# Chapter 2
# Implementing the Process

To address the potential for nanotechnology to impact chemical and biological (CB) defense and proliferation, the *Nanotechnology for Chemical and Biological Defense Project* – known as NanoCBD2030 – was designed to explore the potential use and misuse of nanoscience, nanotechnology, nanoengineering, and analogous emerging technologies in order to formulate a strategy to inform and guide the development of federal science and technology capabilities for the next 25 years.

The charges to those involved in all parts of this effort were the following:

1. Innovate solutions and strategize potential countermeasures to current CB threats leveraging revolutionary developments in nanotechnology,
2. Anticipate proliferation scenarios in which nanotechnology is put to malicious use by terrorists or nation-states,
3. Strategize potential countermeasures to defend against such uses, and
4. Recommend research directions and priorities to enable the long-term science capabilities for CB defense.

A significant part of the *Nanotechnology for Chemical and Biological Defense Project* was the workshop sponsored by the Department of Defense's Chemical and Biological Defense Program (CBDP), which brought together a diverse set of practitioners and researchers in Santa Fe, New Mexico in 2007. The workshop substantially contributed to the development of scenarios on and strategies regarding the potential benefits and threats of nanotechnology for national security.

This book attempts to capture the unique insights gleaned from a distinctive mix of leading experts in science, international security, military affairs, intelligence, medicine, engineering, and policy, who participated in various parts of this project, most notably as participants in the NanoCBD2030 Workshop. While logistical considerations limited the total number, the group comprised many individuals who have not been normally called on to evaluate this emerging intersection of science, technology, security, and policy. The study participants were selected to encourage the open exchange of intellectually provocative ideas and to entertain challenging concepts. The majority of the participants were chosen for their expertise with different aspects of CB defense or with nanotechnology – from the cutting edge scientific to operational, intelligence, economic, and political science experience. In addition to their

M.E. Kosal, *Nanotechnology for Chemical and Biological Defense*,
DOI: 10.1007/978-1-4419-0062-3_2, © Springer Science+Business Media, LLC 2009

recognized expertise, participants were chosen on the basis of their diverse real-world operational and analytical experience.

An example of profound utility of having scientists and technologists interact more closely with operators can be found in the history of research on shipboard firefighting. A purely requirements-oriented approach drove researchers to develop bigger and more powerful nozzles to get more water to a fire faster and with higher velocity. In the 1980s, a technology was proposed that could pinpoint flame location through smoke and mist, which enabled the use of less but more precisely directed water to extinguish a fire. This realization drove basic science toward a new field of thermal imaging, rather than continuing only to improve fluid flow through nozzles.

The terms nanotechnology, nanoscience, and nanoengineering are broadly defined and applied in this book. Unless there is a specific reason for differentiating the terms, nanotechnology has been used throughout the study as a stand-in descriptor to encompass nanoscience, nanotechnology, and nanoengineering. In alignment with the National Nanotechnology Initiative definition, "nanotechnology is the ability to work – to see, measure, and manipulate – at the atomic, molecular, and supramolecular levels, in the length scale of approximately 1 to 100 nm range, with the goal of understanding and creating useful materials, devices, and systems that exploit the fundamentally new properties, phenomena, and functions resulting from their small structure." Interaction distances are not the sole determinant of relevance; however; the emphasis is on the unique properties or capabilities that are conveyed at the nanoscale. Further, the term nanotechnology refers to more than working with a lone atom or single molecule. Working at the nanoscale may be most relevant when translated from the nanoscale through the micro- and mesoscale ("middle" scale) to the macroscale. As a result, the technologies and necessary infrastructure to interact, manipulate, and generate the materials or products on the nanoscience scale were also considered as part of the workshop. For example, a microelectronic mechanical system reactor capable of enabling self-assembled materials with unique properties at the nanoscale from macroscale fit well within the workshop and study charge.

## Scenario-Based Planning

*Scenario planning is a tool for ordering one's perceptions about alternative future environments in which one's decisions might be played out.*

Peter Schwartz, 1996[1]

A number of scenarios were considered that were based on combinations of various environmental factors. These were then used to generate recommendations for action, including a list of overarching, strategic research directions. The goal was to generate innovative and revolutionary concepts of the application of nanotechnology and analogous emerging technologies for CB defense and counterproliferation.

Scenarios are routinely used not only in corporate strategic planning[2] but also in public policy planning[3] and national security planning.[4] In finding ways to consider the key drivers and identify the more visionary paths, traditional "requirements-driven" planning for R&D is inadequate.[5] A systematic method of long-term planning was needed that is more useful in cases of large uncertainties in the external drivers on the enterprise. Scenario-based planning endeavors to gain knowledge for the future by understanding the most uncertain and significant driving forces affecting potential outcomes. It is a group process which encourages learning and a better understanding of the nature and impact of organizational actions. The process is structured intentionally to break simple extrapolations and enable nonlinear and dynamic ways of capabilities-based planning. By setting discussions far enough in the future – far enough beyond facts and forecasts – discussants will encounter less defensive behavior and a more shared sense of purpose.[6]

## *The Process*

The goal of this process was to identify major factors and events that would drive global change through 2030. To do this, four alternative global futures were developed in which these drivers would interact in different ways from the present through 25 years in the future. Each scenario was intended to lead to plausible, national security, and technology policy-relevant stories of how this future might evolve. Each story would highlight key uncertainties, discontinuities, and unlikely or "wild card" events, and identify important policy and technical challenges.

Technically robust scenarios may illustrate the potential malfeasant cooption of nanotechnology. Scenario analysis is useful for defense planning and resource allocation, with the goal to enable detection and possible interdiction before threats become imminent, to defeat nanotechnology-based threats at a distance, and to mitigate consequences of such an attack. Presenting scenarios in any area with risks for application to weapons must be approached with great sensitivity and consideration. In this process, scenarios were grounded thoroughly in observed scientific results available in the open literature. It was also important to exclude details an adversary would need to turn a concept into an operation or a technology into a weapon. The scenarios discussed herein are not intended to be exhaustive but are intended to help delineate the possible from the realm of science fantasy.

The subject matter of this chapter was approached with great sensitivity and care. Foremost, the scenarios described herein are grounded thoroughly in scientific research vetted through the open literature rather than in science fiction or fantasy. While all of the underlying science is real, the scenarios are notional. Operationalization of the threat scenarios or any individual threat was intentionally excluded. These scenarios are not a "terrorist roadmap" or even a guide for a well-financed state with advanced infrastructure. Additionally, scenarios that have previously been suggested, generally of the "nano-bot" or "grey goo" variety, are addressed and in some cases debunked. The degree of difficulty and intricacy of the scenarios varies substantially. Steps 1–3 used in the overall study process were loosely based on Peter Schwartz's scenario planning process.[7]

1. Independent drivers affecting the enterprise were identified and isolated for independent versus dependent variability. These factors included the relationship between science and national security, the unfolding science of nanotechnology, the underlying science of CB weapons, the perspective of the warfighter, and the pace of technology change.
2. From the independent drivers identified, two critical key drivers that are both important and the most uncertain were selected. The two key drivers that met this criterion were the pace of technology change – ranging from evolutionary to radical – and the evolving nature of warfare – ranging from traditional to highly irregular. This can be concisely portrayed in terms of the principal adversary to the US varying from a traditional Westphalian state to nonstate actors lacking a specific homeland. Plotting these two drivers orthogonally resulted in four speculative "worlds" that could exist in 2030, as shown in Fig. 2.1. The selection of these two drivers demonstrates the overarching relevance of the science and technology factors to defense policy and international security factors.
3. On the basis of the characteristics in each quadrant, notional scenarios – short stories – of potential futures were drafted.

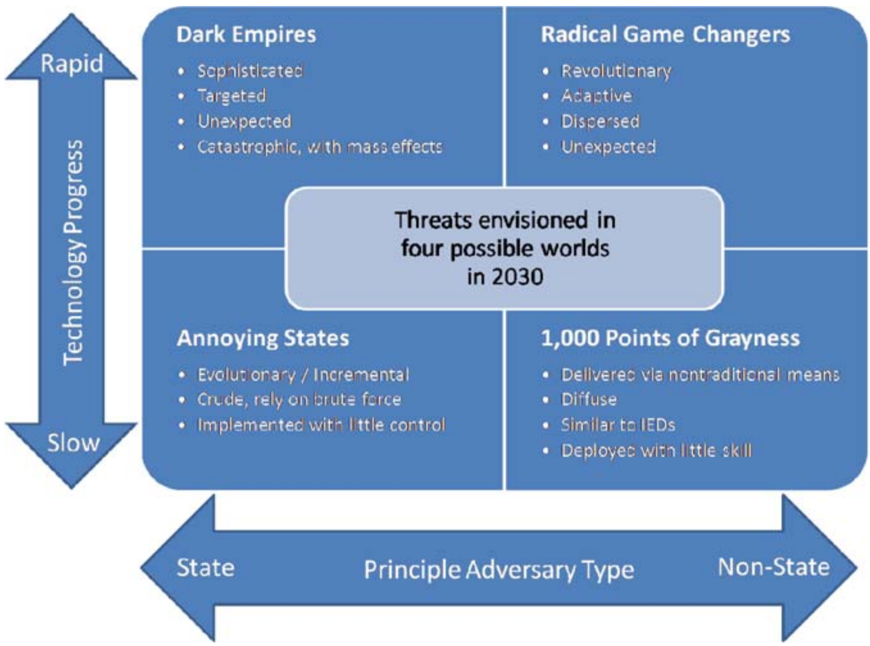


**Fig. 2.1** The characteristic descriptors – shown in quadrants – of notional 2030 worlds that drove the scenario development process

4. After that, the implications of each scenario for the science and technology community were determined, including consideration of active "red-teaming" the defensive countermeasures and "blue-teaming" the proliferation scenarios. These implications are described in details in Chapts. 3 and 4.
5. On the basis of these implications, plausible research and development strategies to respond to each scenario's implications were developed. These strategies are complied in Chap. 5.
6. Finally, science and programmatic management policy recommendations to enable the US to respond more fully to current CB defense agents and future threats were developed. These recommendations are included in Chap. 5.

A more detailed discussion of the scenario process follows.

## *Creation of 2030 Worlds*

Four worlds were envisioned, as shown in Fig. 2.1.

### Radical Game Changers

*Radical Game Changers* is a 2030 world driven by nonstate actors and rapid technology development. It is a revolutionary, adaptive, and dispersed world, in which the unexpected routinely must be anticipated. The armed forces, civilian personnel, and national infrastructure are facing a new and radically different set of challenges. This world is characterized by asymmetric and nontraditional threats to the US. Sophisticated nonstate actors are likely to develop significant and unexpected set of CB agents that have the high potency and maximum detection and protection avoidance. Answering such radical challenges will require an equally radical change in the detection and protection strategies from known to unknown. In addition, the increased potency and lethality of these agents will drive diagnostic speed and increased integration between diagnostics and countermeasures. In addition to traditional investment to develop revolutionary capabilities, this world may likely require stronger interactions with nontraditional disciplines such as anthropology and more effective use of strategic communications.

### Annoying States

*Annoying States* is a 2030 world driven by state actors and slow technology development. It is an evolutionary, traditional, incremental, and brute force world that extends linearly from traditional military operations – similar to many twentieth century low-level conflicts. In addition to concerns of proliferation of traditional twentieth century CB agents, improvised chemical or biological dispersive devices, such as those that co-opt industrial chemicals and basic industrial processes, are not atypical for this world. Drivers in this world include simple dispersion of classical and industrial knowledge, increase in many small- or medium-sized regional state-on-state conflicts, the need for accurate monitoring, and the capability for quick attribution, as well as sharpened diplomacy.

**Dark Empires**

*Dark Empires* is a 2030 world of state actors and rapid technology development. It is a sophisticated world that deploys threats with catastrophic and mass effect and, in which, the unexpected routine must be anticipated. This class of scenarios deals with the technologically sophisticated state adversary capable of delivering multiple threats to multiple allied targets both domestic and overseas – the peer competitor, who will have not only a sizable uniformed military of its own but also intelligence and technological institutions on which to draw support. Innovation is highly likely, underpinned, and funded by large state institutions and access to materials, processes, and knowledge across a sophisticated technological state. Drivers include prevention through international diplomatic means (both traditional and new), large-scale, integrated monitoring capabilities, as well as quick and robust attribution and response.

**1,000 Points of Grayness**

*1,000 Points of Grayness* is a 2030 world driven by nonstate actors and slow technology development. This is a diffuse world which subverts traditional delivery systems or benevolent commercial technology and turns them into threatening and indiscriminate purposes, using relatively unskilled technologies to pursue disperse insurgent tactics. Like the Annoying States world, crude improvised chemical or biological dispersive devices, such as those that co-opt industrial chemicals, are not atypical for this world. Like the Radical Game Changers World, this world will likely require stronger interactions with nontraditional disciplines, such as anthropology, human terrain knowledge, and more effective use of strategic communications.

## *Envisioning Scenarios in the Four Worlds*

In order to encourage disruptive leaps forward in nanotechnologies and enabling systems and minimize linear extrapolation, the setting for construction of the notional scenarios was such that one might imagine falling asleep and awakening in 2030 in each of these four possible worlds. The “four worlds” (or quadrants) have different assumptions about the pace of technology change over the next 20 years and include consideration of accessibility, cost, globalization, economic, social, and political factors. These are matrixed against a consideration of traditional “state-based” enemies and the more irregular “nonstate” adversaries. Within the workshop setting, participants were divided into focus groups for the development of specific scenarios. The groups were charged to examine the

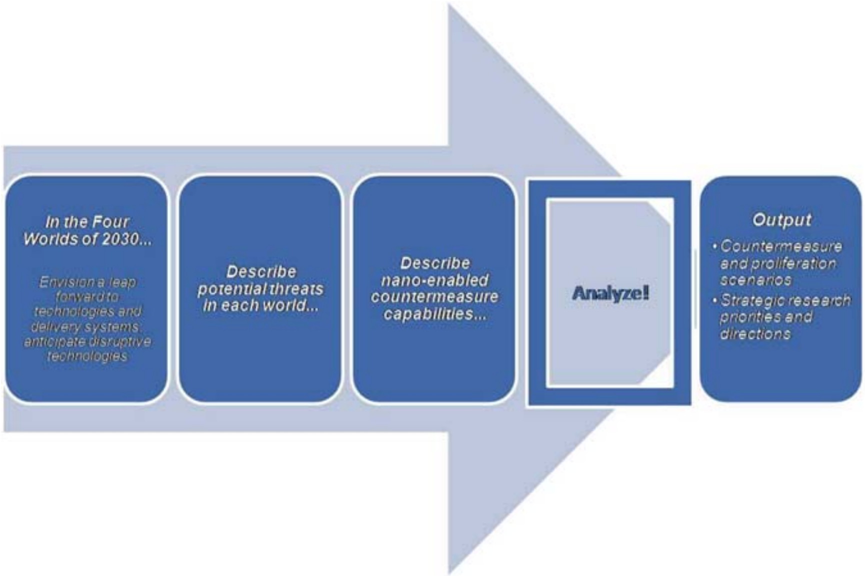


**Fig. 2.2** Overall process

development of countermeasures and the challenges of malfeasant cooption of nanotechnology. This process is shown in Fig. 2.2.

For countermeasures development, possible CB defense capabilities against areas where the US currently lacks solutions or has less than ideal passive defense capabilities were explored. One example is standoff biological detection or featherweight personal protection filters. Ideas were separated in to four general areas: (1a) detection and diagnostics of biological agents, (1b) detection and diagnostics of chemical agents, (2) physical protection, (3) decontamination, remediation, and consequence management, and (4) medical countermeasures. Each area had some overlap, which became more apparent throughout the course of the project.

For each quadrant of the worlds, the desired state of countermeasure development was conceived and then new fields that could contribute to capability development were identified. Additionally, enabling infrastructures upon which such capabilities will depend and the limits to the use of countermeasure against different adversary types were considered.

For the misuse of nanotechnology, the groups explored scenarios in which state or nonstate adversaries might use nanotechnology applications against the US and allies. These groups also considered proliferation challenges. The specific threats considered were new or nanoenabled biochemical agents; malfeasant exploitation of the toxicological or other deleterious health effects; evasion of vaccines, innate human immunity, or other medical countermeasures; and self-assembled materials and devices to molecular assemblers. All of the scenarios developed were based on sound scientific principles and within technical capability of the best scientists in the best laboratories; they also purposely lack meaningful concepts of battlefield operations.

For each quadrant of the worlds, the focus groups then asked how nanotechnology might be used against US forces and our allies. They looked at the worst, technically reasonable scenarios. Other questions also included the consequences of the principal threats, and whether they are catastrophic or of limited use. This included discussion of how weapons might be delivered and the enabling infrastructure required. The limits to acquisition by the different adversary types were also discussed, and finally, the factors that could drive proliferation forward or hinder it.

After presenting the scenarios to the overall workshop, the focus groups shifted emphasis to identifying and developing research directions with strong science and national security justification to achieve those 2030 capabilities for countermeasures and strategies toward limiting the threat of malfeasant actors, realizing any part of the 2030 proliferation scenarios. General considerations included the identification of supporting research directions needed and bottlenecks to overcome to achieve success, delineation of factors – technical and nontechnical – that would slow or speed development of countermeasure capabilities or threats, and articulation of key developments (breakthroughs, new platforms, and enabling infrastructure, and so on) that have to occur by 2010 and 2020 for the 2030 scenarios to occur.

For the challenges of malfeasant cooption of nanotechnology, the participants also identified critical nodes or events to interdict negative consequences or crucial development points that are most disconcerting form a national security perspective, that is, places where effective programs can be implemented to prevent or limit a threat. Participants also considered the overall national security component supporting the need to develop such capabilities or the need to decrease the risk of a proliferation scenario. As a final component, the workshop considered the types of organizations or research entities that might be fostered in order to generate the innovative and revolutionary countermeasures for 2030.

## Using Scenarios to Roadmap and Prioritize

The scenarios generated in this process were used to help guide different communities – scientists, technologists, manufacturers, and end-users – to narrow their focus on technology drivers and to generate relevant research needs. At the end of the process, the scenarios were ranked by the attendees at the workshop using a balloting method to help pinpoint the highest priorities. This method took all viewpoints into account and resulted in a high fidelity list. These results are described further in Chapters 3 and 4 and the details are listed in Chapter 6.

### *Value of This Approach*

The NanoCBD2030 workshop and study gives the national and homeland security science and technology communities a forward-leaning roadmap of research directions for nanotechnology applications in CB defense. The process provides the DoD with an effective means of planning research and development tactics for relevant nanotechnology applications. The resulting recommendations can be leveraged for homeland security as well as such complementary aspects as intelligence and diplomacy, adding additional value to the effort. The strategic directions generated by the NanoCBD2030 Project have been used in the DoD's planning and budget process, and these outcomes will continue to influence the development of future directions for the nation.

## References

1. Schwartz P (1996) The art of the long view: Planning for the future in an uncertain world. Doubleday Business, New York.
2. Wack P (1985) The gentle art of reperceiving, *Harvard Business Review*. September-October: 73–89.
3. Kahn H (1960) On Thermonuclear War. Greenwood Press, West Port.
4. National Intelligence Council (2000) Global Trends 2015: A Dialogue About the Future with Nongovernment Experts. Government Printing Office 041-015-00211-2. http://www.dni.gov/nic/PDF_GIF_global/globaltrend2015.pdf Accessed 30 June 2008.
5. Department of Defense (2006) Defense Science Board Summer Study on 21st Century Technology Vectors. http://www.acq.osd.mil/dsb/reports.htm Accessed 30 June 2008.
6. Ringland G (2002) Scenario Planning Managing for the Future. Wiley, Chichester.
7. Schwartz P (1996) The art of the long view: planning for the future in an uncertain world. Doubleday Business, New York.