Appendix B: Systems Analysis and Verification Research

In its review of verification technology research, OTA found little large-scale systems analysis in comparison with that usually applied to weapons technology research (as in the case, for example, of SDI). This appendix illustrates one such kind of analysis, "network analysis" that could be applied to verification technology problems.

Introducfion: Judgments Under Uncertainty

Assessing the value of arms control provisions, regimes for verifying compliance, and specific monitoring systems for those regimes involves many complex judgments that must be made under conditions of uncertainty. Nevertheless, the Senate must implicitly or explicitly make such judgments (or accept the judgments of others) when it chooses or declines to ratify an arms control treaty. Both Houses of Congress acceptor reject such judgments when they choose to support or modify Administration proposals for arms control verification technology research.

There is no way to eliminate all the uncertainties surrounding these judgments. No technical calculations can dispel uncertainties about future events or settle disagreements about the values to place on policy outcomes; therefore, calculations will not produce objectively "right" answers. Nevertheless, it is possible to apply analytic methods that clarify where the uncertainties lie and make more explicit the assumptions of those proposing different courses of action. Such methods may at least produce *better* answers than the unstructured playing of hunches. They may also lead to identification of areas of research that could reduce some uncertainties.

NetworkAnalysis of Evasion Strategies and Verification Measures

Analysts at Lawrence Livermore National Laboratory have suggested a method to ". . identify potential weaknesses in [an] overall treaty verification system, to highlight the evasion and breakout strategies least likely to be detected or deterred, and to determine the individual verification measures that offer the greatest benefit."[18] They propose a five-phase process of analysis, outlined below.

1. Identify Soviet Evasion Objectives

Determine how particular evasive actions might lead to a militarily significant advantage. If different objectives are possible, assign relative weights to them.

2. Develop Network Model of Evasion Strategies

A simpli.tied example of such a model is given in figure 4. Developing the model involves identifying steps that the Soviets would have to perform to achieve their objectives. Evasion strategies consist of sequences of steps that would lead to deployed weapons (or other treaty violations). The example the Liver-more analysts use is a network for the manufacture of small, single-stage ballistic missiles.

3. Estimate Evasion Probabilities

Estimate the probability that treaty evasions associated with each step in the network would be undetected by verification measures in force at that step. These estimates are by nature subjective judgments. Analysis of this kind forces the experts to make their judgments explicit. Agreement among experts would be desirable, but where disagreements exist, analysts can perform separate evaluations to show what differences those disagreements make. Moreover, additional technical research on specific verification measures may narrow the range of disagreements and increase confidence in judgments.

4. Determine Evasion Strategies Least Likely To Be Detected

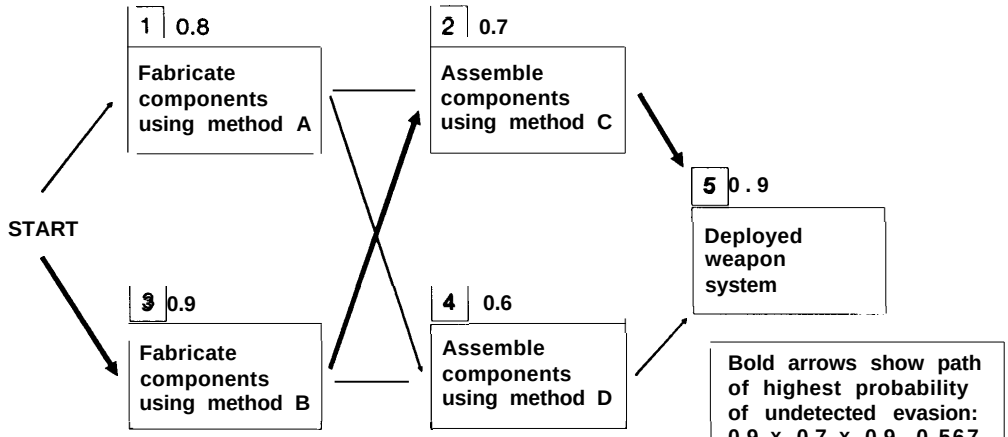
For each evasion strategy, multiply the probabilities of successful evasion of the individual steps.

5. Analyze Results and Perform Sensitivity Analysis

The advantage of **a systematic analysis like this is** that it clarifies the effects of varying assumptions, estimates, and strategies. For example, the analysis might show that a monitoring regime that had a relatively small chance of catching violations at each of several manufacturing steps would have a fairly high overall probability of detecting significant

[18] Thomas A. Edmunds and R. Scott Strait, *A Network Methodology for Evaluation of Treaty Verification Options* (Livermore, CA: Center for Technical Studies on Security, Energy, and Arms Control, Lawrence Livermore National Laboratory, September 1989), p. 1.

Figure 4--Network Representation of Evasion Strategies and Probabilities



Path	Undetected evasion probability	
o → 1 → 2 → 5	0.504	
0 → 1 → 4 → 5	0.432	
0 → 3 → 2 → 5	0.567	Highest probability of undetected evasion
o +3+4+ 5	0.486	

In this schematic diagram of possible paths to the deployment of a weapon system, each step has an estimated probability that it will go undetected. The likeliest evasion path is the one in which the multiplied probabilities of the steps come out the highest, in this case the path through steps 0,3,2, and 5. Note that efforts to reduce the probability of successful evasion at Step 3 to below O.8 could just induce the violator to use Step 1 instead, and therefore such efforts would not be worthwhile.

SOURCE: Adapted from Lawrence Livermore National Laboratory, 1990.

numbers of deployed weapons. Or, it might show that even greatly improving the chance of detection at one step might not be worthwhile, because it would simply cause the evader to choose an alternate step. Figure 4 illustrates this point.