

GLOBAL THREAT REDUCTION INITIATIVE



Subgroup Exercise 7, Part 3

Task 1

Objective: Apply information from previous lectures and exercises to develop a more effective security system for the radioactive materials. The exercise will be conducted as a team (for each sub-group), and will be facilitated if the group can divide the responsibilities contained in the tasks below to specific team members. The Sandia Sub Group facilitator will provide assistance as requested, but will otherwise only observe.

Threat: Assume a threat of two persons, one of which is an active insider. The insider has access and authorities appropriate for the role. Limit the insiders to either: a guard, a radiation worker, a manager, or a member of housekeeping staff. The insider is either: bribed, disgruntled or coerced. If coerced, insider will not harm anyone. If bribed, insider will not harm co-workers. If disgruntled, insider will harm all. The outsider adversary is a criminal (or terrorist) desiring theft of radioactive material (or sabotage and release of radiation). Tools of the outsider are any tools than can be purchased by the public, a small utility van or truck, a handgun and/or hunting rifle, and a small amount (5 kgs) of TNT, and knowledge and experience with the tools, weapons, and explosives.

- Assumptions:**
- Police can respond to UMC 7 minutes: number of police and weapons in 1st response based on actual situation in Lithuania.
 - Adversary delay introduced by the 1 officer is 15 seconds, 2 police officers is 45 seconds
 - Follow up response to UMC in 18 minutes: number of police and weapons in follow up response based on actual situation in Lithuania.
 - Unless tactical plan and UMC familiarity exists for police, an additional 10 minutes is required for deployment to target area (if needed).
 - Tactical Entry requires an additional 5 minutes after deployment to target area
 - Neutralization Success:

# of Police Officers	Contain 2 Adversaries at UMC perimeter (theft)	Contain 2 Adversaries at source room (theft)	Tactical Entry and Neutralize 2 Adversaries (sabotage)
1	Very Low	Medium	Very Low
2	Low	High	Low
3	Low	Very High	Medium
4	Medium	Very High	High
5+	High	Very High	Very High



Sandia National Laboratories

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. . SAND# 2013-



GLOBAL THREAT REDUCTION INITIATIVE



- Required effectiveness :
 - Both Detection (timely) and Neutralization effectiveness: High
 - Or Either Detection or Neutralization Effectiveness Medium, and other is Very High

Scenario 1:

- A. Selecting either the Blood Center or Vivarium, brainstorm possible weaknesses in the UMC security system detection, access control, delay or response.
- B. Develop an adversary scenario (using the exercise 5 scenario as an example) to steal a radioactive source or entire device from the blood bank or Vivarium using the adversary threat defined above.
- C. Estimate the adversary delay along the scenario path, and the points of possible detection, along with their likelihood (H, M, L) using data developed in exercises 4 and 5.
- D. Employing response assumptions, estimate likelihood of security system effectiveness (i.e. estimate detection effectiveness and neutralization effectiveness)
- E. Develop detection, assessment, access control, delay and response improvements to improve effectiveness
 - a. Try to minimize cost of improvements
 - b. Try to minimize operational impact of improvements
 - c. Estimate detection and neutralization effectiveness and compare to requirement.

Scenario 2:

- A. Selecting either the Blood Center or Vivarium, brainstorm possible weaknesses in the UMC security system detection, access control, delay or response.
- B. Develop an adversary scenario (using the exercise 5 scenario as an example) to sabotage in place the radioactive source(s) or entire device from the gamma knife using the adversary threat defined above.
- C. Estimate the adversary delay along the scenario path, and the points of possible detection, along with their likelihood (H, M, L) using data generated in Exercises 4 & 5.
- D. Employing response assumptions, estimate likelihood of security system effectiveness (i.e. estimate detection effectiveness and neutralization effectiveness)
- E. Develop detection, assessment, delay and response improvements to improve effectiveness
 - a. Try to minimize cost of improvements
 - b. Try to minimize operational impact of improvements
 - c. Estimate detection and neutralization effectiveness and compare to requirement.

Output

Prepare a summary briefing of both scenarios, including results of all 5 steps for each scenario. Briefing does not require a slide presentation.

