Chapter Twelve

THE "DAY AFTER" METHODOLOGY AND NATIONAL SECURITY ANALYSIS

David Mussington

The development of analytic tools to help those making national security policy is driven by the need for usable answers and the urgency of the threats facing the United States. The interaction of these two drivers has produced an array of approaches that favor insights derived from experience with international phenomena. *After all, conducting empirically valid tests of means-ends relationships in international politics is all but impossible, so implicit models must substitute for hard-to-get experimental data.* Most analysts resort to historical comparisons, reasoning via analogy, or conceptualizations that are mathematically rigorous but empirically dubious or even trivial. The "lessons of history" are said to counsel, variously, caution or haste, conservatism or aggression. Appeasement is seen as dangerous, deterrence as infallible but tenuous. Similarities between cases present and past are endlessly discussed with no firm conclusions possible or persuasive—at least as determined through analysis alone.

Decisionmakers are left with concepts and models that necessarily rest on assumptions about the international system, the decisionmaking and behavioral imperatives of nation-states, and the relationship of military, economic, and political power to the shaping of international outcomes. How can such broad perspectives be converted into something more immediately usable for analyzing complex international phenomena? Abstractions are inevitably gross generalizations of empirical conditions; when adapted to public policy, they are driven by the special needs of decisionmakers for a

simplifying schema to understand complex conditions, and by the high level of uncertainty that characterizes political change.

One source of control (in what would otherwise be an unconstrained process) is to exploit the subject matter expertise of issue area specialists as well as rules of thumb presented by diplomatic and military *practitioners* in national security. These rules can form frameworks for understanding complex phenomena. And if these frameworks are made explicit, public policy analysis can subject them to logical and—to some extent—empirical scrutiny sensitive to temporal, technological, and political-economic factors. A setting comporting to a complex real-world international security problem can thus be represented by an abstraction based on what experts hold to be an assessment of a region, technology, or set of relationships. Yet expert-derived frames of reference are not facts, as such, but facts as implied by the conclusions and insights held by fallible human beings. Creating an environment to help this process along is what exercise designers do. Scenario designs, table-top game structures, decisionmaking simulations, and forecasts of future political-military, economic, and technological change—all of these offer tools to meet such analytic requirements. The Day After exercise methodology is one way to elicit structured expertise that channels specialist knowledge into policy dilemmas faced by decisionmakers in the short, medium, and long term.

This chapter describes this approach and shows how it was applied to real-world problems in two projects. It also discusses the value of the Day After methodology, including the special scenario design requirements necessary for successful usage.

THE METHODOLOGY IN BRIEF

A Day After exercise entails a multistage presentation of a hypothetical future, as shown in Figure 12.1. A scenario is derived from contemporary events and policy dilemmas. For design purposes, the scenario time line is divided into a future history and three steps involving actual game play, as follows.

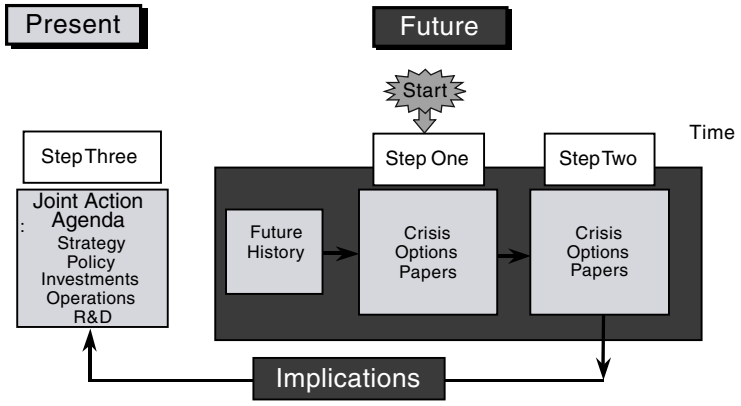

Figure 12.1—Generic Schematic of Day After Exercise Methodology

The Future History. This portion of the Day After exercise methodology is laid out on a time line that starts with the present and then offers a logical sequence of political-military, diplomatic, economic, technological, and policy-related events that identifies the key processes and actors. Background information built into the future history establishes the credibility of the event framework outlined in the next part of the exercise. The more detailed and nuanced the presentation of issues in the future history, the more the follow-on phases can unfold so as to illuminate the policy areas examined.

Step One. Step one involves a policy crisis generated by the actors, processes and entities introduced in a future history that highlights threats to entities or interests important to the United States and/or its allies. The actors are further developed by the decisions they make against a background of specific events. The scenario culminates in a definite escalation. At the end of step one, participants must collectively arrive at decisions appropriate for managing the crisis presented. They must identify the core objectives that policymakers should pursue, and they should decompose the issues entailed in adopting the favored approach to meet those objectives.

Step Two. The crisis escalates steeply in step two in a closely structured and focused evolution of the policy dilemmas and decision

imperatives. Although policy responses selected by participants in step one are not directly used in the unfolding events, participants are confronted with step one decisions partially consistent with their step one deliberations. The remaining agenda of responses outlined at the onset of step two intensifies the crisis situation, in order to sharpen the policy dilemmas presented, and challenges the consensus crisis management approach selected earlier by the group. Participants must decide what actions are needed to address the situation effectively, and they must examine the likely consequences of what they decide or fail to decide.

Step Three. In step three, the participants return to the present and are asked to evaluate the situation in light of the exercise experience. Dilemmas are presented from the perspective of contemporary policy choices on the grounds that a framework of prospective actions, policy decisions, and plans could prevent or mitigate the severe conditions described in the scenario narrative. Participants are asked to seek consensus on responses and to clarify areas of pronounced disagreement. Thus, the issue agenda *following* the exercise is addressed so as to advance the identification of potential solutions.

APPLICATIONS AND EXERCISE DEVELOPMENT

The lengthy developmental process responsible for a successful exercise belies the set-piece nature of the Day After approach. Well before the exercise is run, it is tested, different scenarios and issue agendas are explored, and potential participant responses are pondered. An exercise test series helps explore a large number of scenario/issue combinations. The design process subjects this exploration to a disciplined comparative analysis, confronting possible futures with consistent questions and concepts from the perspective of participants in decisionmaking.

Many subjects and issues have been explored using this exercise methodology. Two examples are (1) strategic information warfare (SIW) and mechanisms for addressing significant infrastructure vulnerabilities and (2) electronic commerce technologies (cyberpayments) and international money laundering.

Strategic Information Warfare

Because the sponsor of the SIW exercise was the U.S. Department of Defense (DoD),[1] the focus was on information warfare (IW) as a potential impediment to the exercise of U.S. military options. Those options were themselves predicated on established plans and programs for the timely and efficient delivery of military equipment and personnel to regions designated as strategic to the protection of U.S. friends, allies, and interests. IW threats are introduced directly into existing concepts of strategic security. Although IW is characterized by unique phenomena (i.e., particular weapons and strategic utilization concepts), it is examined in a framework prestructured by well-understood political-military models.

Undertaken in 1995, the SIW Day After exercise was one of the first systematic policy development efforts to explore the potential dilemmas and decisionmaking imperatives associated with society's increasing dependence on information infrastructures. The exercise was developed at a time when basic concepts of vulnerability, crisis stability, and crisis management in the information domain were each relatively unfamiliar. To address this shortfall in rigorous and "high confidence" information warfare conceptualizations, the exercise designers created a hypothetical future in which U.S. critical information infrastructures were targeted by a foreign adversary.

The objectives of the exercise were to

- Describe and frame the concept of strategic information warfare.
- Describe and discuss the key features and related issues that characterize SIW.
- Explore the consequences of these features and issues for U.S. national security as illuminated by the exercises.

---

[1]More precisely, the project sponsor was the Office of the Secretary of Defense (OSD), and the study was defined under the auspices of RAND's National Defense Research Institute.

- Suggest analytic and policy directions for addressing elements of these SIW features and issues.[2]

SIW was framed against challenges—notably asymmetric threats to U.S. national security—deriving from post–Cold War national security imperatives. Information attacks, delivered against information infrastructures accessible via the Internet and the public telephone network, were perceived as potentially serious new vulnerabilities for U.S. military forces.[3]

The SIW exercise used a Persian Gulf scenario, with impacts in the continental United States (CONUS) and Southwest Asia. The Persian Gulf was chosen as the venue for the exercise as the result of a lengthy test series that examined four different scenarios to see which best illuminated policy and strategy issues considered analytically important by RAND researchers and the DoD sponsors. The four scenarios were as follows:[4]

- *Persian Gulf major regional contingency (circa 2000).* Iran seeks hegemony over the Persian Gulf region by overthrowing the Saudi Kingdom via an antiregime organization within Saudi Arabia. A major military crisis develops. The U.S. government decides to deploy forces as a deterrent maneuver. Iran and the local Saudi opposition conduct IW attacks on the Saudi and U.S. governments.
- *Strategic challenge by China in the Far East (circa 2005).* China makes a very aggressive move toward regional dominance. The Taiwanese government declares "independence." China conducts a robust combined-arms military operation, including the use of SIW to deter a forceful U.S. political-military response.
- *Instability in Moscow (circa 1999).* A Russian federation, ruled by a weak central government, is in thrall to several transcontinental criminal organizations (TCOs). A major fissile material diversion

---

[2]Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War*, MR-661-OSD, RAND, 1996, p. xii.

[3]For a detailed discussion of these issues, see *Critical Foundations: Protecting America's Critical Infrastructures*, the Report of the President's Commission on Critical Infrastructure Protection (PCCIP), Department of Commerce, Washington, DC, 1997.

[4]Molander, Riddile, and Wilson, *Strategic Information Warfare,* p. 6.

to Iran is attempted by a Russian TCO. A Russian TCO makes extensive use of offensive and defensive IW to counter opposition from the United States, several major states within the European Union (EU), and the Russian government.

- *A second Mexican revolution (circa 1998).* The Mexican government faces major challenges from the Chiapas region in southern Mexico and from antiregime movements in northern Mexico. The Mexican revolutionary movements and nongovernmental organization (NGO) allies in North America make extensive use of perception management techniques to dissuade the U.S. government from taking any forceful political, economic, or military action to shore up the beleaguered Mexican regime.

This spectrum of scenarios was adopted to explore in what contexts SIW tools, techniques, and use concepts could be studied. The Persian Gulf was selected to satisfy both the researchers' analytic judgments and the sponsors' policy development requirements,[5] for the following reasons:

- The potential of physically damaging attacks on the United States put in question the physical sanctuary of CONUS.
- A fundamental tenet of U.S. military strategy is to deploy forces to suppress would-be regional hegemons before they succeed and graduate to would-be global hegemons.
- Iran would consider a Persian Gulf scenario to be strategic warfare. Whether a regional adversary uses IW to fracture a coalition or to undermine U.S. or European domestic support for intervention, it plays a strategic game and thus forces the United States into a strategic engagement as well.
- The strategic vulnerabilities and attacks that the United States and its allies might suffer introduce the possibility that other strategic weapons (e.g., nuclear weapons) might be either brandished or used outright.

OSD's planning requirements were a major factor as well. In the end, it is hard to differentiate the scenario's timing and locale from the

---

[5]Molander, Riddile, and Wilson, *Strategic Information Warfare,* p. 8.

analytic reasons underlying scenario selection. This is to be expected where experiential data are obtained using such focused exercise techniques. The policy concepts under examination were a product of independent researcher expertise and repeated interaction with a governmental client. Interactions between clients and sponsors were deliberately structured so that the interests and priorities of the involved departments and senior decisionmakers could be understood. This understanding was then used to write the scenario, which, in turn, was iterated with the sponsor before being subjected to the test series.

Note, however, the interactive nature of the scenario choice process. The exercise tests—which used the other scenarios as well as the one ultimately selected—were each tested in a series lasting from February through June of 1995. Participant feedback on issues, exercise design, and strategy and policy concepts was integrated into each successive test. The entire process was designed to elicit the maximum participant exposure to concepts, scenario variations, and policy problems—in essence, serving as a collective exploration of policy alternatives and possible futures.

Cyberpayments and Money Laundering

The Day After exercise that focused on international money laundering and cyberpayment technologies[6] was undertaken for the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN). The concern was that money launderers would use advanced payment system technologies to conceal their illicit activities.

FinCEN is an interagency clearinghouse for financial crime; it also administers reporting requirements for financial institutions under the Bank Secrecy Act.[7] Many analysts feared that the adoption by narcotics traffickers and transcontinental criminal organizations (TCO) of advanced information technologies would sharply cut the

---

[6]*Cyberpayments* is a term FinCEN coined to describe new payment system technologies that facilitate decentralized (and increasingly, peer-to-peer) value transfers analogous to the exchange of paper currency. Examples of these products include Internet-based e-cash products (such as cybercash) and stored value–type smart card instruments (such as the Visacash and Mondex products).

[7]For information about FinCEN, see http://www.ustreas.gov/fincen/.

efficacy of law enforcement's investigative tools and techniques. Such fears lent urgency to the discussions during the test series. They also opened the research sponsor to new ways of countering emerging patterns of payment system abuse.

RAND analysts, none of whom had any background in researching financial institutions or financial crime, undertook a direct and self-conscious research effort to orient themselves to the money laundering and financial crime landscape. This necessitated a close collaboration with the client and with stakeholders from the financial sector (whom the client helped identify).

The study's objectives were ambitious.[8] The main goal was to explore the dimensions and implications of potential future illicit uses of cyberpayment systems by money launderers and others seeking to conceal funds from governmental authorities so as to identify—at least in a preliminary fashion—possible law enforcement and regulatory responses.

This exercise brought together both public- and private-sector stakeholders. Indeed, FinCEN's interest in the project was driven by hopes that it could serve as a venue for interaction between the public and private sectors. The project's design and question formulation activities were helped by great cooperation from financial firms. As new technologies were anticipated in the payment system, financial industry figures argued for close coordination among state and federal regulatory agencies and private depository institutions. The Day After project served this end and helped to deepen the debate on cyberpayments and the future of payment system technologies.

The research goals of this project were to[9]

- Describe the then-current cyberpayment concepts and systems.
- Identify an initial set of cyberpayment characteristics of particular concern to law enforcement and payment system regulators.

---

[8]See Roger C. Molander, David A. Mussington, and Peter A. Wilson, *Cyberpayments and Money Laundering: Problems and Promise*, MR-965-CTI, RAND, 1998, p. 2.

[9]Molander, Mussington, and Wilson, *Cyberpayments and Money Laundering,* p. 3.

- Identify major issues that cyberpayment policies will need to address.
- Array appropriate approaches to address potential cyberpayment system abuse in a set of potential action plans.

The last goal was particularly challenging. The potential for responses to problems discovered during the exercise was clearly tied to how accurately the future of electronic payment systems was portrayed. The credibility (and longevity) of any recommendations produced by the project were contingent on good technological and market predictions.

Participants included representatives from the executive branch of the U.S. government, the cyberpayment industry, the banking industry, Congress, and academia. Exercise experiences were recorded in the test series underlying the final version of the scenario and in the final operational play itself.

The scenario selected was developed in collaboration with law enforcement officers expert in financial crime and money laundering investigations. It involved a large money laundering system that narco-traffickers used to conceal drug earnings. Funds transfers were concealed by using stored value–type smart cards for street-level drug purchases and then uploading the value into the financial system using merchant stored-value upload terminals. "Participating" store owners received a 4 percent "commission" on each of these transfers. Once the funds reached the financial system, they were electronically transferred offshore using sophisticated layering and integration techniques to hide their ultimate destination.

The scenario narrative then described the compromise of critical technologies used in the manufacture of stored value–type smart cards themselves. This created an even greater threat, one to the integrity of the U.S. and international financial systems. The final portion of the scenario involved a fictional proposal by the Mexican finance ministry to modernize its own banking infrastructure through the adoption of modern electronic banking technologies. This gave money launderers a potential opportunity to penetrate a brand new financial structure and secure unprecedented money laundering capabilities over the long term. The threats to financial system integrity

motivated decisionmaking during the future history, step one, and step two.[10]

The exercise findings contained the responses of participants to such dilemmas along with a major analytic examination of those perspectives for integration into competing themes and frameworks. The action plans produced for the report were thus the product of expert assessments by third parties (exercise participants) and post hoc analysis of the deliberations by RAND analysts.

Comparison of the Two Implementations of the Methodology

A comparison of the two projects helps to illustrate the different contexts in which policy analysis interfaces with decisionmaking. In the SIW project, analysts developed scenarios in advance of their real-world appearance by extrapolating known technological trends and factoring in the continuing concerns of the national security community about potential impediments to the execution of U.S. national military strategy. Because U.S. national military strategy focuses on projecting power overseas rather than on defending the homeland, the analysis concentrated on infrastructure vulnerabilities relevant to military preparedness. Similarly, the adoption of asymmetric "counter–information infrastructure" strategies by potential adversaries would place the sanctuary of homeland into question. Hence, infrastructure concerns are related to the concern over the weakening influence of distance as a barrier to potential attacks.[11] These two concerns motivated the selection of both the scenario and the types of attacks presented.

The principal objective of the cyberpayments and money laundering study was to help facilitate a dialogue between government and private-sector personnel on a subject of near-future importance. This project involved a much more in-depth concept-creation process, one in which a community not used to thinking systematically about national strategies was introduced to wide-ranging concepts

[10]See Molander, Mussington, and Wilson, *Cyberpayments and Money Laundering,* Appendix B, Exercise Materials.

[11]Homeland security emerged as the preeminent national concern following the events of September 11, 2001.

through the scenario design process. The decentralized nature of law enforcement here gave rise to diverse assessments of long-term trends in criminal activity and to potential investigative countermeasures. Federal law enforcement authorities lead the anti-money laundering arena, but must collaborate with state and local law enforcement officials in individual cases. The international component of anti–money laundering law enforcement activities adds further complexity.

Concepts created in this exercise range from a listed feature set for cyberpayment instruments that defines their importance for potential misuse by money launderers, to a mechanism for tracing Internet-based electronic fund transfers.[12] Both concepts contributed to a framework that defined the technologies of importance to law enforcement and the opportunities for law enforcement to leverage these technologies to enhance investigations. An issue that emerged very quickly during this design process was the lack of clear metrics or measures for anti–money laundering techniques and strategies. Before the project, research sponsors did not appreciate how automation could help evaluate competing strategies for interdicting illicit funds movements. During the test series, this factor was proposed by the design team and emerged as a major focus of future attention for decisionmakers.[13]

Another difference between the two projects stemmed from their differing analyst-sponsor relationships. DoD has had a historically close relationship with RAND (and other independent think tanks). Thus, well-known contracting vehicles and advisory relationships existed for supporting policy analysis. FinCEN, by contrast, had never used independent third-party analysts. The analysts thus needed to foster a close working relationship with FinCEN staff during the exercise design process. Analysts and FinCEN staff had to negotiate who was to author the recommendations of the outbrief report. RAND had to preserve the independence (and peer-review quality control) of the project report's findings while showing sensitivity to the concerns of a client that feared public embarrassment if the exercise results "got out in front of" government policy.

---

[12]Molander, Mussington, and Wilson, *Cyberpayments and Money Laundering,* p. 21.

[13]Molander, Mussington, and Wilson, *Cyberpayments and Money Laundering,* p. 27.

The two exercise programs shared a public sector/private sector character. They served as environments to facilitate dialogue *and* as experimental settings in which policy concepts could be discussed, deconstructed, and critiqued. Although the Day After process hinges on bringing disparate communities of experts together, such interaction must be carefully structured to preserve its analytic independence. In the design phase of a Day After project, new concepts are created and discarded as a way of understanding a subject. Sponsors, however, may interpret such notions as indicators of the project's conclusions. As with sausage-making, the process is messy but the results are often worth the chaos of creative interaction.

The Day After and Analytic Independence

Analysis of the findings is central to the Day After methodology. The exercise designers undertake this analysis, ideally at arm's length from the research sponsor. Because sponsors are extremely engaged in exercise design, they often feel the need to "manage" the production of the report summarizing the project's deliberations and thematic insights. Yet the independence of these two items must be maintained.

A narrative report of findings, records of answers to questions, guidelines used for discussion, and concept creation is, quite appropriately, a shared enterprise; sponsors often provide note-takers and equipment to record deliberations accurately. Nevertheless, analyzing the *meaning* of the facts, insights, and conclusions of experts who interacted within a hypothetical scenario under severe time constraints remains the task of the exercise analysts. They, alone, share a conceptual understanding of the subject matter *and* an architectural knowledge of the scenario construct. Because the exercise scenario necessarily evokes real-world dilemmas, practitioners and policymakers may bring powerful preconceptions to a review of the scenario findings. The Day After method requires that the principal architects of the scenario materials act as filters, differentiating the details and nuances of the story line from the participants' responses to the story. The two projects described above evolved in ways that highlighted the importance of bias control. Both times, RAND was asked to extend the exercise results into a more in-depth examination of the subject matter. The first produced a

conceptual framework for understanding the emerging IW policy environment. The second expanded issues addressed in a domestic U.S. setting into an exercise involving 27 countries from the Americas and the Caribbean.[14]

Although details differed in each case, some thematic points can be made. First, the *SIW Rising* document was prepared entirely by the design team, using traditional analytic approaches entailing brainstorming and internal RAND presentations of interim insights, followed by the drafting and redrafting of analytic concepts and models. The resulting policy framework was derived from the reports and exercise experiences achieved during other successful exercise projects. Analyzing those findings generated recurrent themes and insights that contributed to a statement about the nature of the IW setting as it may develop over the next few decades.[15]

Second, the sponsor received the report's analytic framework but not a clear "action plan" for the agency's evaluation. The sponsor already was familiar with the key concepts; many had gained support from Defense Science Board publications and other publicly available research. *SIW Rising* contributed to the policy debate by exposing senior OSD and ASD C3I (Assistant Secretary of Defense for Command, Control, Communications, and Intelligence) staff to concepts that emerged from the non–national security environment that had the potential to affect their plans and priorities.

The follow-on 26-nation cyberpayments study focused on the investigative and prosecutorial implications of money laundering using emerging payment system technologies. It required a new scenario, one that added a section on Internet gambling to the base case of potential misuse of cyberpayments technologies for the purposes of money laundering. The multijurisdictional investigative and prosecutorial nature of the money laundering problem was the focus for much of the design activity, which included employees of the

---

[14]The two reports concerned are Roger C. Molander, Peter A. Wilson, David A. Mussington, and Richard F. Mesic, *Strategic Information Warfare Rising*, MR-964-OSD, RAND, 1998; and David A. Mussington, Peter A. Wilson, and Roger C. Molander, *Exploring Money Laundering Vulnerabilities through Emerging Cyberspace Technologies*, MR-1005-OSTP/FinCEN, RAND, 1998.

[15]Molander, Wilson, Mussington, and Mesic, *Strategic Information Warfare Rising*, pp. 33–38.

Caribbean Financial Action Task Force (CFATF) and the Commonwealth Secretariat of the United Kingdom.

Because the cyberpayments exercise was meant to build a consensus action plan to address legislative, policy, and operational changes in anti–money laundering activities, its scenario had considerable political sensitivity. Thus, the scenario had to be iterated with the research sponsor to a much higher degree than usual, with considerable and detailed dialog taking place on the timing, technical description, and credibility of scenario details. In addition, the test series for the exercise entailed coordinating materials among the 26 countries participating, as well as translating game materials into Spanish.

Interaction with industry representatives provided the required details on Internet gambling and transnational electronic banking trends. Technical details in the exercise were updated with this new information, and elements from the prior exercise were also used. Scenario component reuse is a central feature of Day After scenario design; it leverages issue expertise acquired across a number of different potential projects.

The educational component of the cyberpayments exercise was much more pronounced than any other component (many Caribbean nations lacked basic familiarity with the subject matter). It was important that we educate while avoiding the perception that the Day After approach was "U.S. lecturing." Shared insights and consensus building were the clearest process objectives in the project's execution. The project achieved its objectives, with a draft agenda of priorities resulting from the meeting. In turn, model legislation to respond to many of the policy dilemmas identified within the Day After scenario was to be collaboratively developed by several participating countries. Overall, the exercise helped international dialogue; it also prepared the ground for further policy development.

THE VALUE OF THE DAY AFTER

The Day After method helps decisionmakers and policy analysts address complex subjects in an environment of hypothetical threats to policy goals and objectives. The design of scenarios in this methodology is critical, with plausibility and technical accuracy balanced

against the need to focus participant attention on the key themes and analytic issues.

As noted, the Day After requires the creation of a quasi-experiment in which expert insights serve as basic facts in the context of a dynamic scenario. Assumptions that go into the scenario's future history are made as explicit as possible and then honed during repetitive testing of the exercise materials and scenario details.

The Day After methodology can frame futures that challenge analyst and research sponsor assumptions. Can a Day After scenario escape the preconceptions of the designers or the research sponsor? The answer is a qualified yes. It is possible to define scenarios and pose issue questions that challenge the presumptions of both the research sponsors and the researchers. It is not an easy task to accomplish, however, and requires a self-conscious and skilled exercise design approach.

The Day After methodology offers a mechanism for analyzing policy problems. Until now, the methodology has been applied principally to problems with a dynamic component—where technology and technological change affect the policy environment in unpredictable ways. Addressing such situations requires that maximum scope be given to exploring policy futures in order to discern thematic and issue-specific points of decision critical to the goals and/or interests of the research sponsor. This exploration feature of the Day After exercise design process differentiates it from other, more static gaming methodologies.

Lastly, the Day After method educates and raises the consciousness of participants by immersing them in an environment where they suspend disbelief and are made to challenge the views and perceptual frameworks they bring to specific problems. This forces participants to "come up to speed" quickly on complex policy problems and makes them familiar with the characteristically great uncertainty of future-oriented, technologically rich policy environments. The value of this last contribution should not be underestimated. Policymakers face difficult choices, in areas where information is hard to distinguish from advocacy. By offering a critical and rigorous process in which facts and biases are examined, the Day After methodology makes a powerful contribution to the tool kit of policy analysis.