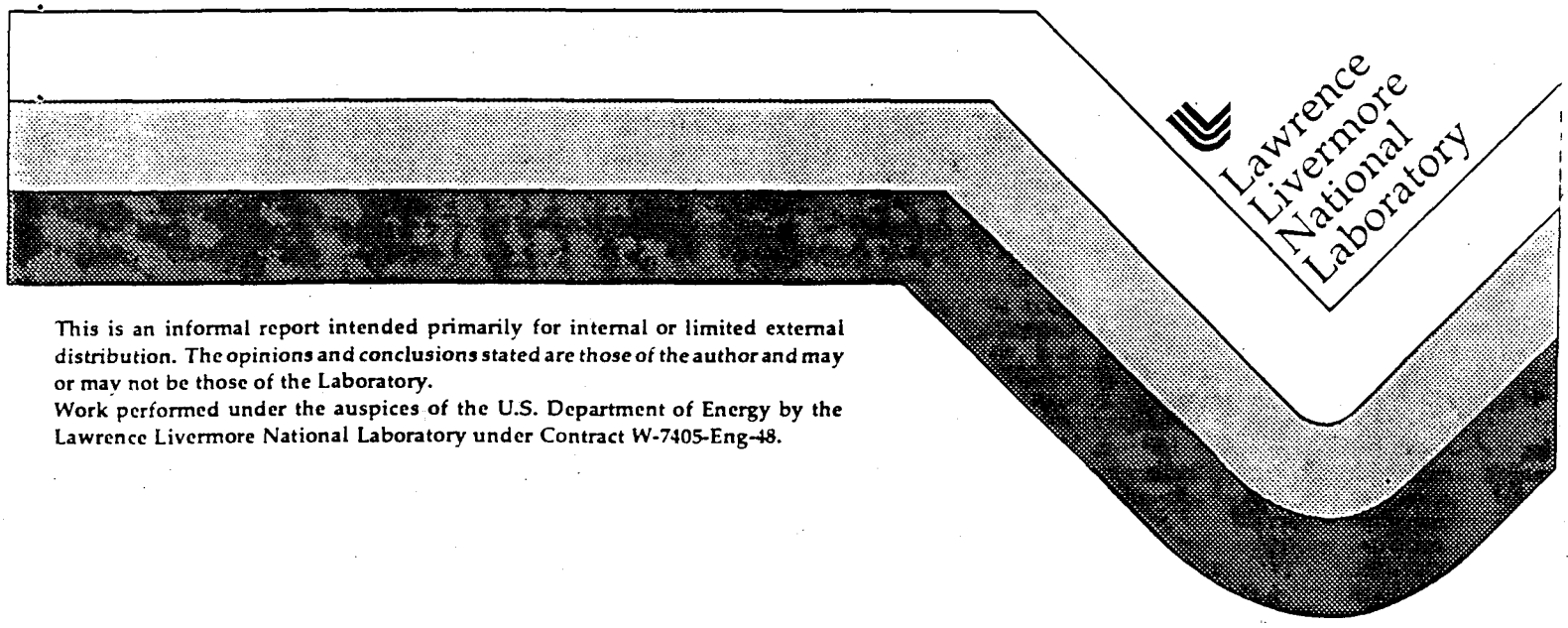
UCID-21817

A Network Methodology For Evaluation Of Treaty Verification Options

Thomas A. Edmunds
R. Scott Strait

September 1989



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

Price Code	Page Range
A01	Microfiche
Papercopy Prices	
A02	001-050
A03	051-100
A04	101-200
A05	201-300
A06	301-400
A07	401-500
A08	501-600
A09	601

UCID--21817

DE90 004487

Contents

Abstract

In this report, we develop a quantitative methodology using network theory to evaluate verification measures for a bilateral arms control treaty. The methodology is designed to accomplish an integrated evaluation of the total Soviet evasion potential and the complete verification regime while considering the interaction among different verification measures. The method can be used to identify potential weaknesses in the 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. The methodology is demonstrated using a hypothetical example of verification of limits on small single-stage ballistic missiles under a hypothetical treaty.

1. Introduction

Bilateral arms control treaties place numerical and other limits on many different strategic weapon systems. Monitoring compliance with a treaty requires a complex system relying on many different verification measures. These measures vary significantly in terms of their effectiveness, intrusiveness, and financial costs. Similarly, the verification measures are designed to detect and deter a wide range of possible Soviet treaty evasion strategies. Identification of acceptable, cost-effective verification measures is a challenging problem; these measures must maximize the ability to detect and deter Soviet violations and breakout attempts of greatest concern. An integrated evaluation of the complete arms control treaty verification system and the total Soviet breakout potential is required. The evaluation should incorporate interactions among the different verification measures and the possible Soviet evasion strategies.

In this report, we describe a quantitative evaluation methodology that addresses these needs. The methodology is based on a network representation of a complete verification system and the possible Soviet breakout strategies. It is designed 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. Its application is demonstrated by evaluating the verification of production and deployment limits for small single-stage ballistic missiles under a hypothetical treaty protocol.

Section 2 of the report presents the network evaluation methodology. Each of the subsections discusses one of the methodology's five phases in greater detail. Section 3 employs an example of verification of limits for small single-stage ballistic missiles under a hypothetical treaty to demonstrate the methodology. Section 4 summarizes the methodology, and two appendices provide further details on the methodology and the example.

2. Network Methodology

In negotiating verification provisions for an arms control treaty, the U.S. should consider the possibility of Soviet evasion and what constitutes a militarily significant evasion. The level of evasion that is militarily significant can be expressed in terms of specific Soviet objectives of covert production and deployment of various quantities of different weapon systems. Given a set of evasion objectives, we use the methodology to define a Soviet evasion strategy as a sequence of steps which may be taken to achieve an objective. The steps include those necessary for design, production, testing, and deployment

of the specific objective. There may be many feasible evasion strategies. From the U.S. verification perspective, we are most concerned with the evasion strategies that are least likely to be detected.

Possible treaty verification protocols may include a variety of different verification measures. Some measures may be more effective than others in detecting activities associated with the steps in a particular Soviet evasion strategy, and different verification technologies may complement one another in various ways. The uncertainty about whether a particular verification measure will be effective in detecting evasions is treated by assessing a probability of successful evasion at the steps where the measure is implemented. Our network methodology models the interaction among verification measures, evasion strategies, and successful evasion probabilities. The methodology provides a useful tool for ranking possible verification measures in terms of their deterrence effect.

The methodology is composed of five phases: (1) Identify possible Soviet evasion objectives; (2) Develop a network model representing all evasion strategies that meet objectives; (3) For each step in each of these strategies, estimate probability of evasion associated with verification technologies in force at that step; (4) Use an algorithm to determine evasion strategies least likely to be detected; and (5) Analyze results and perform a sensitivity analysis, repeating phases 2, 3, and 4 for different sets of verification measures. The remainder of this section discusses each of these steps individually.

2.1 Phase 1: Identify Soviet Evasion Objectives

In phase 1, the starting point for the analysis, we begin with the determination of what constitutes a militarily significant evasion of the treaty or potential for treaty breakout. Having determined the level of treaty evasion that constitutes a strategically significant advantage, we then identify specific Soviet evasion objectives that might provide such an advantage.

One general class of objectives involves the production of complete weapon systems in excess of the limitations imposed by treaty. These complete weapon systems could be stored or deployed at covert or declared sites. A second general class of objectives involves production and stockpile of major components of weapon systems. These component stockpiles represent a threat because, if the treaty were abrogated, complete weapon systems could be rapidly assembled to gain a strategic advantage in a short time period. We refer to such a scenario as a breakout.

When more than one Soviet objective is identified, we employ a weighting scheme in order to measure the relative desirability (for the Soviets) of meeting these various objectives. Each objective is assigned a relative value on a numeric scale. This value can then be combined with the highest probability of successful evasion for that objective to obtain an overall measure of verification system effectiveness.

2.2 Phase 2: Develop Network Model of Evasion Strategies

In phase 2, we develop a model that represents all Soviet strategies that may be used to evade verification measures in force and achieve the objectives. We represent an evasion strategy by a sequence of steps that must be performed in order to achieve a desired objective. Typically, these steps describe illegal production, testing, and deployment processes for a weapon. Thus, a means of completing all steps in this sequence without detection would correspond to an evasion strategy.

Determining how to divide the production, testing, and deployment of a weapon system into discrete steps depends on a number of factors. These include the production process and its choke points, the physical location of the different parts of the process, and the verification system to be evaluated. The monitoring points of the process for the different verification measures are very important in dividing the process into steps. Because different verification regimes may involve monitoring different steps, phase 2 may have to be repeated for each regime.

It is useful to develop a geometric representation of the interrelationships among production steps, strategies, and objectives. To this end, we employ a network model. In order to illustrate this concept, we consider the illegal weapon production and deployment process depicted in Fig. 1.

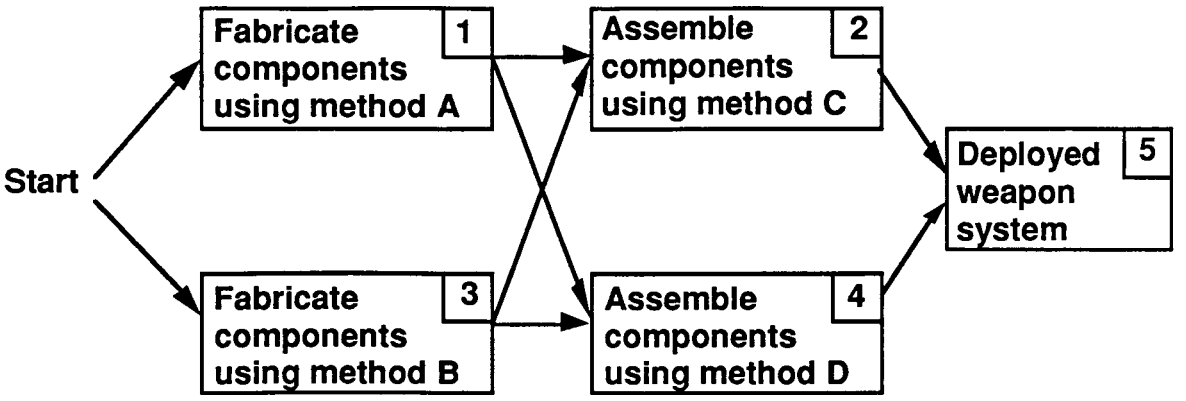


Figure 1. Network representation of evasion strategies.

As indicated in the figure, component fabrication, component assembly, and weapon deployment are required to achieve the objective. The component fabrication task may be accomplished by either evasion method A at step 1 or evasion method B at step 3, while the component assembly task may be accomplished by either evasion method C at step 2 or evasion method D at step 4. The assembled weapon is then covertly deployed at step 5. An evasion strategy consists of a sequence of steps leading to a deployed weapon. Thus, the four evasion strategies in this example are:

Strategy 1: Step 1 → step 2 → step 5 (fabricate components using method A, assemble components using method C, then deploy completed weapon).

Strategy 2: Step 1 → step 4 → step 5 (fabricate components using method A, assemble components using method D, then deploy completed weapon).

Strategy 3: Step 3 → step 2 → step 5 (fabricate components using method B, assemble components using method C, then deploy completed weapon).

Strategy 4: Step 3 → step 4 → step 5 (fabricate components using method B, assemble components using method D, then deploy completed weapon).

Note that a strategy corresponds to a path through the network in Fig. 1 from the point labeled "start" to step 5. The model is therefore able to represent all possible evasion strategies as a collection of paths through the network. The methodology will even display some paths that may be obviously inferior or impractical. The remaining phases of the methodology will reflect their inferior or impractical nature in the probabilities of successful evasion and their inferior nature will be reflected in the results. They are included in the network model because it is advisable to include all possible, and even inferior, strategies rather than risk eliminating important strategies.

2.3 Phase 3: Estimate Evasion Probabilities

In phase 3, for each step in the network we estimate the probability that treaty evasions associated with that step will be undetected by verification measures in force at that step. These probabilities are by nature subjective judgments and may vary depending on one's perspective. They should, of course, be assessed by experts familiar with verification technologies and weapon production processes and, to the extent possible, derived from theory or experiment.

Although there are refined techniques for assessing these probabilities through structured interviews, satisfactory results are likely to be obtained if the probabilities are based on agreement between multiple experts. Where experts disagree on these probabilities of successful evasion, the different opinions should be considered and separate evaluations performed. If the results of the evaluations are significantly different, then further investigation into the differences of opinion is warranted.

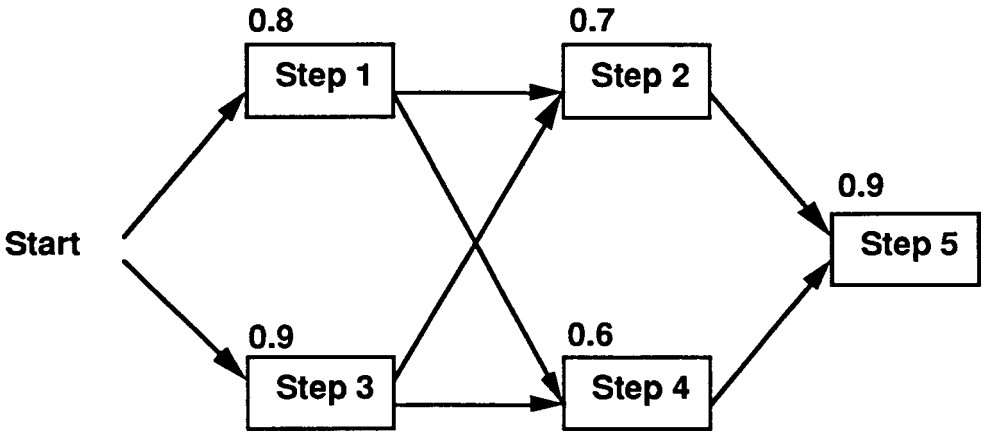


Figure 2. Example of network showing probabilities of undetected evasion for each step.

The probabilities of undetected evasion at a given step should be assessed separately for each verification measure in effect at that step. These probabilities are then combined into a single probability of undetected evasion for the step. If the evasions of the different verification measures are probabilistically independent, then the individual probabilities can simply be multiplied. However, if they are not probabilistically independent, then care should be taken to reflect the dependencies in the combination.

In our example, the evasion probability assigned to step 1 would reflect the likelihood that the Soviets can fabricate illegal components without detection using method A. Note that if no verification measures are in force at a particular step, the corresponding evasion probability is 1.0. In Fig. 2, we have assigned probabilities of undetected evasion to each of the steps of the network in Fig. 1. For example, the probability that the Soviets would be able to successfully evade the verification measures in place at step 1 has been assigned a value of 0.8.

2.4 Phase 4: Determine Evasion Strategies Least Likely to Be Detected

In phase 4, we use the probabilities of undetected evasion for each step estimated in phase 3 to compute undetected evasion probabilities for all possible evasion strategies. The probability that an evasion strategy will be detected is simply 1.0 minus the probability of undetected evasion. The undetected evasion probability for a particular strategy equals the product of the undetected evasion probabilities for each of the steps in the strategy. We use an algorithm which exploits the network structure shown in Figs. 1 and 2 in order to implicitly evaluate all possible evasion strategies in an efficient manner. For each Soviet evasion objective, the algorithm identifies the evasion strategy that meets that objective with the maximum probability of undetected evasion.

The simplest algorithm for identifying strategies having the highest probability of successful evasion is path enumeration. This technique explicitly evaluates all possible evasion strategies, or paths through the network. We illustrate the technique with the example in Fig. 2, where we find the maximum probability path from "start," or step 0, to step 5.

The evasion probability associated with each step is shown above the corresponding box. This example network contains the four paths and associated evasion strategy probabilities. For example, the probability of undetected evasion if the path using steps 1, 2, and 5 is chosen is $0.8 \times 0.7 \times 0.9 = 0.504$, as shown in the following table.

Using the path enumeration technique, one can determine that the evasion strategy with the highest probability of undetected evasion and, therefore, the lowest probability of detection is $0 \rightarrow 3 \rightarrow 2 \rightarrow 5$, with an associated probability of undetected evasion equal to 0.567. This path is shown in Fig. 3.

Path	Undetected Evasion Probability
$0 \rightarrow 1 \rightarrow 2 \rightarrow 5$	0.504
$0 \rightarrow 1 \rightarrow 4 \rightarrow 5$	0.432
$0 \rightarrow 3 \rightarrow 2 \rightarrow 5$	0.567
$0 \rightarrow 3 \rightarrow 4 \rightarrow 5$	0.486

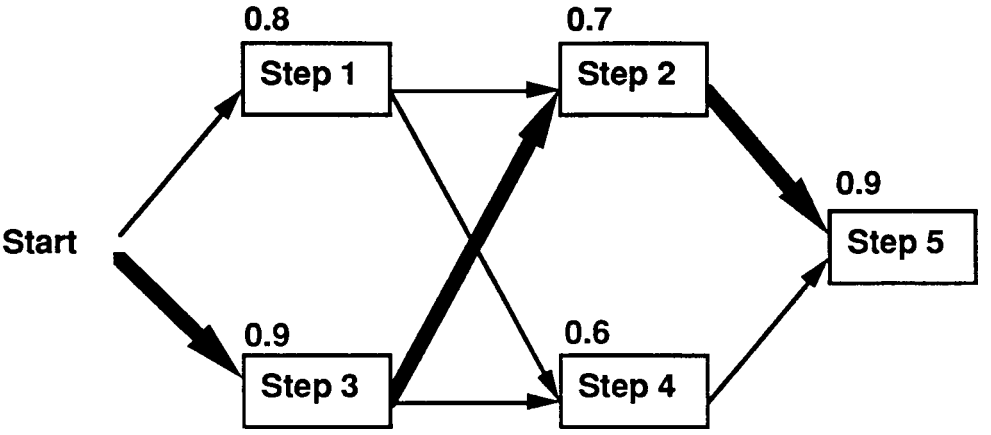


Figure 3. Example of network showing path with highest probability of undetected evasion.

The advantage of the path enumeration approach is that it explicitly represents all possible evasion strategies. Such an approach may be warranted if the model contains relatively few manufacturing steps. The disadvantage of this approach is that the number of paths through the network grows rapidly with network size. We use a more efficient method of determining the specific strategies least likely to be detected, a variant of Dijkstra's Algorithm, which is presented in Appendix A. Rather than determine the evasion probability for all paths through the network, it selectively evaluates those paths with the highest probabilities of undetected evasion.

2.5 Phase 5: Analyze Results and Perform Sensitivity Analysis

Finally, in phase 5 we analyze and interpret the results to identify the evasion strategies least likely to be detected and to identify the single verification measures and verification regimes that are most effective. As part of this effort, we perform a sensitivity analysis by repeating phases 3 and 4 for different verification regimes. Additionally, we may need to review phase 2 to ensure that all possible Soviet evasion strategies that may be employed to defeat the verification technologies are represented in the network model.

The results of the algorithm are represented as a figure of merit, which is used to compare the deterrent effect of different verification measures. It is computed for each evasion objective by multiplying the objective's undetected evasion probabilities obtained in phase 4 by the objective's relative weights determined in phase 1. We compare the figure of merit when a particular verification technology is in force with the figure of merit obtained when that technology is not in force. This provides a quantitative measure of the value of that particular verification technique, taking into consideration changes in Soviet evasion strategies in response to the introduced verification technology. In this manner, we identify the verification techniques that are most effective in detecting Soviet treaty violations.

At this phase of the methodology, we also test the sensitivity of the results to any inputs whose values may be controversial or subject to disagreement. In many cases the results will not change significantly when the inputs are changed. In such cases no further analysis is required. In cases where the results are highly sensitive to the input values, we need to further analyze the input values to resolve the important uncertainties. If this is not practical, then the results should be presented so as to reflect important differences of opinion.

The following section demonstrates each of the phases of the network methodology, using an example of verification of numerical limits on small single-stage ballistic missiles.

3. Hypothetical Example

In this section we demonstrate the network methodology for verification of small single-stage ballistic missile limits under a hypothetical treaty. This example is representative of the verification of limits on Soviet SS-23s that would have been required had the INF Treaty not completely eliminated that class of weapon. We begin by assuming that a treaty evasion of 20% in excess of treaty limitations is the smallest that would be militarily significant.

For our hypothetical example we have assumed that Soviet small single-stage ballistic missiles use a solid propellant. There are four major elements in the production of small single-stage ballistic missiles that use solid propellant: motor case production, propellant production, rocket motor assembly, and final missile assembly. All of these processes can take place at a single facility or at geographically separate facilities. We have assumed that the Soviet small ballistic missiles use the cartridge loading method of rocket motor assembly, allowing the propellant production and rocket motor assembly to occur separately.

We make two basic assumptions regarding quality control of missile manufacturing processes, assumptions that affect the topology of our network. First, we assume that fuel-cartridge and motor-case production lines must be qualified with static tests of produced rocket motors. Second, we assume that flight tests are important only to qualify the motor-case production line.

Inventories of small ballistic missiles would be difficult to determine due to refire capability of the launchers and relatively small size of the missiles. Consequently, we assume that national technical means (NTM) reconnaissance technologies such as satellites and high altitude aircraft are augmented with other, more intrusive techniques. Our hypothetical treaty includes provisions to monitor small missile inventory through accounting procedures implemented at assembly facilities. These additional provisions are:

- Only the rocket motor of a missile is tagged at its assembly site.
- Egress perimeter/portal monitoring (PPM) is implemented only at the rocket motor assembly site, with inspection rights based upon size and weight of exiting containers or vehicles.
- Anytime/anywhere suspect site inspections (SSIs) are allowed, to verify absence of treaty-limited items (e.g., excess rocket motors or complete missiles) at undeclared facilities, i.e., those not subject to other verification provisions.
- On-site inspections (OSIs) are allowed, to verify rocket motor tags at declared deployment and storage sites.

3.1 Example Phase 1: Soviet Evasion Objectives

There are several possible configurations of small ballistic missiles that could give the Soviets the militarily significant advantage of 20% over treaty limits. Each of these is a possible evasion objective. For example, the Soviets may or may not require flight testing of illegal missiles that are produced with covert production facilities. In addition, they may deploy illegal missiles at covert or declared sites. To represent these possible configurations, we include the following four evasion objectives in our model:

a) **Illegal, flight-tested missiles at declared sites:** The Soviets could deploy the illegal missiles at declared deployment sites, where they might be used for reload. The missiles have been flight-tested so that the Soviets will have a high degree of confidence in their strike capability.
b) **Illegal, flight-tested missiles at covert sites:** The Soviets could deploy the illegal missiles at covert sites. Missiles based at such sights would necessarily evade any verification measures provided in the treaty for declared missile sites. These missiles have also been flight-tested.
c) **Illegal, non-flight-tested missiles at declared sites:** The Soviets eliminate the possibility of detecting illegal missiles at test ranges if the missiles do not require flight testing. A corresponding higher probability of successful evasion may compensate for reduced missile reliability.
d) **Illegal, non-flight-tested missiles at covert sites:** This objective may be attractive if test ranges and legal deployment areas are monitored.

There are additional possible Soviet evasion objectives, including the stockpiling of rocket motors for later breakout. However, in order to keep the example to an easily explainable size, we will limit ourselves to the above four objectives.

Because the model involves multiple evasion objectives, we must establish a weighting scheme which reflects the relative values of the objectives. In establishing these weights, we note that flight-tested missiles should have a higher value than missiles that have not been flight-tested. In order to reflect the conservative nature of Soviet military planners, we assign a hypothetical weight of 2.0 to missiles that have been flight-tested and a weight of 1.0 to missiles that have been assembled using a covert motor-case assembly line and have not been flight-tested.

3.2 Example Phase 2: Evasion Strategies

Given the hypothetical constraints on small ballistic missile production noted above and the base case verification regime, we may develop our network model of Soviet evasion strategies. Figure 4 includes manufacturing steps required to produce more small ballistic missiles than the hypothetical treaty would allow (i.e., evade the treaty limitations). Boxes in the figure correspond to steps in the production process. As in our example in Fig. 3, evasion strategies correspond to paths through the network from the point labeled "start" to one of the boxes representing an objective, where objectives **a** through **d** identified in phase 1 correspond to boxes 25 through 28, respectively, in Fig. 4. For a detailed description of each step, see Appendix B.

We proceed with a detailed description of a typical evasion strategy or path to one of these objectives. One strategy for achieving objective b, shown in box 26, corresponds to the steps 1, 3, 7, 13, 18, 22, and 26. This strategy corresponds to the following manufacturing steps:

Step 1: Produce 20% more motor cases at a declared manufacturing site than the number of small ballistic missiles allowed under the treaty.
Step 3: Produce 20% more fuel cartridges at a declared fuel-cartridge production site than the number required for missiles specified under the treaty.
Step 7: Assemble the additional illegal rocket motors at a covert assembly site.
Step 13: Static-test rocket motor of legal missile (static testing of legal missiles serves to qualify the declared motor-case and fuel-cartridge assembly lines; static testing of illegal missiles is not required to qualify covert rocket motor assembly line; because a legal missile is used, the evasion probability is 1.0).
Step 18: Assemble illegal missiles at a covert missile final-assembly site.
Step 22: Flight-test legal missile (this serves to qualify declared motor-case production line; flight test of illegal missile is not required to qualify covert assembly lines used).
Step 26: Send illegal missiles to covert storage or deployment sites.

Alternative evasion strategies for achieving the objective shown in box 26 are available. A second strategy corresponds to the steps 1, 4, 10, 15, 18, 22, and 26. Under this strategy, a covert fuel-cartridge production line corresponding to step 4 is used, rather than the declared line shown as step 3. This choice forces the Soviets to perform a rocket motor static test on an illegal missile. Thus, our network model accounts for the logical constraint that a static test of an illegal missile is required if a covert fuel-production line is used.

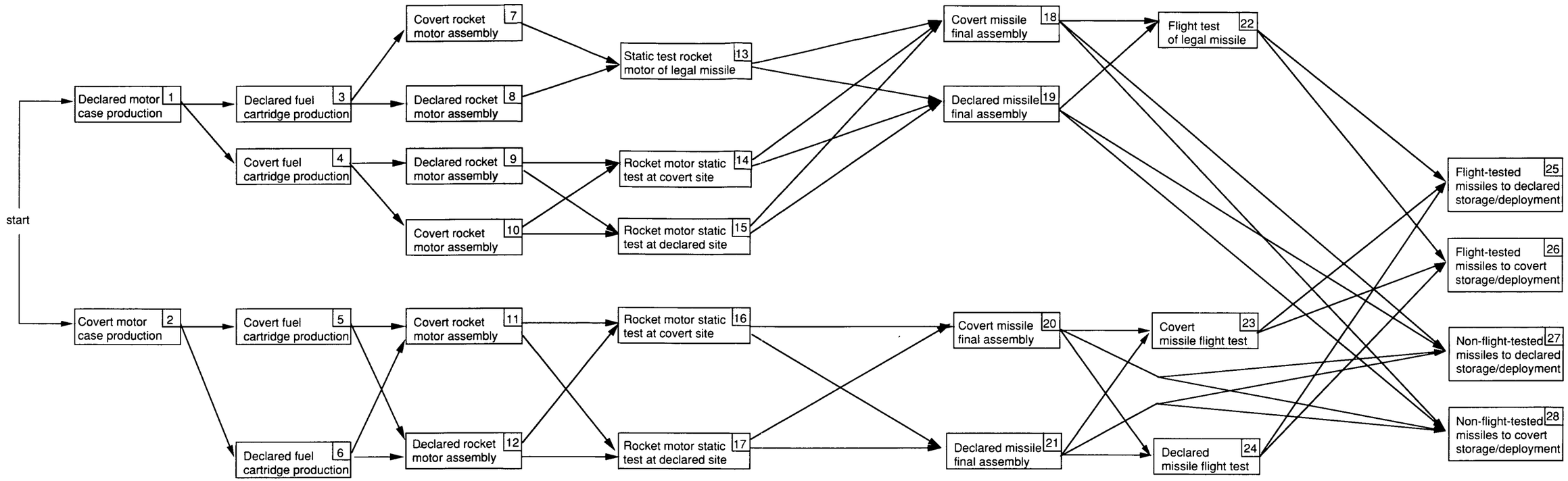


Figure 4: Small Single-Stage Ballistic Missile Manufacturing Network — Base Case Topology

In the example above, it is necessary to distinguish between rocket motors assembled using fuel produced at a declared facility and those assembled using fuel produced at a covert facility. In order to make this distinction, we represent the covert rocket motor assembly task as two different production steps in the network. This allows us to distinguish between the two types of rocket motors, and to determine whether static tests must be conducted on legal missiles (at step 13) or illegal missiles (at step 14 or 15). We emphasize that steps 7 and 10 do not refer to different sites, but rather to different processes used to produce rocket motor components that are assembled at a single site. Other tasks appear at more than one point in the network for similar reasons.

3.3 Example Phase 3: Evasion Probabilities for Each Step

Undetected evasion probability estimates are shown in Fig. 5, where the number above the upper left corner of the box is the corresponding undetected evasion probability. These probabilities are purely hypothetical and are notional only. For example, the probability that the Soviets can avoid detection of a covert rocket motor assembly line (at step 7) is equal to 0.8. An evasion probability of 1.0 implies that no verification measures are applicable at the corresponding step under the base case assumptions. Hence, the evasion probability associated with step 22 is 1.0 because a legal missile is being flight-tested at this step. These estimates are derived in Appendix B and are purely illustrative.

In steps where more than one verification measure is in force, the evasion probabilities for each measure should be assessed separately and then combined to obtain the evasion probability for the step. During this procedure, care should be taken to reflect any probabilistic dependencies among the verification measures. For example, consider the following derivation of the evasion probability associated with step 7, covert rocket motor assembly. As noted in Appendix B, in order to detect activity at step 7, the monitoring country would first have to detect the covert site using NTM (with detection probability $1 - 0.6$) and then detect the illegal missiles on site using an SSI (with detection probability $1 - 0.5$). The monitoring country would then detect the violation only through both NTM detection and subsequent SSI detection. Hence, the detection probability associated with step 7 is $(1 - 0.6)(1 - 0.5)$, and the corresponding evasion probability is $1 - (1 - 0.6)(1 - 0.5) = 0.8$. This evasion probability is shown above step 7 in Fig. 5.

3.4 Example Phase 4: Evasion Strategies Least Likely to be Detected

For each objective in our example, we must determine the evasion strategy least likely to be detected in reaching that objective. This problem is complicated by the fact that several different sequences of production steps may be employed to reach a given point in the network. We must implicitly determine the evasion probability corresponding to each sequence in order to solve our problem.

For example, to complete step 14 in Fig. 5 the Soviets have two options. Under the first option, they could produce motor cases at a declared facility (step 1), produce fuel cartridges at a covert facility (step 4), assemble the rocket motor at a declared site (step 9), and then test the rocket motor at step 14. Under the second option, they would assemble the rocket motor at a covert site (step 10) rather than at a declared site (step 9) in order to reach step 14. Given these two production policies, in order to complete step 14 the Soviets would choose the policy that corresponds to the highest probability of undetected evasion. The probability of undetected evasion under the first policy is $(1.0)(1.0)(0.42)(0.7) = 0.294$, while the probability of undetected evasion under the second policy is $(1.0)(1.0)(0.8)(0.7) = 0.560$. Hence, the Soviets would choose the second policy. The circled number above box 14 in Fig. 6 reflects this choice. (Figure 6 is just Fig. 5 with heavy lines marking the paths of highest probability of undetected evasion.)

When alternative policies are available to reach other points in Fig. 6, our algorithm assumes similar Soviet behavior in order to derive the circled probabilities. In this manner, we determine the strategy and evasion probability associated with each box in Fig. 6, including the objective boxes 25 through 28.

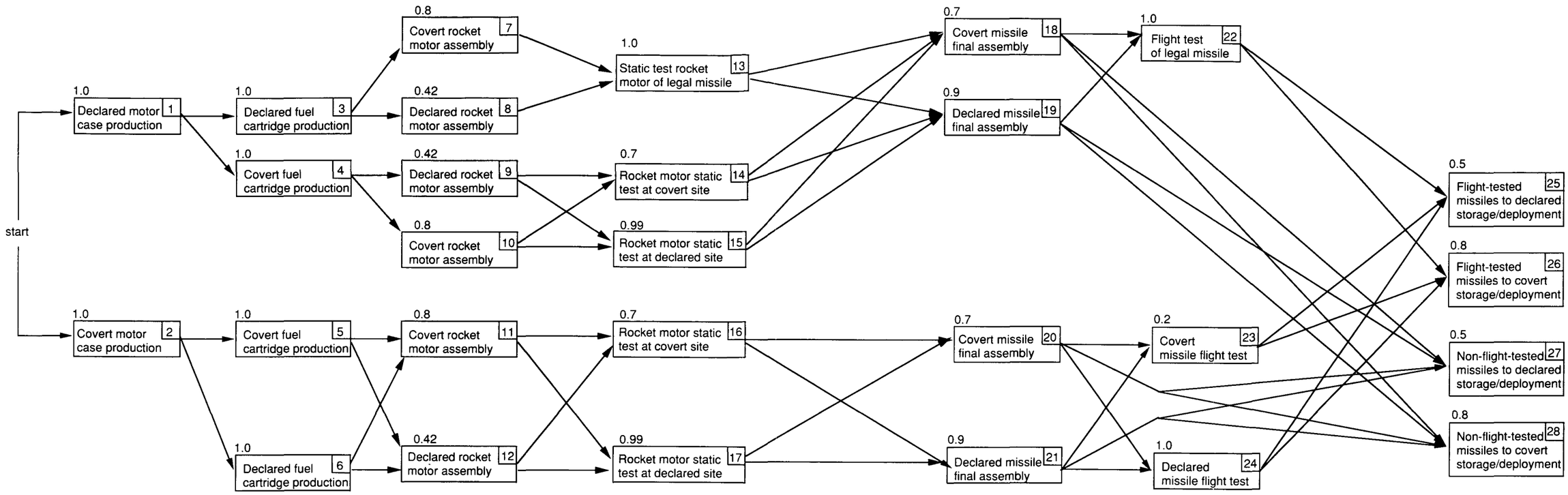


Figure 5: Small Single-Stage Ballistic Missile Manufacturing Network—Base Case Evasion Probabilities

Notes:

a) Evasion probability for activity shown above corresponding box

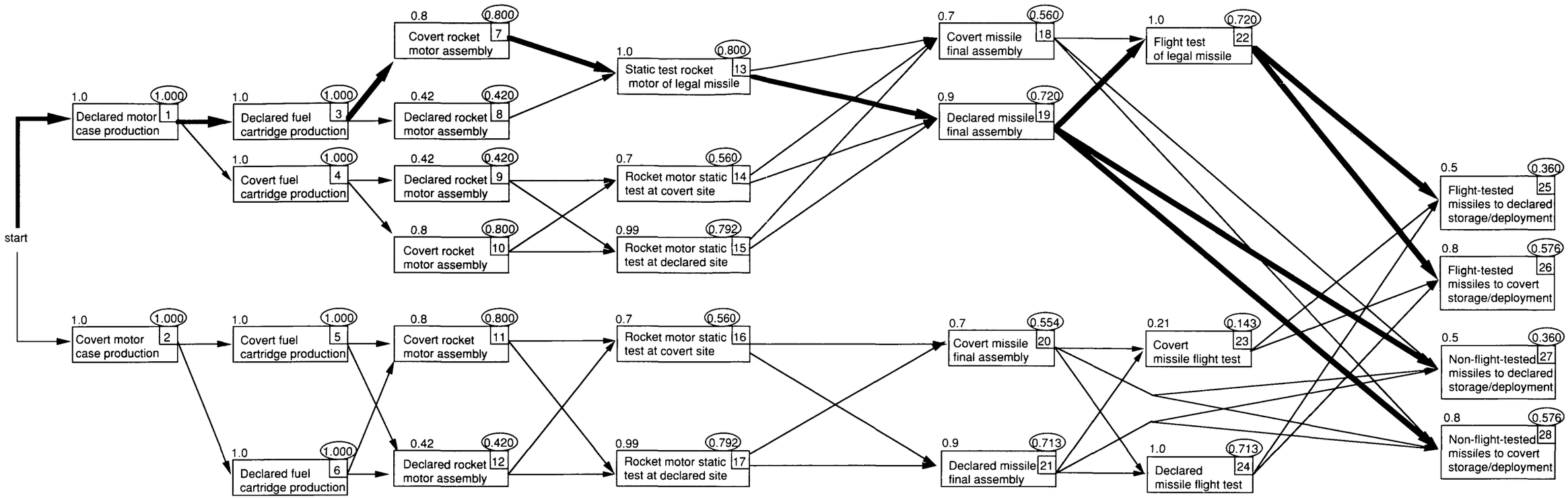


Figure 6: Small Single-Stage Ballistic Missile Manufacturing Network—Base Case Solution

Notes:

a) Evasion probability for activity shown above corresponding box

b) Maximum evasion probability from start shown in: ⬭

c) Soviet evasion strategies shown by bold arrows

3.5 Example Phase 5: Results

We begin this phase by identifying the evasion strategy least likely to be detected for each of the four objectives determined in phase 1 of our example. For each of these objectives, the illegal manufacturing policy with the highest undetected evasion probability has been determined and is shown in Fig. 6 as a sequence of bold arrows. As indicated by the bold arrows, the strategy with the highest probability of undetected evasion is as follows:

(1) Declared motor-case production.
(3) Declared fuel-cartridge production.
(7) Covert rocket motor assembly.
(13) Static test of rocket motor of legal missile.
(19) Declared missile final assembly.
(22) Flight test of legal missile.
(25), (26), (27), or (28) Missiles to declared or covert sites.

The final result of this policy is an inventory of missiles 20% in excess of treaty limitations. The probabilities of undetected declared and covert deployment of missiles are 0.360 and 0.576, respectively. The probabilities associated with flight-tested missiles are the same as those for non-flight-tested missiles because the evasion probability associated with flight testing in this portion of the network (step 22) is equal to 1.0 (there is no on-site monitoring at the test site). For this base case, the figure of merit is computed by taking into account the assigned weights of flight-tested missiles (2.0) and non-flight-tested missiles (1.0), as follows: $(0.360 + 0.576)2.0 + (0.360 + 0.576)1.0 = 2.81$.

The procedure outlined above has been carried out for the following cases, where each case description refers to surveillance measures added to those included in the base case assumptions.

- **Case 1:** In this scenario, the motor cases are tagged and egress PPM is implemented at the declared motor-case production site, reducing the probability of evasion at this step. Because motor cases are now a monitored component, covert motor-case production is prohibited by treaty and can be deterred. To reflect these changes from the base case, in phase 3 of the network methodology we reduce the evasion probability at the declared motor-case production step (step 1) from 1.0 to 0.6 and at the covert motor-case production step (step 2) from 1.0 to 0.8. The output of phase 4 for this case is displayed in Fig. 7. A comparison of the bold arrows in Fig. 6, the base case, with the bold arrows in Fig. 7 reveals that the optimal Soviet evasion strategies change when egress PPM at the declared motor-case production site is added to the base case surveillance methods. Specifically, production is switched from the declared motor-case line at step 1 to the covert line at step 2. The overall effect of this surveillance technique is to reduce the evasion probabilities associated with each of the four objectives. As indicated in Table 1, the corresponding figure of merit is reduced by 20% relative to the base case.
- **Case 2:** In addition to the changes noted in case 1, we include ingress PPM at the rocket motor assembly site. Consequently, we reduce the evasion probability at the declared motor-case production

Table 1: Undetected Evasion Probabilities and Figures of Merit

	Flight-tested missiles		Non-flight-tested missiles		Figure
Case	Declared	Covert	Declared	Covert	of merit
Base	0.360	0.576	0.360	0.576	2.81
1	0.286	0.457	0.286	0.457	2.23
2	0.286	0.457	0.286	0.457	2.23
3	0.280	0.448	0.280	0.448	2.18
4	0.222	0.355	0.222	0.355	1.73
5	0.288	0.461	0.288	0.461	2.25
6	0.178	0.284	0.178	0.284	1.39

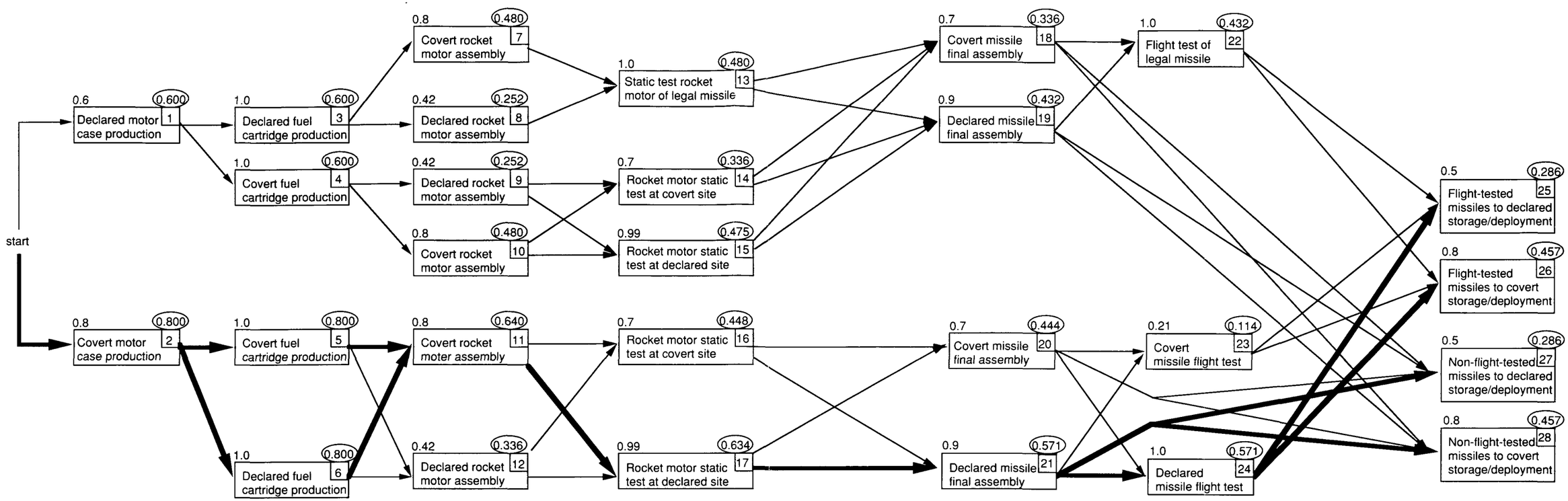


Figure 7: Small Single-Stage Ballistic Missile Manufacturing Network—Case 1

Notes:

a) Evasion probability for activity shown above corresponding box

b) Maximum evasion probability from start shown in: ⬭

c) Soviet evasion strategies shown by bold arrows

d) Egress PPM added at declared motor case production site

site (step 1) from 1.0 to 0.6, at the covert motor-case production site (step 2) from 1.0 to 0.8, and at the declared rocket motor assembly site (steps 8, 9, and 12) from 0.42 to 0.378. Although this case adds ingress PPM at the rocket motor assembly site to the surveillance measures included in case 1, the evasion strategies least likely to be deterred and their probabilities do not change. This is because the optimal Soviet manufacturing policy in case 1 involves bypassing the declared rocket motor assembly step and using covert rocket motor assembly facilities. Hence, increasing surveillance of the declared facility has no effect on the case 1 evasion probabilities. These results are shown in Fig. 8. This case provides an illustration of the need for an integrated evaluation methodology. Although ingress PPM by itself appears to increase verifiability, in this hypothetical example we see that it adds little or no additional detection capability.

- **Case 3:** We add egress PPM at the missile final-assembly site to the base case and reduce the evasion probability at the declared missile final-assembly site (steps 19 and 21) from 0.9 to 0.6. The addition of this verification measure decreases evasion probabilities for both flight-tested and non-flight-tested missiles. The Soviet evasion policy also changes from using declared missile final-assembly facilities to covert missile final-assembly facilities. The corresponding figure of merit is reduced by 22%. This case is illustrated in Fig. 9.
- **Case 4:** In this scenario, we add tagging and egress PPM at the motor-case assembly site and missile final-assembly site. We reduce the evasion probability at the declared motor-case assembly site (step 1) from 1.0 to 0.6, at the covert motor-case assembly site (step 2) from 1.0 to 0.8, and at the declared missile final-assembly site (steps 19 and 21) from 0.9 to 0.6. Soviet evasion strategies change relative to the base case. The strategy for producing missiles changes to one involving covert motor-case production and covert missile final assembly. All evasion probabilities are reduced and the figure of merit is reduced by 38%. This case is illustrated in Fig. 10.
- **Case 5:** In this scenario, we monitor the amount of propellant produced and tag the fuel cartridges. We reduce the evasion probability at the declared fuel-cartridge production site (steps 3 and 6) from 1.0 to 0.8 and at the covert fuel-cartridge production site (steps 4 and 5) from 1.0 to 0.6. Relative to the base case, this measure does not change Soviet policy for production of illegal missiles. However, evasion probabilities are reduced, and the figure of merit is reduced by 20% relative to the base case. This case is illustrated in Fig. 11.
- **Case 6:** We implement all of the verification measures included in the above cases. Soviet evasion strategies change for both flight-tested and non-flight-tested missiles. The corresponding figure of merit is reduced by 50%. This case is shown in Fig. 12.

The preceding example is for illustrative purposes only. We emphasize once again that these results are based upon hypothetical treaty provisions, Soviet missile production processes, and estimates of undetected evasion probabilities.

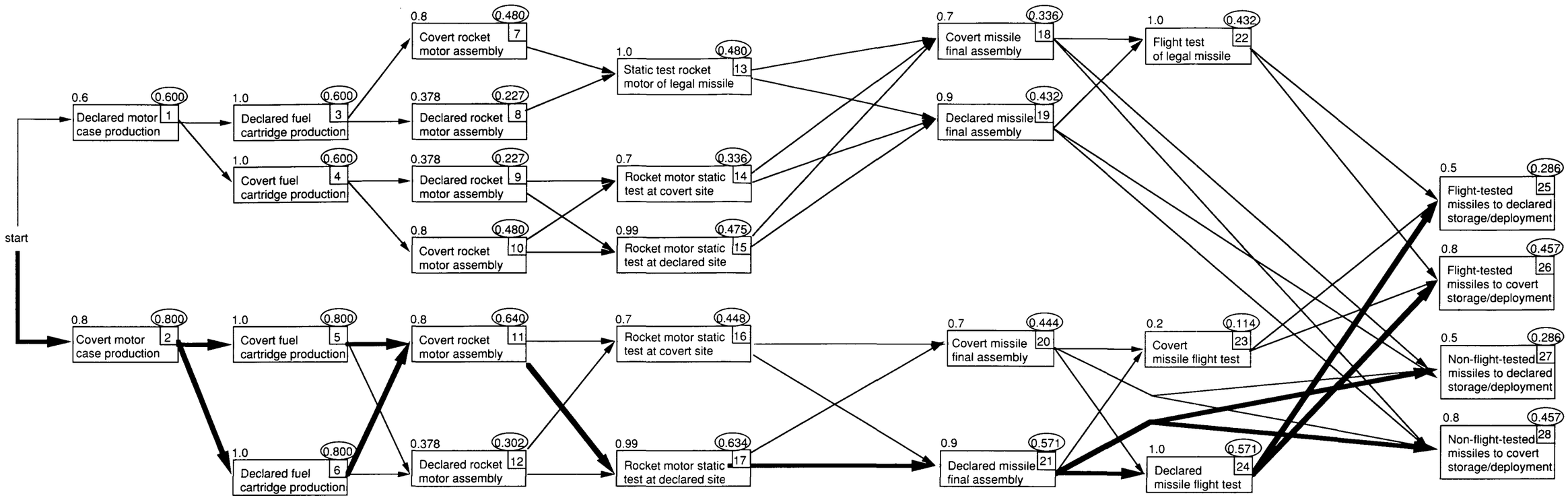


Figure 8: Small Single-Stage Ballistic Missile Manufacturing Network—Case 2

Notes:

a) Evasion probability for activity shown above corresponding box

b) *Maximum evasion probability from start shown in:* ⬭

c) Soviet evasion strategies shown by bold arrows

d) Egress PPM added at declared motor case production site

e) Ingress PPM added at declared rocket motor assembly

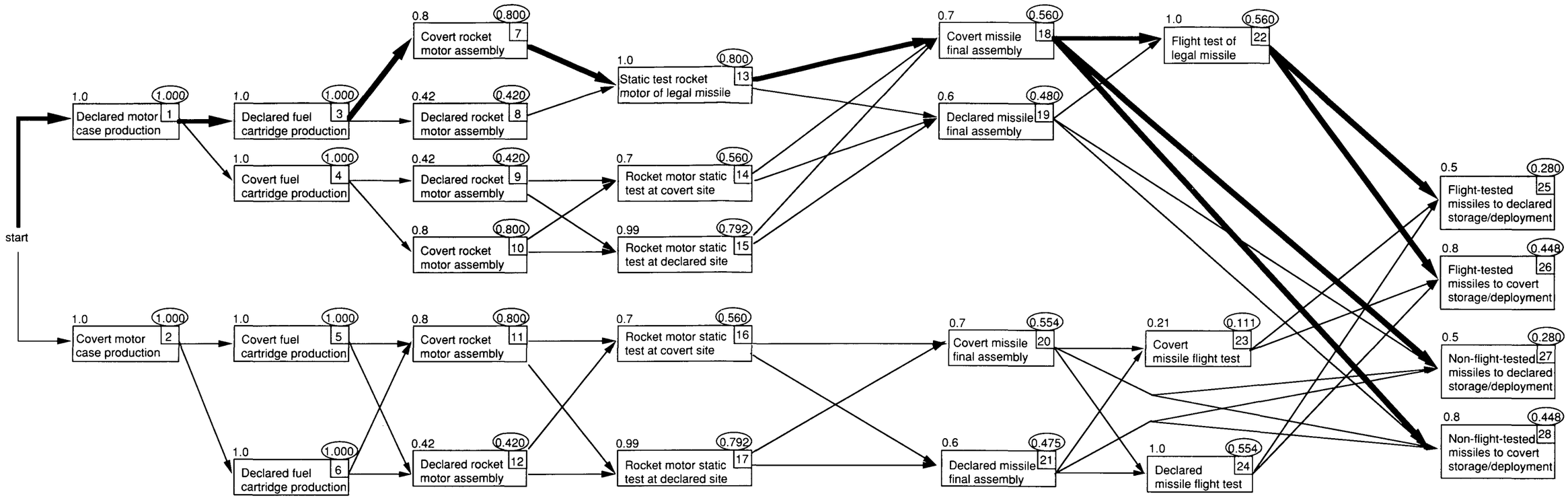


Figure 9: Small Single-Stage Ballistic Missile Manufacturing Network—Case 3

Notes:

a) Evasion probability for activity shown above corresponding box

b) Maximum evasion probability from start shown in: ⬭

c) Soviet evasion strategies shown by bold arrows

d) Egress PPM added at final missile assembly sites

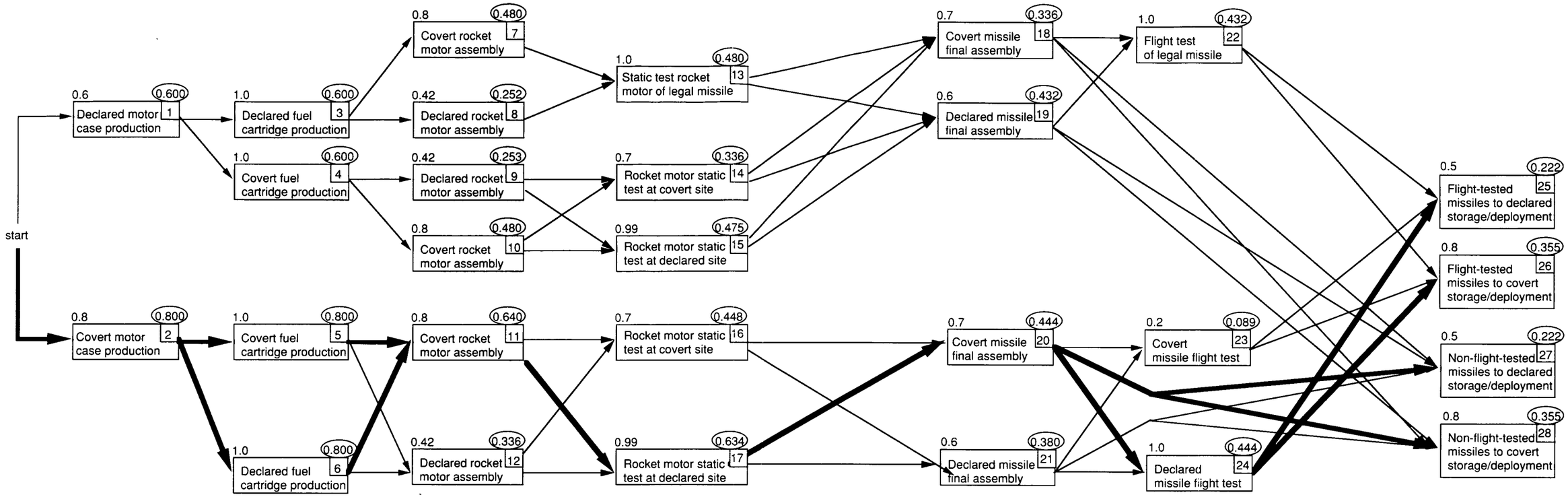


Figure 10: Small Single-Stage Ballistic Missile Manufacturing Network—Case 4

Notes:

a) Evasion probability for activity shown above corresponding box

b) Maximum evasion probability from start shown in: ⬭

c) Soviet evasion strategies shown by bold arrows

d) Egress PPM added at motor case production site

e) Egress PPM added at missile final assembly site

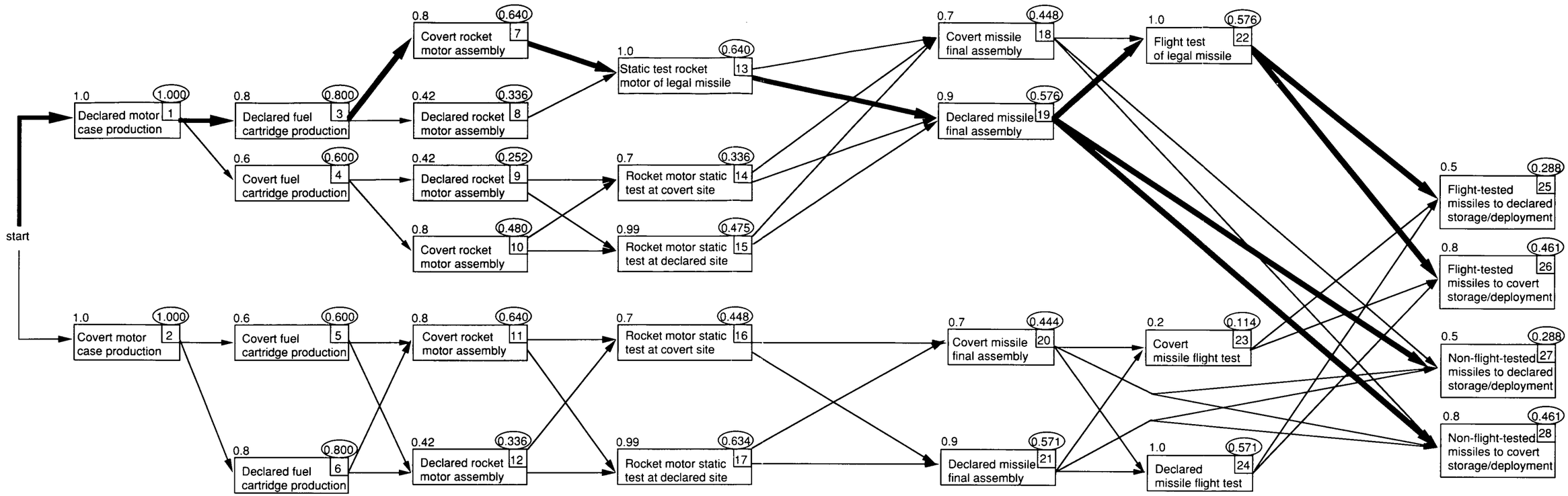


Figure 11: Small Single-Stage Ballistic Missile Manufacturing Network—Case 5

Notes:

a) Evasion probability for activity shown above corresponding box

b) Maximum evasion probability from start shown in: ⬭

c) Soviet evasion strategies shown by bold arrows

d) Add fuel cartridge tagging at declared fuel cartridge production sites

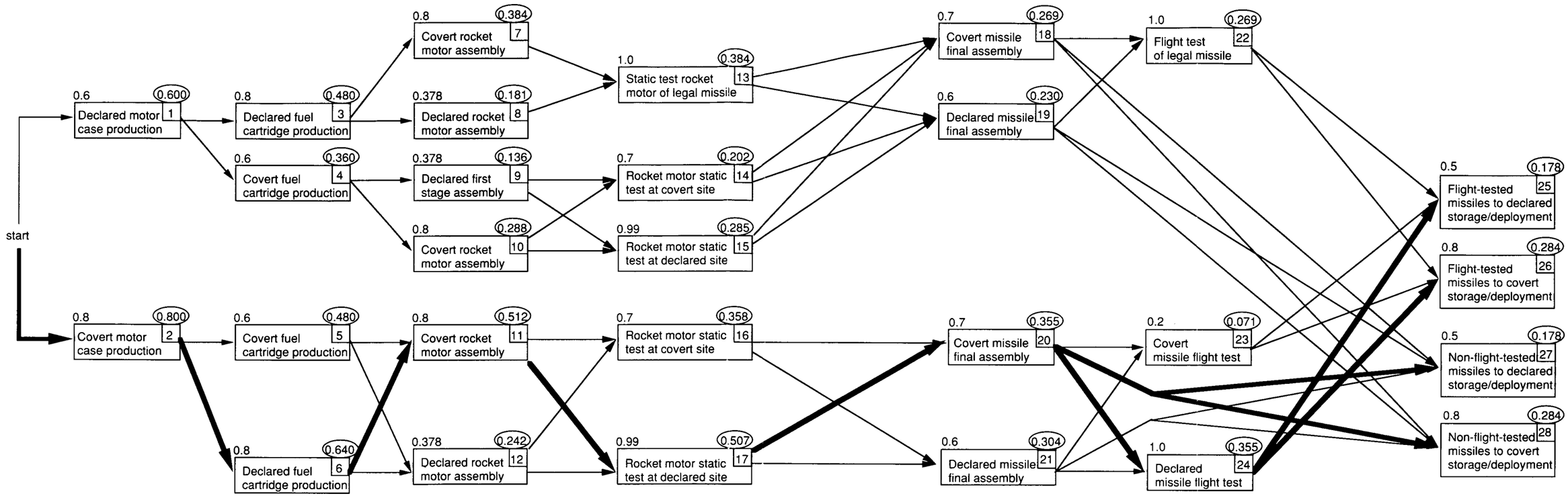


Figure 12: Small Single-Stage Ballistic Missile Manufacturing Network—Case 6

Notes:

a) Evasion probability for activity shown above corresponding box

b) Maximum evasion probability from start shown in: ⬭

c) Soviet evasion strategies shown by bold arrows

d) Egress PPM added at declared motor case production site

e) Ingress PPM added at declared rocket motor assembly sites

f) Egress PPM added at declared missile final assembly sites

g) Fuel cartridge tagging added at declared fuel production sites

4. Summary

The network methodology provides a quantitative tool for assessing the relative values of different treaty verification procedures and technologies. Given estimates of probabilities of undetected evasion associated with detailed verification measures, the model identifies most likely Soviet evasion strategies and the probability of detection associated with each. To complete the analysis, one must consider the financial cost and intrusiveness associated with each of the above verification measures. Such factors as budget, disclosure of sensitive information, and impact on defense operations must be considered in conjunction with the computed effectiveness measures. We emphasize that the model does not supplant human judgment, but rather complements it and structures the decision-making process. The method has been demonstrated for a hypothetical problem but can be easily applied to actual verification decisions.

Acknowledgments

The contributions of Dr. John Harvey, former Deputy Treaty Verification Program Leader for START/INF, and Mark Warmerdam are greatly appreciated. Their review and comments on early drafts of this report helped ensure the applicability of this methodology to actual verification decisions.

Appendix A: Dijkstra's Algorithm

A variant of Dijkstra's shortest path tree algorithm—see Lawler (1976) or Jensen and Barnes (1980)—offers a computationally more efficient technique than the path enumeration approach presented in Sec. 2.4. This algorithm determines the optimal evasion strategy by iterative construction of a tree, adding steps to the tree one at a time. The step selected for addition is the one with maximum cumulative probability. We illustrate this algorithm in Table A-1, using the example data in Fig. 3.

Table A-1. Illustration of Dijkstra's Algorithm, Using Data in Fig. 3.

Iteration	Candidate steps	Add step	Path element	Cumulative probability at step	Steps in tree
1	1,3	3	(s-3)	0.9	3
2	1,2,4	1	(s,1)	0.8	3,1
3	2,4	2	(3,2)	0.63	3,1,2
4	4,5	5	(2,5)	0.567	3,1,2,5

Hence, the manufacturing policy associated with highest undetected evasion probability consists of steps 0, 3, 2, and 5. The corresponding evasion probability is 0.567.

In order to implement this network methodology, problems could be formulated and the corresponding network drawn using a microcomputer graphics package. A data file reflecting this network could then be developed and accessed by a program which finds the maximum probability paths to selected nodes in the network. If a logarithmic transformation is applied to the evasion probabilities, an existing implementation of Dijkstra's shortest path algorithm could be used to find the desired maximum probability paths.

References

Jensen, Paul A., and J. Wesley Barnes, *Network Flow Programming* (Wiley, New York, 1980).

Lawler, Eugene L., *Combinatorial Optimization: Networks and Matroids* (Holt, Rinehart and Winston, New York, 1976).

Appendix B: Details of Base Case Example (See Fig. 5)

Step	Description	Verification Measures	Successful Evasion Probability
1	Produce extra motor cases at declared site	None	1.0
2	Construct and operate covert motor-case production facilities	None	1.0
3	Produce extra fuel cartridges at declared site	None	1.0
4	Construct and operate covert fuel-cartridge production facilities	None	1.0
5	Same as 4	None	1.0
6	Same as 3	None	1.0
7	Construct and operate covert rocket motor assembly facilities (in order to detect, must first detect covert site with NTM, then detect illegal rocket motors at site with SSI, therefore composite evasion probability is equal to $1 - (1 - 0.6)(1 - 0.5) = 0.8$)	NTM SSI Composite	0.6 0.5 0.8
8	Assemble extra rocket motors at declared site, then transport through egress PPM (can detect independently with NTM or PPM, therefore composite evasion probability = $0.7 \times 0.6 = 0.42$)	NTM PPM Composite	0.7 0.6 0.42
9	Same as 8	NTM PPM Composite	0.7 0.6 0.42
10	Same as 7	NTM SSI Composite	0.6 0.5 0.8
11	Same as 7	NTM SSI Composite	0.6 0.5 0.8
12	Same as 8	NTM PPM Composite	0.7 0.6 0.42
13	Static-test legal rocket motor at declared site—this qualifies declared motor-case line (step 1) and declared fuel-cartridge line (step 3)	None	1.0
14	Static-test illegal rocket motor at covert site—this qualifies covert fuel-cartridge line (step 4) (in order to detect, must first detect covert site with NTM, then detect illegal rocket motors at site with SSI, therefore composite evasion probability is equal to $1 - (1 - 0.5)(1 - 0.4) = 0.7$)	NTM SSI Composite	0.5 0.4 0.7
15	Static-test illegal rocket motor at declared site—this qualifies covert fuel-cartridge line (step 4)	NTM	0.99

16	Same as 14—this qualifies covert motor-case line (step 2) and covert fuel-cartridge line (step 5) if used	NTM SSI Composite	0.5 0.4 0.7
17	Same as 15—this qualifies covert motor-case line (step 2) and covert fuel-cartridge line (step 5) if used	NTM	0.99
18	Assemble missiles at covert site (must first detect covert site with NTM, then detect illegal rocket motors at site with SSI, therefore composite evasion probability is $1 - (1 - 0.5)(1 - 0.4) = 0.7$)	NTM SSI Composite	0.5 0.4 0.7
19	Assemble missiles at declared site	NTM	0.9
20	Same as 18	NTM SSI Composite	0.5 0.4 0.7
21	Same as 19	NTM	0.9
22	Flight-test legal missile—this qualifies declared motor-case production line (step 1)	None	1.0
23	Flight-test missile at covert site—this qualifies covert motor-case production line (step 2) (detect with either NTM or SSI, therefore evasion probability is $(0.3)(0.7) = 0.21$)	NTM SSI Composite	0.3 0.7 0.21
24	Flight-test illegal missile at declared site—this qualifies covert motor-case production line (step 2)	None	1.0
25	Store or deploy extra missiles at declared sites—rocket motor has been static-tested if covert fuel-cartridge or motor-case lines used, missile has been flight-tested	NTM OSI Composite	1.0 0.5 0.5
26	Store or deploy missiles at covert sites—rocket motor has been static-tested if covert fuel-cartridge or motor-case line used, missile has been flight-tested (must first detect covert site with NTM, then detect illegal missiles at site with SSI, hence composite probability is equal to $1 - (1 - 0.6)(1 - 0.5) = 0.8$)	NTM SSI Composite	0.6 0.5 0.8
27	Store or deploy missiles at declared sites—rocket motor has been static-tested, missile not flight-tested	NTM OSI Composite	1.0 0.5 0.5
28	Store or deploy missiles at covert sites—rocket motor has been static-tested, missile not flight-tested (must first detect covert site with NTM, then detect illegal missiles at site with SSI, hence composite evasion probability is equal to $1 - (1 - 0.6)(1 - 0.5) = 0.8$)	NTM SSI Composite	0.6 0.5 0.8