UCRL-JC-
PREPRINT 122784

CONF-960647--2

A Probabilistic Security Risk Assessment Methodology for Quantification of Risk to the Public

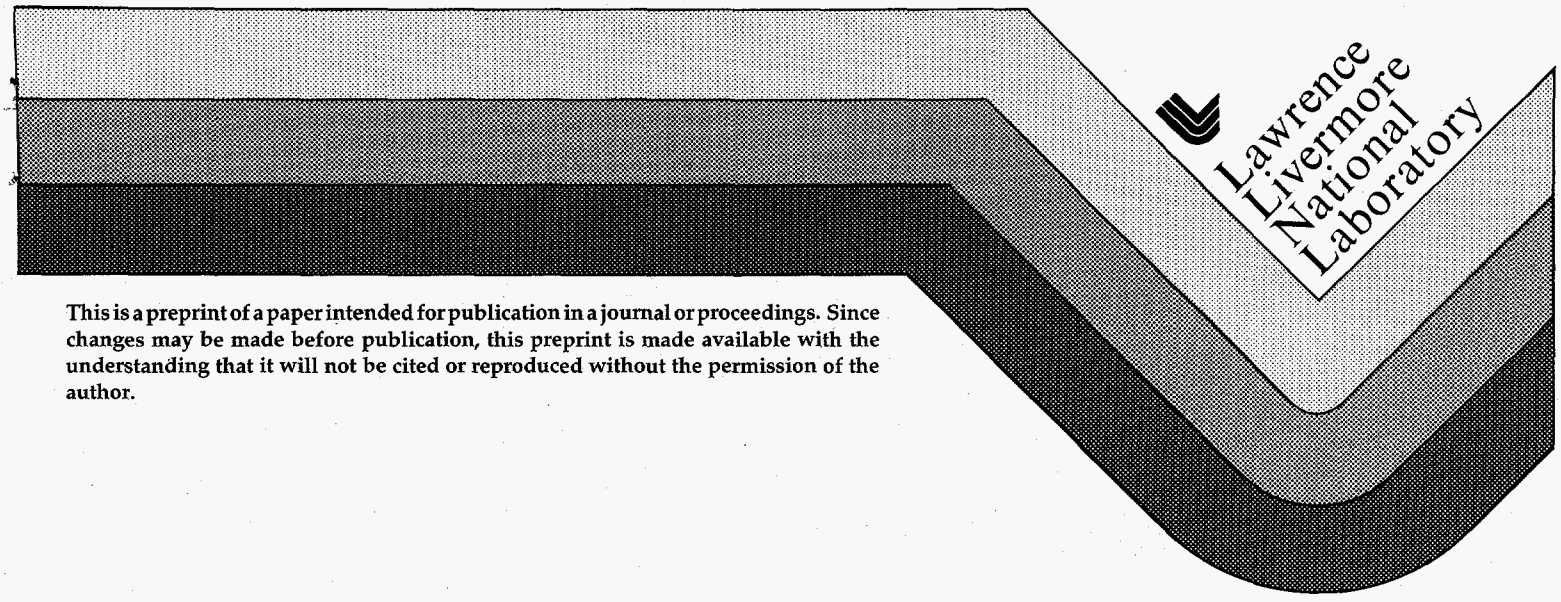
Douglas Stephens, John A. Futterman, Alfred A. Parziale, Andrew Randazzo, and Arnold S. Warshawsky

Lawrence Livermore National Laboratory

This paper was prepared for submittal to the
PSAM-III/ESRL '96
International Conference on
Probabilistic Safety Assessment and Management

Crete, Greece
June 24 - 28, 1996

January 19, 1996



A Probabilistic Security Risk Assessment Methodology for Quantification of Risk to the Public*

Douglas Stephens, John A. Futterman, Alfred A. Parziale,
Andrew Randazzo, and Arnold S. Warshawsky
Lawrence Livermore National Laboratory
Livermore, CA 94551 USA

Abstract

We describe a methodology for obtaining probabilistic risk estimates of deliberate unauthorized acts, integrating estimates of frequencies of serious plots, probabilities of avoiding detection and interdiction, probabilities of successful action, and consequences of the act. This methodology allows us to compare the risks of deliberate acts with those of accidents and to identify the most cost-effective risk reduction measures through cost-benefit analysis.

1 Introduction

Quantitative probabilistic *safety* assessments in the chemical and petroleum industries, in nuclear power and nuclear weapons, and in the health sciences, environmental protection, waste management, aerospace, and transportation date to the 1970s. Extensive databases of accident scenarios, likelihoods, consequences, and cost-benefit estimates for risk reduction have been developed. Thus quantitative probabilistic safety assessment of public risk is relatively mature.

Nuclear *security* assessment is also relatively advanced. The U.S. departments of Energy and Defense have policies and standards for site security. Each site prepares security plans, carries out self-assessments, and undergoes inspections to ensure compliance. Verification is estimated through force-on-force (FOF) exercises using Multiple Integrated Laser Engagement System (MILES) equipment, vulnerability and conflict simulation, and expert judgment.

In most such security assessments, however, only conditional probabilities for defeating a security attack are obtained. Estimates of public risk are not obtained, because the frequency of attack is not estimated but is set to unity.

Quantification of security risk is required if overall public risk (comprising both safety and security risks) is to be reduced. Moreover, quantification makes it

* Work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

possible to rank risk-reduction options using cost-benefit calculations. Costs include R&D to establish technical feasibility, implementation costs, and impacts on operations and/or safety. Benefits generally result from avoided "incident costs"—the product of the costs and lifetime probability of an incident. Combination of cost-benefit analysis with decision analysis allows the optimization of public surety (safety and security) with limited resources (funds, personnel, etc.).

We have developed a methodology that yields an overall probabilistic estimate of the risk to the public from terrorist capture of a U.S. nuclear weapon. We believe that the methodology is readily applicable to quantitative security assessments for other deliberate acts, such as theft of fissile material.

2 Methodology

Figure 1 outlines the methodology. Given a threat assessment, one estimates attack likelihoods and interdiction probabilities, characterizes the attack site, conducts conflict simulation, and quantifies the consequences of a successful attack.

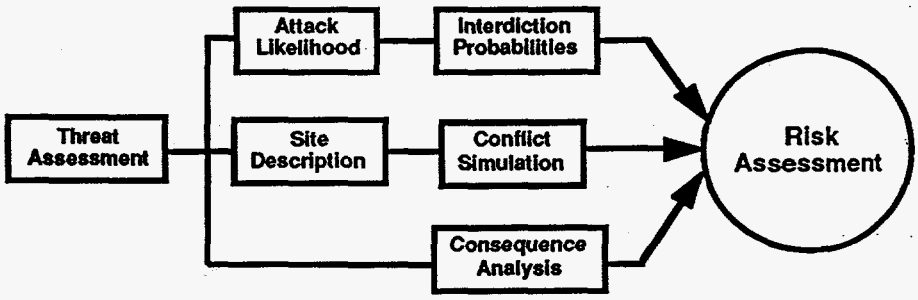


Figure 1. Probabilistic Security Risk Assessment Methodology.

We calculate the risk R of a deliberate unauthorized act as a product of frequencies and conditional probabilities:

$$R = F_0 P_{AI} P_T C, \tag{1}$$

where

F_0 = frequency of serious attempts to carry out the act (also called the frequency of human intent). Factors influencing F_0 include the goals of the adversaries, the risks they undergo vs the value of the act to them, and the difficulty of acquiring the resources necessary to carry out the act.

P_{AI} = Conditional probability of avoiding detection, prevention, and interdiction, from the time of decision, through obtaining approvals and resources, acquiring weapons and equipment, surveilling the site, and assembling the team at the site to carry out the act.

P_T = Conditional probability of success in carrying out the act.

C= Consequences of a successful act.

Figure 2 gives a simple overview of the terrorist scenario and risk computation for the case of attempted possession and detonation of a nuclear weapon. Frequencies and probabilities are indicated in the figure as terrorist attempts propagate to only one of several outcomes, some leading to success, some to failure. Terrorist attempts begin with serious plots at frequency F_0; if there is no plot, there is no following threat. If a plot occurs, either it is interdicted before an assault is launched on a site containing a weapon, in which case there are no adverse effects, or it is not interdicted before the attack, with probability P_{AI}.

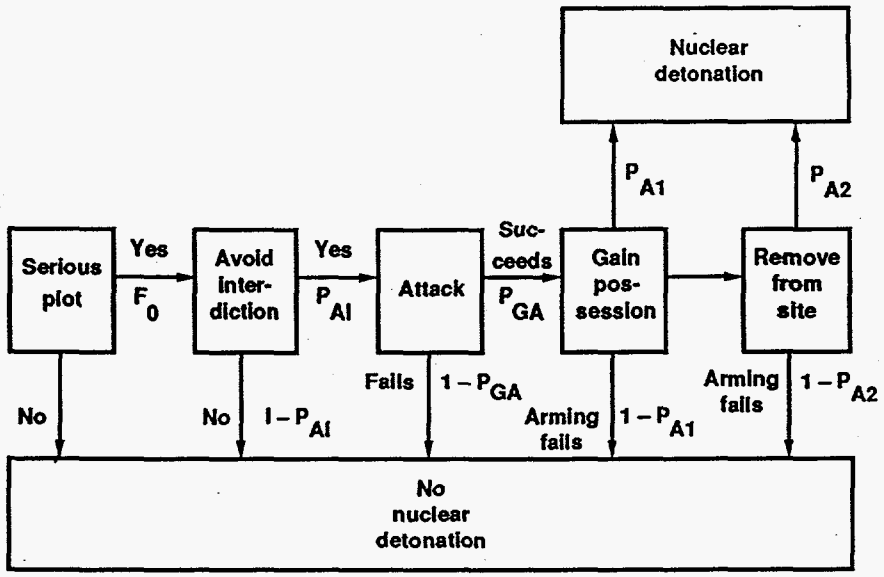


Figure 2. Terrorist scenario for attempted theft and detonation of a nuclear weapon, showing principal frequencies and probabilities used in risk computation.

Once the attack starts, the terrorists may fail to gain possession of a nuclear weapon, in which case no detonation ensues. Conversely, there is a probability P_{GA} that they gain possession of a weapon.

The terrorists now have possession and either attempt to arm and detonate the weapon on-site with probability P_{A1} or fail with the result that no nuclear detonation occurs (although non-nuclear detonation, with fissile material dispersal, is possible). The second pathway is that the attackers remove the weapon off-site and attempt to arm and detonate it at another location, with a probability P_{A2}. Again, if the attackers fail, no nuclear detonation occurs. In this example, then, the factor P_T in Eq. (1) is given by $P_{GA}P_{A1}$ or $P_{GA}P_{A2}$.

The consequences in this example would result from nuclear detonation or fissile material dispersal, and would vary strongly depending on local conditions.

3 Computations

3.1 Frequencies of Serious Plots

To estimate frequencies of human intent, one should use direct or (if necessary) surrogate data. If no relevant data exists, expert judgment must be elicited. In any case, the frequency of human intent is likely to be the most uncertain element in a risk assessment.

For a LLNL case study of attempted theft and detonation of a nuclear weapon, no relevant data existed, so we estimated plot frequencies by eliciting expert judgment from the nuclear counter-terrorism community. The resulting probability distribution spanned a wide range.

3.2 Likelihoods of Avoiding Preemption

Similarly, the likelihoods of adversaries avoiding detection and preemption can be obtained from law enforcement and counterterrorism data [1, 2] and/or by elicitation of expert judgment. Some agencies collect data on attempts that were detected and preempted as opposed to those that were successful, so this estimate should be much less uncertain than values for plot frequencies. In our case study, we used both expert judgment and FBI statistics [2].

3.3 Probabilities of Successful Theft or Attack

Likelihoods of successful theft or attack can be estimated using vulnerability assessments. The U.S. Department of Energy uses ASSESS (Analytic System and Software for Evaluating Safeguards and Security) [3] and SEES (Security Exercise Evaluation System) [4] for this purpose.

ASSESS develops an adversary sequence diagram or a critical-path representation of a facility. Many scenarios (paths, safeguard components, procedures) and both insider and outsider threats can be modeled. The model calculates a risk based on the probabilities of interruption and neutralization of the adversaries. ASSESS is fast and powerful, but its neutralization model is simple and does not include conflict simulation. For conflict simulation, we use SEES.

The SEES conflict simulation is high-resolution, item-level, multi-sided, event-driven, and interactive: the location of each soldier is calculated, given the posture and movement orders specified by the operator(s). Lines of sight and small arms fire (and associated hits and kills) are calculated automatically. Delays can be programmed for physical security features such as berms, fences, and locks. A complete FOF simulation involving several tens of combatants can be simulated by as few as two operators.

Wurtsmith AFB and Ellsworth AFB have reported good agreement between SEES simulations and actual FOF exercises. SEES can be used to pre-screen scenarios for actual FOF exercises, and it offers more reliable statistics than individual FOF exercises.

We have used LLNL's SEES conflict simulation to model the outcomes of terrorist attacks on an example weapons storage site. We modeled two scenarios: on-site arming of a weapon, and theft of a weapon from the site.

We developed a representation of the storage site (local topography, roads, fences, gates, cameras, intrusion sensors, storage bunkers, towers, and other buildings). Then we specified force structures (armament, vehicles, and communications). We divided the defenders into roving patrols, quick-response forces in storage-area buildings, and security-response forces off site. The attackers approached the site on foot and in a truck; if any survived, they left the site by truck, and, if they removed a weapon from a bunker, by helicopter.

Since SEES is event-driven, we could collect a variety of statistics, including timelines for the engagement, shots fired, hits, misses, and kills, and attacking or defending force levels. Thus we could explore the influence of force structure, doctrine, and tactics on force draw-down over time, defender and attacker success probabilities, and the duration of attacker contact with a weapon.

4 Consequences

Consequences can be expressed in many ways. The consequences of the theft and detonation of a nuclear weapon depend strongly on the details of the detonation mode, location, population density, and weather conditions and may vary from trivial effects to hundreds of thousands of fatalities.

These effects (property damage, contamination, health effects, and fatalities) can be estimated by regional transport, diffusion, and fallout codes that contain appropriate biological models. Existing models include the transport and diffusion codes MATHEW/ADPIC [5], which allow for terrain dependence, and ERAD [6] and KDFOC3 [7] for fallout computations. Consequences may be expressed by metrics such as contaminated land areas or fatalities, or they can be converted to monetary terms by suitable cost analysis [8].

5 Conclusion

We have described a methodology for combining estimates of frequencies of serious plots, probabilities of avoiding detection and interdiction, likelihoods of successful theft, and consequence analysis to carry out probabilistic risk estimates of deliberate unauthorized acts. Thus risks to the public can be assessed and compared with risks of high-consequence accidents. Methodologies, codes, and some databases are available, although more work is needed.

Conflict simulation using high-fidelity combat models such as SEES can highlight potential site security problems and solutions, including alternative tactics by security personnel and alternative protective features and equipment.

Finally, the assessment process in itself provides a number of valuable insights into the threat, vulnerabilities, and the more cost-effective risk reduction measures.

References

1. Patterns of Global Terrorism 1993. Office of the Secretary of State, Office of the Coordinator for Counterterrorism, Department of State Publication 10136, April 1994
2. Terrorism in the United States 1993. U.S. Department of Justice, Federal Bureau of Investigation, Terrorism Research and Analysis Center, National Security Division, 1994
3. Al-Ayat R. A., Cousins T. D., and Matter J. C., An Overview of ASSESS—Analytic System and Software for Evaluating Safeguards and Security. In: Proceedings of the 30th Annual Meeting of the Institute of Nuclear Materials Management, Orlando, FL, July 1989
4. Friedman G., The Security Exercise Evaluation System (SEES) V2.0 Accreditation Process. Lawrence Livermore National Laboratory, Livermore, CA, UCRL-ID-113105, April 1993
5. Lange R., ADPIC—A Three-Dimensional Particle-in-Cell Model for the Dispersal of Atmospheric Pollutants and its Comparison to Regional Tracer Studies. J. Appl. Meteor. 1978; 17:320–329
6. Boughton B., and DeLaurentis J., Description and Validation of ERAD: An Atmospheric Dispersion Model for High Explosive Detonations. Sandia National Laboratory, Albuquerque, NM, SAND92-2069, 1992
7. Harvey T., Serduke F., and Peters L., KDFOC3: A Nuclear Fallout Assessment Capability, Lawrence Livermore National Laboratory, Livermore, CA, UCRL-52338 draft in progress
8. Stephens D. R., Hall C. H., Holman G. S., Graham K. F., Harvey T. F., and Serduke F. J. D., Probabilistic Cost-Benefit Analysis of Enhanced Safety Features for Strategic Nuclear Weapons at a Representative Location. In: Proceedings of PSAM-II, Vol. 2, session 57, pp. 13–18, San Diego, CA, March 20–25, 1994

DISCLAIMER