models should deliver is artificial. Strategic risk analysis for CIKR dictates a logic-based or semi-quantified approach. Using sound logic, fully addressing the core requirements of risk analysis, and focusing on the problem should be the tenets for strategic risk analysis.

Threat analysis is an essential factor of strategic planning. Although this appears to be self evident, some security analysis models do attempt to assess risk without assessing threat. Models that lack a threat component appeal to users who assume that the government has a monopoly on threat information and that they have no way of obtaining it from the government. The CARVER methodology, one of the best-known examples of an analytic tool that does not have a threat component, allows a user to prioritize attack scenarios by focusing exclusively on vulnerability and consequence.[9] Although there are significant challenges in public–private information sharing, this solution—to simply ignore threat—is misleading at best and disingenuous at worst. It overstates unlikely scenarios, especially attacks where the adversary has a very low capability.[10] This can cause an organization to overlook scenarios that are much more likely, even though they do not produce catastrophic consequences. Security and risk analysis without threat is a two-legged stool; because it may lead to illogical conclusions, it may be a poor foundation for any serious prioritization of efforts or resources.

Even simplistic threat assessments allow some meaningful differentiation of threat levels. The Federal Emergency Management Agency guide on risk assessment (FEMA 452), for

---

[6] *Homeland Security Presidential Directive* 7. December 17, 2003, http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html, accessed 10 April 2008.
[7] *National Infrastructure Protection Plan*, 1.
[8] *National Infrastructure Protection Plan*, 35.
[9] See the Product Surety Center's primer, "CARVER Plus Shock Method for Food Sector Vulnerability Assessments," 2005.
[10] For an in-depth discussion of the repercussions of ignoring terrorist threat, see Jeremy Shapiro's "Managing Homeland Security," The Brookings Institution: Washington DC, 2008. http://www.brookings.edu/papers/2007/0228terrorism_shapiro_Opp08.aspx, accessed 10 April 2008.

example, allows a user to make an estimation of threat based on the complexity of the task and the difficulty of obtaining and working with the necessary materials.[11] Although this has the potential to underestimate the capability of a terrorist group in an attack method that they have not demonstrated, it does allow an analyst to review open-source information and prioritize the threat accordingly.

This type of model would suffice for an individual organization assembling a risk-based strategy for its own security efforts. However, it does not allow a comparison of risk levels across organizations, given the potential for differences of opinion in threat levels. For equitable comparison, there needs to be a central authority to coordinate and – at a minimum – set the assumptions for the threat analysis. For a national-level comparison of infrastructure, it falls upon DHS to provide that threat analysis.

For CIKR risk, there are two major communities – the Intelligence Community (IC) and the infrastructure protection community – that must collaborate on all aspects of risk to produce the most accurate assessments for terrorism risk to critical infrastructure. Similar to the military decision-making process where intelligence initiates the planning, and all functional areas participate in the entire process, CIKR risk assessments must be shepherded by the infrastructure protection community with threat as the initiating component. The *threat* referred to in the NIPP is an intelligence-based estimate on terrorism – the unwanted act or event in the risk equation.[12] A threat-based strategy, however, means that all components of risk (threat, vulnerability, and consequence) model are shaped by the focus on terrorism. According to Jeremy Shapiro of the Brookings Institute, "[T]his analysis of the terrorist threat implies several priorities for U.S. homeland security—and, conversely, several areas that do *not* need greater attention or spending."[13] A threat-based approach to terrorism risk shapes the decision-making environment for the policy-maker.

Threat

Threat, defined for CIKR risk purposes as an intelligence-based estimate of terrorism against critical infrastructure, must incorporate the evidence along with the analysis of subject matter experts on terrorist capabilities and intentions to attack the United States. This estimate must reflect the judgment of the level of government to which the threat and risk analyses apply. For example, an intelligence-based estimate for a strategic level risk assessment model may not be applicable for an assessment for tactical purposes. Although the information sharing at DHS is evolving to a more effective system, inclusive of state and local governments as well as federal, the nature of intelligence and protection of sources and methods makes the prospects of a strategic level assessment fully being applicable at a tactical level unlikely. However, the prospects bode well for sharing of knowledge and understanding of the estimates between the levels of government.

---

[11] Federal Emergency Management Agency, FEMA 452. Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings, January 2005, p 1-21.
[12] *National Infrastructure Protection Plan*, 39.
[13] Shapiro.

Intelligence is not an exact science; therefore, DHS should not try and make it such by attempting to force a highly quantified model for the sake of an equation. Rather, one must tailor the model to the assessment process and allow review of the data (as appropriate and in accordance with classification standards) and analyses behind the threat assessment for debate. This transparency will in turn allow alternative analyses and assessments to build upon the overall risk analysis. Additionally, the threat methodology must represent the community of stakeholders. In developing a threat model that incorporates the collective knowledge and data from the IC, along with the security needs of the infrastructure protection community, the model must serve as a mechanism to consider multiple theories, weigh evidence, and guide consensus.

Vulnerability

In the context of terrorism risk, developing a methodology for vulnerability analysis must take into account the potential adversary. Therefore, a design of the vulnerability model should incorporate terrorism experts who can provide the insight through the lens of the terrorists. Models that do not utilize terrorism expertise in the development have the potential to bias the model towards unrealistic expectations that may create unattainable standards of invulnerability.[14] Risk analyses support the allocation of limited resources; a vulnerability model that only considers the judgments of security experts misses the vector analysis that terrorism experts can bring. For example, many vulnerability models are only developed with experts that look at the problem of how security professionals view the vulnerabilities and not how adversaries view the vulnerabilities. Collaboration between security experts and terrorism analysts provides the ideal approach to developing a vulnerability model for terrorism risk.

Consequence

As defined in the NIPP, a consequence assessment should measure the potential loss in four categories: public health and safety, economic, psychological, and governance impacts.[15] The four categories are consistent with the ideology and motivations of the terrorist threat – terrorist goals to destroy the U.S. economy, government, and impose psychological harm. In practice, however, most methodologies focus on economic and loss of life because those aspects are more easily quantified. Quantification of the economic losses and loss of life is an important aspect of modeling consequence, but that alone diverts focus from the whole which includes public health and safety, psychological, and governance impacts. Some methodologies measure economic loss and loss of life quantitatively with actual dollar values and relegate the other categories spelled out in the NIPP to qualitative assessments that are not integrated, leaving the assessment bereft of fundamental elements crucial to support decision-making at the national level of government. Therefore, whatever the type of methodology (quantitative, semi-quantitative, or qualitative), it must incorporate all categories into its methodology. Quantification is not merely using real dollar values; therefore, one would have to

[14] Shapiro.
[15] *National Infrastructure Protection Plan*, 103.

establish equivalencies or utilities to develop consequence models quantitatively that take into account all categories where the measurements do not directly translate into dollar values. In this approach, a risk index or levels of severity are appropriate for risk analysis.

Wrapping Our Hands Around Threat

The infrastructure protection community can do all it can to create a collaborative environment between all levels of government and the private sector; however, the challenges with respect to obtaining threat assessments for risk purposes are uniquely a government-to-government function. "To receive better threat information from the U.S. government, the critical infrastructure protection community must acknowledge inherent limitations of intelligence analysis and then help formulate requests for threat information, knowing that no single approach or tool will give a decision-maker the full perspective needed to manage risk."[16] DHS is the unique government organization that makes this government-to-government interaction a reality. Through DHS, the IC and infrastructure protection community can learn each others' characteristics and develop a common understanding of the requirements for a terrorism risk assessment.

Case Study – Strategic Homeland Infrastructure Risk Assessment

The Strategic Homeland Infrastructure Risk Assessment (SHIRA) provides a national-level terrorism risk assessment that offers a snapshot of the highest risk to the nation's critical infrastructure and key resources. The SHIRA utilizes an interagency, DHS-led process to analyze and produce assessments of threat, vulnerability, and consequence, and combines the data into a single measurement of risk for purposes of comparison. The methodology uses a structured method to quantify government and non-government expert opinions. Where modeling or quantified assessments already exist, their output can be easily captured in the SHIRA framework, which is based on accepted risk analysis principles and was designed to be as simple as possible. Text descriptions used by government experts to assign numerical values were designed to best match the data quality and to minimize double-counting of risk factors.

The SHIRA is a scenario-based model where Sector Specific Agencies (SSAs) that represent each CIKR sector applied terrorist attack methods of concern to their individual sectors. HITRAC, through coordination with the IC partners, provides a standard set of terrorist attack methods and descriptions. The SSAs then apply selected attack methods of concern to their sectors and create worst, most-likely scenarios. The IC assesses the threat of each attack method to each sector and the SSAs assess the vulnerability and consequence for each of their respective scenarios. Where applicable, HITRAC will assess vulnerability and consequence through independent outside subject matter experts to assist and augment the SSAs in their rankings.

---

[16] French, Geoffrey S. "Intelligence Analysis for Strategic Risk Assessments". *Critical Infrastructure Protection: Elements of Risk*. Critical Infrastructure Protection Program: George Mason University School of Law, December 2007, 12. http://cipp.gmu.edu/archive/RiskMonograph_1207_r.pdf, accessed 15 April 2008.

The relationship between the threat, vulnerability, and consequence assessments is represented:

Risk = Threat × Vulnerability × Consequence *(Equation 1)*

The risk is computed based on a standard probabilistic model where a quantification of a consequence is weighted in proportion to the probability that it will occur. This is expressed:

$$\mathbf{R = P \times C} \quad \textit{(Equation 2)}$$

where **R** is risk, a measure of the concern presented by a threat scenario, **P** is the probability that the threat scenario will occur, and **C** is the consequence if the threat scenario occurred and an attack was successful.

It is important to note that the number of terrorist attacks does not support a statistically significant calculation of probability. The SHIRA assesses the severity of threat and vulnerability as a proxy for probability. The probability that a threat scenario will occur is therefore calculated in terms of the likelihood that an adversary will launch the attack described in the attack method (represented by the variable $\mathbf{T_P}$, where the subscript is used to note probability), and the likelihood that the target of the threat scenario is vulnerable to the attack (variable $\mathbf{V_P}$). This is expressed:

$$\mathbf{P = T_P \times V_P} \quad \textit{(Equation 3)}$$

Thus, the risk equation becomes:

$$\mathbf{R = (T_P \times V_P) \times C} \quad \textit{(Equation 4)}$$

SHIRA Threat

DHS works closely with the other members of the IC to identify the appropriate terrorist attack methods and then quantify the threat from each. The attack methods used in the SHIRA are those where terrorists have demonstrated a capability or where intelligence reporting indicates that terrorists are making an effort to acquire the capability.

The SHIRA threat analysis addresses both a terrorist group's capability and intent to attack. To estimate capability, DHS examines both the demonstrated capability and takes into account the group's efforts to acquire or augment that capability. To estimate intent to attack, DHS first assesses general terrorist interest in attacking the sectors of infrastructure and then examines specific intent to use one of the attack methods against a specific sector. These are illustrated in Figure 1 and explained in more detail below. The benefit of this approach is that it is relatively simple (compared with other approaches to

probabilistic threat), it measures severity of threat in a way that allows expert consensus, and the results closely match qualitative threat analysis.

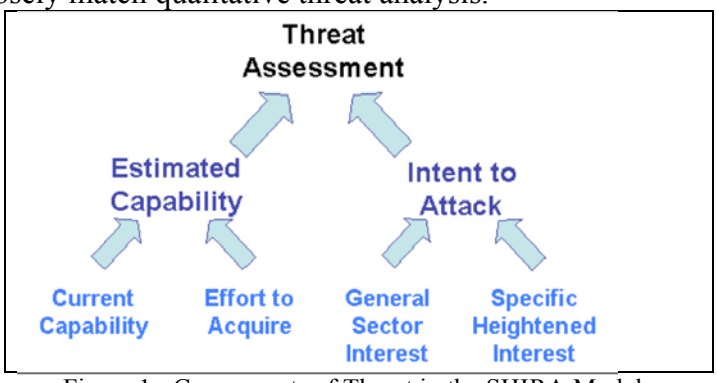

Figure 1: Components of Threat in the SHIRA Model

Framework for the Analytic Process

The SHIRA approach supports interagency consensus on the analytic conclusions in three ways. First, DHS uses defined thresholds to delineate stages of capability and degrees of intent. Second, DHS provides ranking guidance to help participating analysts assess operational capability (i.e., the means, materials, and expertise to launch the attack described in the attack method), operational plans (i.e., a terrorist initiative to which personnel or funding has been assigned), and other relevant factors in a consistent manner. Third, DHS provides the initial rankings and the intelligence reporting that contributed to the analytic judgments. This approach provides transparency into the process and rankings, which allows debate and a means for resolution.

Estimated Capability

When assessing terrorist capabilities, DHS uses analysis of both historical attacks and intelligence reporting for an assessment of near-term risk. The SHIRA defines estimated capability as having two components: current capability and effort to acquire the capability. *Current capability* considers historical incidents and knowledge of existing capability, whereas *effort to acquire* evaluates an adversary's attempts to gain or build upon a capability (the maturity of the acquisition process or the degree of effort and progress of the acquisition process). For a high-level assessment such as the SHIRA, an assessment of the effort to acquire a capability helps account for uncertainty, as well as provides a mechanism for allowing for the potential increase in capability within the near-term timeframe of the analysis.

Table 1 lists the ranking levels and criteria for the components of estimated capability. The criteria for *effort to acquire* are meant to represent an intermediate step to the next level of *current capability*. (That is, a ranking of 3 in effort to acquire is intermediate between level 2 and 3 in current capability.) In this way, the ranking table would be used as a progression from level 0 in effort to acquire to a 4 in current capability.

Table 1: Ranking Table for Estimated Capability					
Component	**Ranking level**				
	0	**1**	**2**	**3**	**4**
Effort to Acquire a Capability	No effort to acquire the capability	Adversary is pursuing the capability by attempting to develop internal expertise, obtain materials, or recruit experts	Adversary has an organized attempt to obtain either materials or expertise needed to advance the capability	Adversary has internal training, expertise, and access to materials required to develop the capability	Adversary has training or operational plans to develop the capability to launch an attack in the United States
Current Capability	No evidence of existing capability to execute the attack	Evidence of existing pre-operational skills	Suspected operational capability	Overseas operational capability confirmed by credible intelligence	Domestic operational capability confirmed by credible intelligence

Intent to Attack

As stated above, to estimate intent to attack, DHS first assesses the terrorist group's general interest in attacking a sector of infrastructure and then examines specific intent to use one of the attack methods against a specific sector. *General sector interest* reflects the adversaries' general desire to attack a specific sector, irrespective of attack method. As with its approach for estimating capability, DHS defines criteria for separating the sectors into tiers. The criteria are meant to be specific enough to make clear distinctions between the tiers, but flexible enough to accommodate analytic judgments. The tiers do not reflect raw numbers of reports, but rather the meaning of the reports. Table 2 contains the definitions for the tiers for general sector interest.

Table 2: Rankings for General Sector Interest	
Ranking	**Description**
Tier 1	There is a body of evidence or credible reporting and analysis including multiple threat or threat streams originating from numerous sources regarding the intent of the group being evaluated to attack the sector in the United States.
Tier 2	There is credible reporting and analysis depicting a threat originating from a single source or a limited set of sources regarding the intent of the group being evaluated to attack the sector in the United States
Tier 3	There is reporting depicting threat or threat streams originating from sources of undetermined credibility regarding the intent of the group being evaluated to attack the sector in the United States.
Tier 4	There is no known information or analysis concerning a terrorist threat to the sector in the United States.

The ranking of *general sector interest* is used as the baseline of a terrorist intent to attack the sector in ranking scenarios (i.e., the use of a specific attack method against a specific sector) where there is no intelligence to identify the intent of a terrorist group to attack. Where scenario-specific intelligence is available, DHS assesses *specific heightened interest*, which reflects historical precedent or current intelligence reporting. Although foreign attacks provide many of the data with regard to intent, the SHIRA criteria

separate those that occur in security environments different from the United States. Table 3 defines the rankings used for specific heightened interest in a scenario.

Table 3: Rankings for Specific Heightened Interest	
Ranking	**Description**
A	Intelligence indicates a **heightened interest** in using the attack method against the sector in the United States or Western Europe (e.g., operational plan or attack, or credible source, multiple reports, sustained interest, etc.).
B	Intelligence indicates a **moderate interest** in using the attack method against the sector in the United States or Western Europe (e.g., multiple reports from different sources of varying credibility, recurring interest, etc.).
C	Intelligence indicates a **weak interest** in using the attack method against the sector in the United States or Western Europe (e.g., few reports of less than credible sources, anecdotal interest, etc.).
D	Any group has had a successful attack, failed attack, or disrupted operational plan to launch an attack against the sector outside of the **United States or Western Europe** using the attack method described.

Combining the Estimates

There are two ways of combining the intent and capability levels, depending on the needs of the overall risk model. The SHIRA model requires the quantification of the threat to support its risk analysis. This approach uses a measurement of severity as a proxy for probability, and each capability and intent levels are assigned a value between 0 and 1. By using a consistent logic to adjust the intervals between the values, the scale reflects analytic judgments of distance between the levels and translates the ordinal rankings into a cardinal value. Because the SHIRA model treats the two aspects of threat separately, it treats *estimated capability* and *intent to attack* as independent probabilities. The threat, therefore, is a function of (or the multiplication of) the capability and the intent to attack. The product is a value on a scale of 0 to 1.0 and used as the threat ranking in the SHIRA equation, treated equally with vulnerability and consequence. For risk models that do not allow multiplication or cannot utilize a quantified threat level, the SHIRA threat model can combine the two factors with Boolean logic and produce a threat level on a low to high scale, as appropriate (see Figure 2).

Current Capability: 4							
Effort to Acquire: 4							
Current Capability: 3							
Effort to Acquire: 3							
Current Capability: 2							
Effort to Acquire: 2							
Current Capability: 1							
Effort to Acquire: 1							
Current Capability: 0							
	A	B	C	Tier 1	D/ Tier 2	Tier 3	Tier 4

Figure 2: An illustration of Boolean combination of intent and capability levels where red indicates high, orange indicates medium-high, yellow indicates medium, blue indicates medium-low, and green indicates low.

The equation for $\mathbf{T_P}$ is:

$$\mathbf{T_P = (I \times Ca)} \quad \textit{(Equation 5)}$$

The final number provides an indication of the relative severity of the threat for each attack scenario and represents a probability that an attack will occur.

SHIRA Vulnerability and Consequence

DHS works closely with the infrastructure protection community, through the NIPP framework, to obtain data and analytic judgments on vulnerability and consequence. SSAs, representing a unique community of interest within infrastructure, provide the expert judgments for their respective sector. Each sector utilizes the intelligence-based terrorist attack methods to create relevant scenarios for their sector under the guidance of worst-most likely; the SSAs apply an attack method to an asset, representative asset, or system in their sector that represent the worst-most likely scenario. For each scenario, a vulnerability and consequence rankings are determined through the SHIRA model framework.

Framework for the Analytic Process

Similar to the process for the threat assessment, the vulnerability and consequence assessments follow the steps of defining thresholds and providing ranking guidance. DHS works with representatives from the SSAs who determine which attack methods pose nationally significant risk in their respective sectors and assess the consequences of and vulnerability to those potential terrorist attacks.

Vulnerability

The SSAs take into account three different aspects of vulnerability: (1) the difficulty in identifying the asset and its criticality; (2) the effectiveness of the countermeasures in place in preventing the attack from succeeding; and (3) if the countermeasures fail, whether the attack will have the desired effect. This last consideration allows the SSAs to evaluate the robustness or the degree to which a CI/KR system can resist the attack. In many infrastructure systems, individual nodes may be highly vulnerable, but the system is still highly resistant to the destruction or disruption of a single node. As with the other risk factors, the SHIRA process provides the definitions and guidance for ranking each component of vulnerability.

Table 4: Ranking Levels for Vulnerability					
Component	**Ranking Level**				
	0	**1**	**2**	**3**	**4**
Recognizability	Asset is very unlikely to be recognized; adversary would require a highly trained expert or access to classified or highly sensitive information	Asset is unlikely to be recognized; an adversary would require some special knowledge or training	Asset is somewhat likely to be recognized; an adversary would require a moderate amount of research	Asset is likely to be recognized; an adversary could identify this asset will minimal effort.	Asset is very likely to be recognized; any adversary could easily identify this asset.
Countermeasure Effectiveness	The existing counter-measures are very likely to defeat the attack.	The existing countermeasures are likely to defeat the attack.	The existing countermeasures are somewhat likely to defeat the attack.	The existing counter-measures are unlikely to defeat the attack.	The existing countermeasures are very unlikely to defeat the attack.
Robustness / Resistance	The asset is very likely to resist, withstand, or contain the damage from the attack.	The asset is likely to resist, withstand, or contain the damage from the attack	The asset is somewhat likely to resist, withstand, or contain the damage from the attack.	The asset is unlikely to resist, withstand, or contain the damage from the attack.	The asset is very unlikely to resist, withstand, or contain the damage from the attack.

The variable used for the likelihood of vulnerability to an attack method, $\mathbf{V_P}$, is based on government expert judgments of three factors.

- Recognizability (**Rg**): The likelihood that the adversary will be able to identify and locate the asset and its significance, taking into consideration labeling, signage, press, uniqueness, and the adversary's knowledge.
- Countermeasure Effectiveness (**Ce**): The effectiveness of the countermeasures protecting the asset, specifically in the areas of denial, detection, and interdiction.
- Robustness / Resistance (**Rs**) The asset's or system's level of ability to sustain the attack without countermeasures, due to inherent resistance, system resistance, and independence.

Each component is ranked on a 0 to 4 scale, and each ranking is assigned a value in the range of 0 to 1. As with threat, the intervals between the values assigned to each level of vulnerability are set to represent analytic judgments of their contributions to an overall vulnerability level. These values are multiplied, hence,

$$\mathbf{V_P = Rg \times Ce \times Rs} \quad \textit{(Equation 6)}$$

The final number provides an indication of the relative severity of the vulnerability for each attack scenario and represents a probability that an attack will succeed.

Consequence

To assess consequences, SSAs consider loss of life, economic losses, and the psychological or behavioral impact of an attack, as described in each attack method, in a worst, reasonable case scenario. Ranking tables are then used to standardize responses and assign values that range from negligible consequence to catastrophic national consequences.

Table 5: Ranking Levels for Consequence

Component	Ranking Level (SHIRA Severity)				
	0 **None/ Negligible**	**1** **Minor**	**2** **Moderate**	**3** **Significant**	**4** **Catastrophic/ Severe**
Loss of Life	Attack likely to produce no fatalities	Attack likely to cause less than 100 fatalities	Attack likely to cause greater than 100 fatalities	Attack likely to cause greater than 1,000 fatalities	Attack likely to cause greater than 10,000 fatalities
Economic Losses	Estimated costs from the attack are likely less than $100 million	Estimated costs from the attack are relatively minor, in the range of $100 million to $1 billion	Estimated costs from the attack in the range of $1 billion to $10 billion	Estimated costs from the attack in the range of $10 billion to $100 billion	Estimated costs from the attack in excess of $100 billion
Psychological / Behavioral Impact	No major change in population behavior, or effects on social functioning locally or nationally.	Occasional or minor loss of nonessential social functions in a circumscribed geographical area.	Loss of many nonessential social functions in a circumscribed geographical area.	Dysfunctional behavior and disruption of important social functions for a sustained period.	Loss of belief in government and institutions; widespread disregard for official instructions; widespread looting and civil unrest.

The consequence of a potential terrorist act is based on several constituent components: loss of life, economic losses, and the psychological impact on the populace, and is represented by the variables **L, E,** and **Ps**, respectively. The estimates can be based on expert opinion, quantitative assessments, if available, or modeling and simulation, if applicable. The framework ranks these components from 0 through 4. These component values are added for a cumulative total and normalized. The final number provides an indication of the relative consequence for each attack scenario.

The consequence rankings are measures of severity in the context of the SHIRA and are assessed on a common interval scale, where the assessed severity is equivalent within each column and rises linearly from one description to the next in each row. The broad range in each severity level is a result of the scope of the SHIRA, a national level assessment inclusive of all CIKR sectors. The interval scale also allows for a national level risk framework that can incorporate more granular assessments of specific assets and systems. The components of consequence follow a logical progression for national level consequences horizontally; vertically, the severity levels provide levels of equivalency that reflect the current decision-making judgment of the DHS. These equivalencies can be modified based upon decision-maker input.

To get the total consequence, the SHIRA takes the average of the consequence components:[17]

C = (L + E + P) / 3 *(Equation 7)*

The SHIRA model normalizes the consequence to a range of 0-100 by multiplying by 25:

C = [(L + E + P) / 3] * 25 *(Equation 8)*

Combining the Components for Risk

To produce the final value for the risk of the scenario, the SHIRA multiplies the value for consequence from Equation 8 by the probability that the scenario will occur, which in the SHIRA is the product of the threat and vulnerability variables.

In this view, the process of computing the value of risk is equivalent to calculating the expected value of a random variable with two possible states – C, the consequence of the attack scenario succeeding, and 0, the consequence of the attack scenario not succeeding.[18] Thus:

R = Prob(attack does not succeed) * 0 + Prob(attack succeeds) * C *(Equation 9)*

R = Prob(attack succeeds) * C *(Equation 10)*

R = (T * V) * C *(Equation 11)*

In this context, the risk value is the expected severity of the consequence.

Path Forward

The SHIRA is a semi-quantitative risk assessment that utilizes tables as guidance for the IC and infrastructure protection community representatives to estimate the components of threat, vulnerability, and consequence. The success of the SHIRA comes from understanding of the requirements for a national CIKR risk assessment coupled with the constraints and limitations of processes, products, people, and technology. The threat rankings provided by the interagency coordination of the IC are the basis for a DHS assessed probability for each ranking. Likewise, the vulnerability rankings provided by the Sector Specific Agencies that represent each CIKR sector, are converted to probabilities by DHS. Additional enhancements to the threat and vulnerability components should focus on the core principles of sound risk analysis. For example, as

[17] Because we consider severity to increase linearly from one linguistic description of each component to the next, averaging is a proper way to obtain a unified measure for consequence severity.

[18] Such a variable is called a Bernoulli random variable and its expected value is
E[variable] = Prob(State1) * Value(State1) + Prob(State2) * Value(State2).

the data become more readily available to DHS, more detailed tables that standardize probabilities associated with the tables will produce more repeatable results. The consequence estimates are based upon large nationally significant ranges; similarly, future enhancements should focus on refining the ranges to allow an easier integration of more detailed analysis.

Several terrorist attack scenarios exist that could lead to consequences not captured under Loss of Life, Economic Losses, or Psychological Impacts factors. For example, while a single attack on a Defense Industrial Base asset could cause health, economic, and psychological impacts, the primary consequences may be a hindrance to the military's operational capacity. Consequently, mission disruption should be added as a fourth consequence factor that could enable all SSAs to account for the impact of an attack on national security and federal operations, public health and safety, and essential public services.[19] By evaluating these effects, the SHIRA could compile a more complete picture of the risk to the nation's CIKR.

The current scope of the SHIRA focuses the assessment of terrorism risk at the strategic level. Although it will remain there, the enhancements and refinements to the model should allow for integration with other models more pertinent for operational and tactical levels. As risk assessments to specific assets and systems proliferate within the infrastructure protection community, DHS should identify and exploit areas of integration. Horizontal and vertical integration of risk analysis and data will provide the backbone for a shared understanding and communication of risk at all levels. Horizontal integration requires information sharing (data, analysis, knowledge) not only within the infrastructure protection or intelligence domains, but also throughout all the components of DHS. The Science and Technology Directorate, for example, provides DHS access to the research capabilities of the nation's universities through the Centers of Excellence. Integration with new research and technology will enable the current practices to reduce the constraints and limitations of current models.

[19] Although the definitions in the guidance documents seem to focus exclusively on governmental functions, the mission areas described go beyond the public sector. Services such as the "orderly functioning of the economy" involve private organizations in the banking and finance sector; the provision of drinking water is an essential service, and in many cases utilities are private entities.

The definitions used in Homeland Security Presidential Directive-7, the National Infrastructure Protection Plan, and the Homeland Security Act have areas of overlap. To help create a mission disruption–consequence factor, the SHIRA team simplified the six components into three groups of mission impacts:

- **Federal and National Security Impact** includes the first two missions (Ensure National Security, Perform Federal Missions) because they both focus on a national scale.
- **Public Health and Safety Impact** includes the next two components (Ensure Public Health and Safety, Maintain Order) because maintaining order is an integral part of ensuring public health and safety.
- **Provide Essential Public Services** group the remaining two components (Provide Essential Public Services, Ensure Orderly Economy) because the best way to ensure an orderly functioning economy is to provide essential public services, especially safe, secure, and reliable banking and finance services.

Conclusion

The foundation of threat-based risk analysis in the SHIRA can serve as the bedrock of future terrorism risk analysis to critical infrastructure at DHS. As the accessibility to critical infrastructure data increases and as the IC becomes more familiar with the infrastructure protection community's needs, the quality of the risk analysis will improve with the more granular or more direct data. The "fusion" concept, under which the SHIRA is produced, if nurtured and allowed to develop into its full potential, will help DHS to fully realize a nascent culture. The SHIRA is a model, methodology, and product developed through the interactions of the various communities of interest along the common thread of threat-based analysis. Its success serves as a microcosm of homeland security: a success based upon the interactions of once disparate entities brought together under a single focus.

Information sharing and collaboration are the fulcrums on which terrorism risk analysis depend; the communities of interest in both the IC and the infrastructure protection community provide a depth and breadth of knowledge that only DHS can harness. DHS alone is the organization that can bring together the private and public sectors of the infrastructure protection community; DHS alone is the organization that can, through its own intelligence organization, bring the IC to the infrastructure protection community; and DHS alone is the organization that can synthesize the data and analysis together to formulate a terrorism risk assessment for critical infrastructure protection. As DHS grows beyond five years, we can assume that information sharing and collaboration will increase and improve between all stakeholders. This will lead to more data to analyze; more data, however, do not indicate better data and better data do not point to better analysis. Greater accessibility to data – both intelligence and critical infrastructure – will allow for more rigorous analysis of terrorism risk and finer granularity in the assessments. The threat-based terrorism risk analysis being cultivated today through projects like the SHIRA will allow DHS to harvest plentifully in the future.

AUTHOR BIOGRAPHY
Geoffrey French is a Program Manager for CENTRA Technology, Inc, and currently supports strategic risk analysis for the U.S. Department of Homeland Security. Mr. French has supported counterintelligence analysis and operations for the Federal Bureau of Investigation and the U.S. Department of Defense. He has a B.A. in History from Wichita State University and an M.A. in National Security Studies from Georgetown University. He is a founding member of the Security Analysis and Risk Management Association.

AUTHOR BIOGRAPHY
Jin Kim is an Analyst for CENTRA Technology, Inc, and currently supports strategic risk methodology and analysis for the U.S. Department of Homeland Security. Mr. Kim has worked in the intelligence community for over ten years -- from tactical Army assignments to strategic assignments supporting the Department of Defense. He has a B.S. in General Engineering from the United States Military Academy and an M.A. in Security Studies from the School of Foreign Service at Georgetown University.

AUTHOR BIOGRAPHY
Pasha Vasilev is an Analyst for CENTRA Technology, Inc, and currently supports a variety of analytical and open source research projects. Mr. Vasilev has worked on assignments involving mathematics and technology for more than five years. He has a B.A. in Computer Science from Harvard University and an M.A. in Law and Diplomacy from The Fletcher School at Tufts University.