UNCLASSIFIED

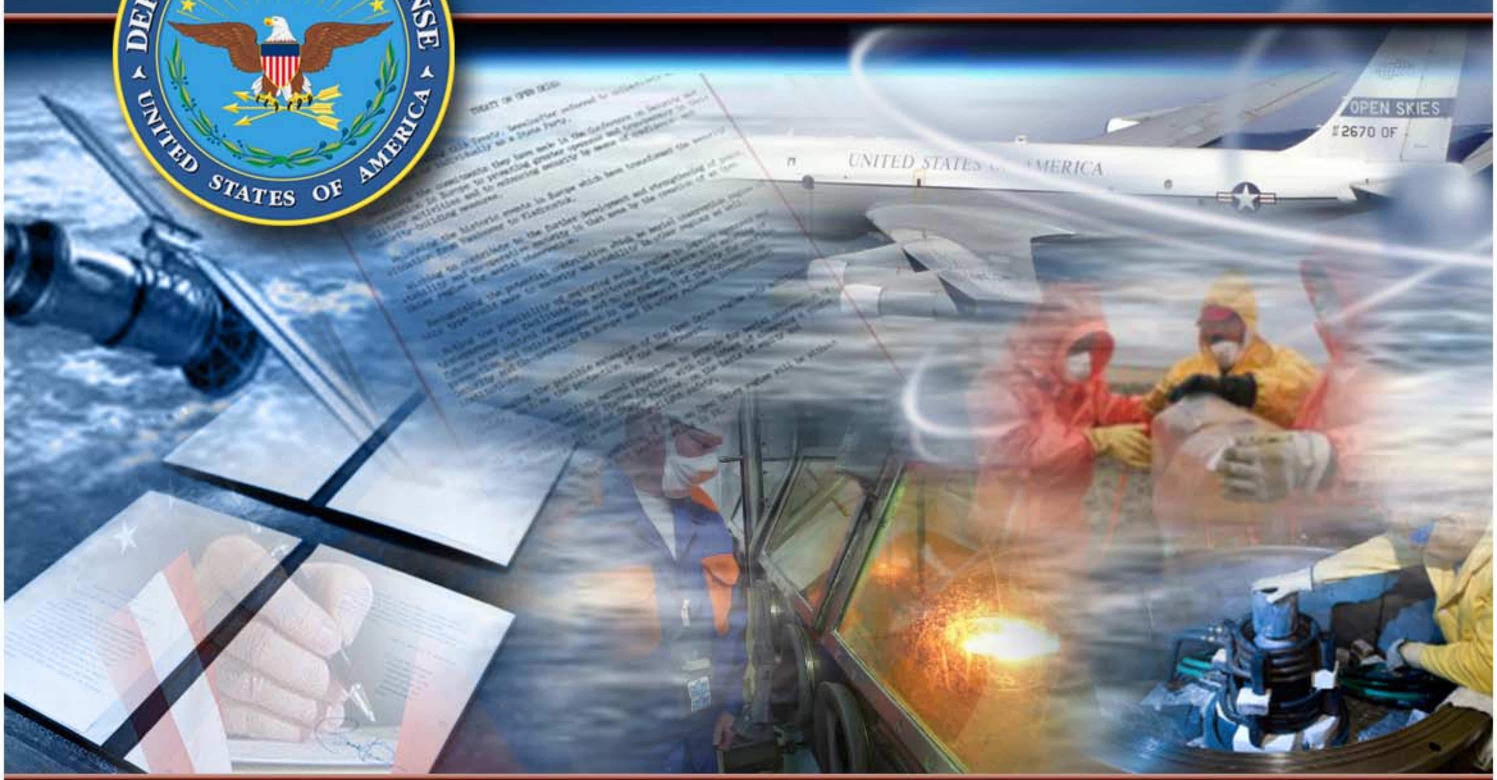
DEPARTMENT OF DEFENSE

DEFENSE SCIENCE BOARD

TASK FORCE REPORT:

Assessment of Nuclear Monitoring and Verification Technologies

January 2014



OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY AND LOGISTICS
WASHINGTON, D.C. 20301-3140

UNCLASSIFIED

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 JAN 2014	**N/A**	

4. TITLE AND SUBTITLE **Assessment of Nuclear Monitoring and Verification Technologies**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defense Science Board 3140 Defense Pentagon, Room 3B888A Washington, DC 20301-3140**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**103**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

The DSB Task Force on the Assessment of Nuclear Treaty Monitoring and Verification Technologies completed its formal information gathering in October 2011, but continued to update factual input through final report review.

OFFICE OF THE SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

DEFENSE SCIENCE BOARD

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY AND LOGISTICS

SUBJECT: DSB Task Force Report on Assessment of Nuclear Monitoring and Verification Technologies

I am pleased to forward the final report of the DSB Task Force on Assessment of Nuclear Monitoring and Verification Technologies.

A relatively straightforward, albeit technically rich, charge was given to this Task Force to assess technologies in support of future arms control and nonproliferation treaties and agreements. The Task Force, however, quickly realized that addressing this charge alone would be of limited value without considering a broader context for nuclear proliferation into the foreseeable future. That realization resulted from a number of factors which included:

- Accounts of rogue state actions and their potential cascading effects;
- The impact of advancing technologies relevant to nuclear weapons development;
- The growing evidence of networks of cooperation among countries that would otherwise have little reason to do so;
- The implications of U.S. policy statements to reduce the importance of nuclear weapons in international affairs, accompanied by further reductions in numbers, which are leading some longtime allies and partners to entertain development of their own arsenals;
- The wide range of motivations, capabilities, and approaches that each potential proliferator introduces.

In such a context, the technical approach for monitoring cannot continue to derive only from treaty and agreement dictates for "point" compliance to the numbers and types formally agreed upon and geographically bounded. Proliferation in this future context is a continuous process for which persistent surveillance tailored to the environment of concern is needed. This leads to the need for a paradigm shift in which the boundaries are blurred between monitoring for compliance and monitoring for proliferation, between cooperative and unilateral measures. Monitoring will need to be continuous, adaptive, and continuously tested for its effectiveness against an array of differing, creative and adaptive proliferators.

The Task Force therefore took a step back to create a comprehensive monitoring framework and to propose both improvements to existing tools and capabilities, as well as new approaches and dimensions to traditional monitoring means. Actions are recommended not only for DoD, but also for agencies in the larger national security community, that co-sponsored the study and for which DoD serves both supporting and supported roles.

Paul G. Kaminski

Dr. Paul Kaminski
Chairman

OFFICE OF THE SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

DEFENSE SCIENCE BOARD

MEMORANDUM TO THE CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: DSB Task Force Report on Assessment of Nuclear Monitoring and Verification Technologies

The Undersecretary of Defense for Acquisition, Technology, and Logistics directed the Defense Science Board to form a Task Force to assess the needs for nuclear monitoring and verification technologies in support of future treaties and agreements. The Terms of Reference stipulated that the Task Force should:

- Summarize future directions in nonproliferation and arms control treaties and agreements, including environment in which implemented
- Project demands on, and assess capabilities of, International Atomic Energy Agency in next 15-20 years with expected growth in nuclear power
- Assess current and projected gaps in technical capabilities to support anticipated monitoring and verification regimes
- Identify promising adaptations from advances made for other purposes; e.g.,
  - Close-in monitoring of targets in low signal/high clutter environments
  - Nuclear forensics and attribution
  - Stockpile stewardship
  - Nuclear weapons effects
  - Countering nuclear threats
- Propose new initiatives where needed, to include RD&T, red/blue teaming
- Perform a net assessment to help identify highest risks associated with potential technical implementation paths
- Recommend [time-phased] programs for DOD, DOE, IC - separate and/or combined - include State, DHS, and others where appropriate

Early in the study, the Task Force agreed that limiting its assessment to treaties and agreements alone, as the study's sponsors anticipated at the beginning of the study, would miss the more challenging problem to national security, namely the growing threat of both vertical and horizontal nuclear proliferation, for which treaties and agreements are important, but not exclusive, mitigating mechanisms. The Task Force therefore expanded its scope to include a broader assessment of technical needs to support nuclear proliferation monitoring within both cooperative and unilateral constructs. The Task Force's deliberations resulted in the following top level conclusions:

1. The nuclear future will not be a linear extrapolation of the past. The nature of the problem is changing significantly in a number of dimensions:

   - The number of actors and geographic scope are becoming too large to anticipate within treaty sanctioned and national technical means (NTM) monitoring regimes alone;
   - Security risks from threshold states are growing;

- Even “traditional” nuclear powers are modernizing in some non-traditional ways;
- The consequences of failing to detect clandestine materials/capabilities become magnified as disarmament proceeds;
- As a result, the lines between intelligence and traditional “monitoring” are blurring.

2. The technologies and processes designed for current treaty verification and inspections are inadequate to future monitoring realities, e.g.,

    - Identifying small or nascent programs,
    - Accounting for warheads instead of delivery platforms,
    - Characterizing nuclear vs. non-nuclear military operations,
    - Application of new technologies.

3. Solutions must involve the collection and exploitation of a wide range of secondary signatures that allow more complete and integrated information on nations’ overall nuclear postures (civil and military), the networks among them…and other players.

4. For both cooperative and unilateral actions, a paradigm shift is called for that includes:

    - Creating a national strategy and implementation plan supported by a planning and assessment team that cuts across agency boundaries chartered to identify needed capabilities that play against many scenarios;
    - Revamping the monitoring framework to identify proliferants early or well before the fact. The framework should:
        - Expand cooperative agreements;
        - Adopt / adapt new tools for monitoring (e.g., open and commercial sources, persistent surveillance from conventional war-fighting, “big data” analysis) across the IC, DOD, and DOE;
        - Develop and integrate technical capabilities with CONOPs;
    - Continuously experimenting to test assumptions, capabilities and approaches, and to get/stay ahead of adaptive proliferants;
    - Planning for a long period of building the political and technical groundwork for the next major steps, whether cooperative or unilateral.

Closing the nation’s global nuclear monitoring gaps should be a national priority. It will require, however, a level of commitment and sustainment we don’t normally do well without a crisis. However, lessons from the past tell us that progress can be made with a sustained effort in which experienced and competent professionals can devote their careers to the quest and pass on their wisdom to successive generations.

Dr. Miriam John
Co-Chair

Dr. Donald Kerr
Co-Chair

Table of Contents

List of Figures

Executive Summary

The Defense Science Board Task Force on Assessment of Nuclear Treaty Monitoring and Verification Technologies was established to examine a broad range of questions concerning the capability of the Department of Defense (DoD), the Department of Energy (DOE) and the Intelligence Community (IC) to support future monitoring and verification of nuclear nonproliferation and arms control treaties. The Terms of Reference (TOR) for the study, found in Appendix B, state the tasking. Given the breadth of the topics of interest to our sponsoring leadership and the time and resources available, the Task Force determined to focus on those aspects of the TOR that address what it views as the priority issue—namely, monitoring for proliferation. Assessments of strategies for monitoring nuclear activities in both permissive and non-permissive environments, and of our current technical capabilities and future requirements for successfully implementing those strategies, were made.

A Nuclear Future Unlike the Past and the Need for a Monitoring Paradigm Shift

Too many factors have changed, and are changing from our historic basis and experience developed throughout the Cold War. The list of factors that should give national leadership pause for concern is extensive, and includes the following:

- The actual or threatened acquisition of nuclear weapons by more actors—with a range of motivations, capabilities, and approaches—is emerging in numbers not seen since the early days of the Cold War. Many of these actors are hostile to the U.S. and its allies, and of greater worry, they do not appear to be bound by established norms nor are they deterred by traditional means;
- In some cases, nuclear forces are seen as the most affordable and effective alternative to deter superior conventional forces; i.e., nuclear weapons are viewed as a legitimate warfighting capability, especially if vital domestic or regional security interests are threatened;
- Fundamental nuclear knowledge is widespread and know-how increasingly accessible.
    - At the same time, ubiquitous information access and widespread observational tools are increasing inherent transparency;
    - However, recognition of such increased transparency by potential or actual proliferants incentivizes the employment of more sophisticated methods of denial and deception;
- The pathways to proliferation are expanding to include networks of cooperation among nations and actors who would otherwise have little reason to do so;
- The growth in nuclear power worldwide offers more opportunity for "leakage" and/or hiding small programs.

In this unfolding nuclear future, monitoring to support treaties is but one part of the overall monitoring requirement that should be driven by monitoring for proliferation. This broader scope presents challenges for which current solutions are either inadequate, or more often, do not exist. Among these challenges are monitoring of:

- Small inventories of weapons and materials, even as low as a single "significant quantity of fissile material";
- Small nuclear enterprises designed to produce, store, and deploy only a small number of weapons—intended as a proliferant's end goal, or as the first steps to achieve larger inventories or more sophisticated capabilities;
- Undeclared facilities and/or covert operations, such as testing below detection thresholds, or acquisition of materials or weapons through theft or purchase;
- Use of non-traditional technologies, presenting at best ambiguous signatures, to acquire both materials and components;
- Theater nuclear forces and associated doctrine, exercises, and training complicated by the use of mobile, dual-use delivery systems;
- Many more players to whom access by the U.S. or its allies will be limited or extremely difficult, some of whom will be globally networked with global access to relevant science and technology.

In short, for the first time since the early decades of the nuclear era, the nation needs to be equally concerned about both "vertical" proliferation (the increase in capabilities of existing nuclear states) and "horizontal" proliferation (an increase in the number of states and non-state actors possessing or attempting to possess nuclear weapons). These factors, and others discussed more fully in the body of this report, led the Task Force to observe that monitoring for proliferation should be a top national security objective—but one for which the nation is not yet organized or fully equipped to address.

The technical approach for monitoring cannot continue to derive only from treaty and agreement dictates for "point" compliance to the numbers and types formally agreed upon and geographically bounded. Proliferation in this future context is a continuous process for which persistent surveillance, tailored to the environment of concern, is needed. This leads to the need for a paradigm shift in which the boundaries are blurred between monitoring for compliance and monitoring for proliferation, between cooperative and unilateral measures. Monitoring will need to be continuous, adaptive, and continuously tested for its effectiveness against an array of differing, creative and adaptive proliferators.

A Comprehensive Monitoring Framework: Two "Whats" and Three "Hows"

The Task Force observed early in its deliberations that there are many communities involved in tackling a piece of the monitoring "elephant," but found no group that could clearly articulate the entire problem nor a strategy for addressing it in any complete or comprehensive fashion.

The Task Force therefore created its own framework, illustrated in Figure ES-1, as a vehicle for communicating its findings and recommendations, but also as a potential starting point for the many agencies involved to see how their efforts might integrate into a more effective whole.

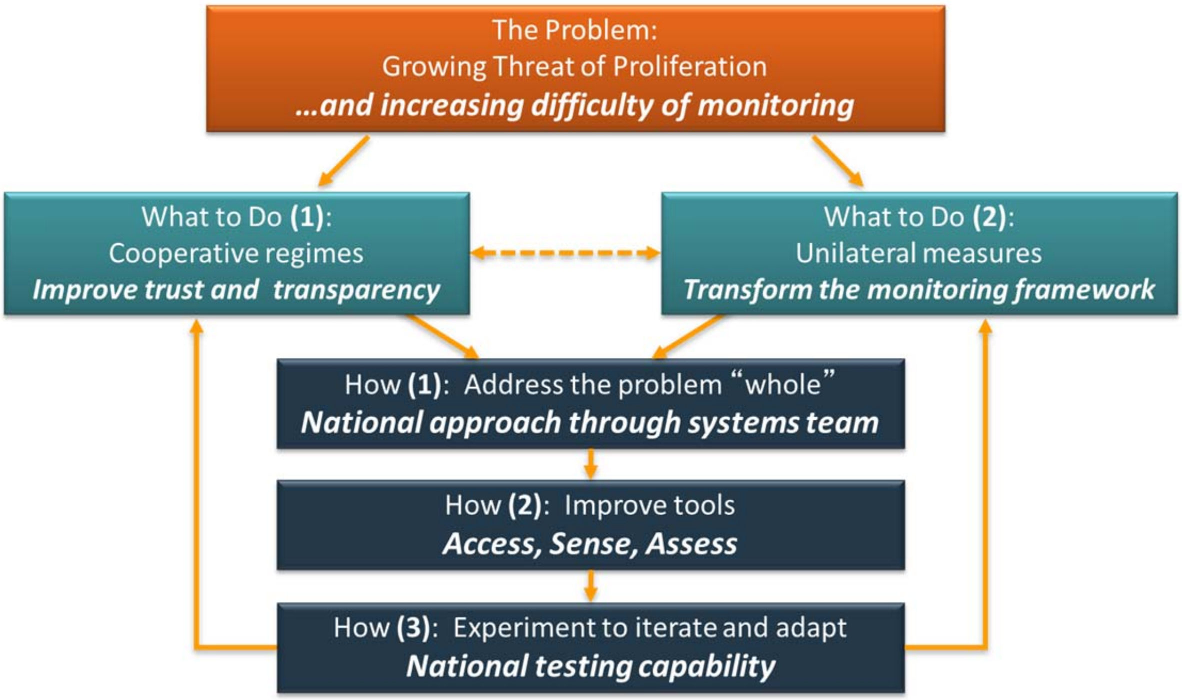


Figure ES-1 Plan for Long-Term Engagement and Commitment

The framework consists of five elements – two "whats" and three "hows." Each of the five, as noted by the byline for each in the figure, has a top-level strategic objective (e.g., the strategic objective for Cooperative Regimes is to improve trust and transparency). The "hows" are intended to contribute to both "whats," and the overall architecture is built with a continuous cycle in which fielded results from the "whats" inform priorities and gaps in the "hows." In turn, new capabilities from the "hows" improve execution of the "whats." The proliferation problem and framework development, plus each of the five elements of the framework are covered in separate chapters of this report. The summary of the findings and recommendations for each of the five elements follows.

Cooperative Regimes: Key Findings and Recommendations

International Cooperation and Transparency

Principal Finding: While many relevant programs and activities exist throughout the government, the U.S. lacks a cohesive, long term, international engagement plan aimed at building cooperation and transparency.

Recommendation: State/Bureau of Arms Control, Verification and Compliance (AVC) (diplomatic), DOE/National Nuclear Security Agency (NNSA)/ Defense Nuclear Non-Proliferation (NA-20) (technical), and DoD/Defense Threat Reduction Agency (DTRA) (operational) should jointly develop such a plan and cooperatively implement their respective/shared responsibilities. The Task Force recommends a 4-phase approach for expanded cooperation, each step of which would gradually evolve to "internationalize transparency inspections." The Task Force approach could be enabled by expansion of the role of the International Atomic Energy Agency (IAEA) for assuming responsibility for the transparency responsibilities that ultimately emerge:

1. Bilateral, cooperative developments and evaluations among P-5 states, building on experience in historic allied partnership programs, as well as the Cooperative Threat Reduction (CTR) program with Russia;
2. Extension to all nuclear weapon states;
3. Expansion to nuclear materials transparency among major states with nuclear power generation;
4. Negotiation of a future Non-Proliferation Treaty (NPT "X") to bring in all nuclear weapon and material programs into a cooperative, multi-lateral regime.

The three lead offices cited should establish a Multi-Agency Roadmap in partnership with other relevant players in the government. The process should include the appointment of a (U.S.) Mission Manager[1] to drive the realization and coordination for this initiative throughout the development process.

Research and Development

Key Finding: Progress in building greater cooperation and transparency will require trusted technical support systems that do not currently exist.

Recommendation: DOE/NNSA/NA-20 should pursue an international research and development (R&D) program in automated monitoring and reporting systems supported by information barriers and authentication to enable more effective and extensive materials monitoring. Trusted information barriers, capabilities for real-time process monitoring and in-field inspection and analysis capabilities should be developed.

DoD/Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs (ASD(NCB)), DTRA, and DOE/NNSA/NA-10 should partner to develop cooperative options for asymmetric nuclear weapons security paradigms; e.g.,

[1] See Chapter 5 for a more complete discussion on the Mission Manager role.

- Sharable technical security principles, practices, and technologies for sites, materials, and components
- Site declaration and portal monitoring
- "Assurance Volume" concepts

U.S Modernization Programs

Key Finding: DoD and DOE are starting to invest heavily in nuclear offense force and facility modernization. The Task Force found only limited consideration being given to more intrusive inspection regimes expected in future treaties and agreements, as part of the new design activities in each Department.

Recommendation: State/AVC, DOE/NNSA, and DoD/Acquisition, Technology, and Logistics (AT&L) should review current U.S. facility and weapon system modernization programs and instruct program managers, if necessary, to plan for accommodation of greater transparency measures. Methods for red teaming and performing vulnerability assessments should be developed and exercised routinely, for both existing and planned facilities, systems, and operations.

Unilateral Measures: Key Findings and Recommendations

Principal Finding: The guiding principle for monitoring to detect undesirable nuclear activity should be detection of activities as early in the planning and acquisition of a capability as possible in order to provide the greatest number of options for slowing or reversing the effort. New intelligence, surveillance, and reconnaissance (ISR) technologies, demonstrated in recent conflicts, offer significant promise for monitoring undesirable nuclear activity throughout the world. The nature of these technologies in the context of the monitoring challenge, however, is that the technologies are most effective when applied in an integrated architecture.

Recommendations: The IC (led by the National Counterproliferation Center [NCPC]), DOE/NNSA, DoD/DTRA and Department of Homeland Security (DHS)/Domestic Nuclear Detection Office (DNDO), should develop a joint roadmap, supported by the necessary systems analysis and engineering capabilities[2], to implement an integrated, more comprehensive and responsive monitoring architecture for nuclear weapons activities worldwide, expanding upon the more general, but static approaches currently employed. The roadmap should make clear the lead and support roles for all involved. As the legislated interagency lead for the Global Nuclear Detection Architecture (GNDA), DNDO should incorporate this more expansive monitoring architecture into the GNDA. The monitoring architecture should be structured to:

[2] See next section "Address the Problem Whole."

- Create "corridors of observation" in multiple domains (geographic, commercial, individuals, financial…) based on open source and available multi-intelligence (INT) information;
- Establish "patterns of life" within corridors that are suspicious;
- Focus persistent monitoring assets on individuals and activities of greatest concern that emerge from patterns of life analyses;
- Assemble and analyze data from all sources to support verification or identify previously unknown concerns;
- Use results of analyses to iterate—i.e., to provide ever more focus for intelligence taskings, as well as provide guidance for needed improvements in technical and operational capabilities.

National Security Staff (NSS) should request that DoD integrate the architectural elements into a global awareness system that:

- Builds on lessons and experiences of successful national security capabilities, such as the Counter IED Operations Center (COIC), NSA's counter-terrorism capabilities, NCPC's counterproliferation efforts, and on DOE's Proliferation Risk Analysis Program;
- Builds also upon the lessons and experience of the IC's Treaty Monitoring Manager3, which at the height of arms control monitoring in the late '80s and early '90s, proved to be an effective vehicle for coordinating the work of multiple organizations and collection activities;
- Uses the Monitoring and Verification (M&V) National Testing Capability (described and recommended in Chapter 6) as the key operational assessment vehicle to test a range of scenarios.

The IC should recast DOE/IN's historic "nth country" analytical capabilities into an "nth group" effort, adapted to the wider range of actors and designs accompanying both vertical and horizontal proliferation.

- The "nth group" program should serve as a community asset for helping to characterize proliferation pathways from available data and advancing technology, and posit pathways to guide collection priorities.

Address the Problem "Whole": Key Findings and Recommendations

Principal Findings: Experienced professionals in M&V have declined in number, but those engaged still tend to address the problem as an extension of approaches used in past treaties

[3] The responsibilities of the Treaty Monitoring Manger are discussed more fully in the context of proliferation monitoring in Chapter 5.

and agreements. As further agreements drive both the U.S. and other signatories to smaller numbers of weapons, the price for inaccuracies increases. The monitoring challenge is further complicated by the many dimensions of proliferation discussed above.

A more robust approach is needed, one that is derived from common community characterization of the problem in its full breadth, depth, and extent; i.e., a systems approach. In addition, there is a need to re-grow a knowledgeable workforce, especially systems analysts to support threat assessment, trade-off analyses, and investment prioritization. Historic contributors such as the DOE national laboratories remain critical to addressing the nonproliferation problem. However, the Task Force believes that the responsible agencies would benefit from enlisting a wider array of performers (other labs, contractors, academia) to address the full complexity of this problem space that calls for new, as well as improved, tools.

Recommendations: As the lead agencies, State/AVC, ASD(NCB), NNSA and NCPC should create the processes and oversee the following steps:

- Establish a "White Team" whose charter is to characterize the comprehensive Monitoring and Verification Framework, relating threat events and actions to monitoring requirements, both cooperative and unilateral.
    - The White Team should be assigned to a "home" agency, but supported and governed by an interagency "board" whose members have sufficient authority to influence any needed changes in strategy and program directions at their home agencies.
- Ensure a common understanding among agency leads for addressing all aspects of the framework, including policy, diplomacy, operations, and research, development, test & evaluation (RDT&E).
    - It is critical that those agencies involved in implementing M&V capabilities maintain a high degree of unanimity on how M&V problems and challenges are characterized, and how they will be addressed in order for the White Team to be both effective and sustainable. The adoption of common frameworks (such as that proposed in this report) can contribute to developing a common understanding of national strategy, goals, and pathways for accomplishing those goals.

The foundation established with the two steps above leads to the following implementation steps, again under the charge of the leading agencies:

- Adapt or create integrated implementation plans. No single agency has purview over the totality of the responsibilities in the M&V mission, but integration "across the seams" is required.

  - The NSS, with support from the Office of Science & Technology Policy (OSTP), should assess progress annually.
- Establish an institutionalized interagency planning process that evolves with the threat.
  - The nature of the M&V problem and solution spaces has changed considerably over the past decades. Undoubtedly, the challenges and proposed solutions will continue to evolve in the coming years. Therefore, not only must the analytical framework used by the White Team evolve, but the plans and priorities across the government must evolve as well.
- Enlist a wide range of contributors.

Improve the Tools: Key Findings and Recommendations

Improving Access

Principal Finding: Improving access is essential for making progress against the low and/or obscured signal of incipient proliferators.

Recommendation: The responsible agencies in the IC and DoD should rebalance existing investments and/or grow new programs in R&D to develop improved approaches for obtaining access across an array of scenarios and environments.

Expanded Sensing and Assessment

Principal Findings: The advances in persistent surveillance, automated tracking, rapid analyses of large and multi-source data sets, and open source analyses to support conventional warfighting and counterterrorism have not yet been exploited by the nuclear monitoring community. Conversely, developers of these capabilities are largely unaware of the challenges and requirements for nuclear activity monitoring.

Radiation detection remains important for monitoring and verifying sources of special nuclear material (SNM) when access allows inherent range and background limitations to be overcome. The technical communities involved have had a mixed track record of fielding new capabilities in spite of coordinated and sustained investments in R&D. The problem appears to lie in the gap between researchers and operators, who do not come together early enough in the development process to ensure that both technical and operational requirements are addressed.

Two specialized capabilities critical to monitoring require support to enable the monitoring architecture proposed in this report:

- The Open Source Center (OSC), which is proving to be a particularly effective organization in helping to identify the “corridors of interest”, but has limited resources to devote to routine monitoring of other groups or nations.

- The U.S. Atomic Energy Detection System (USAEDS, operated by the Air Force Technical Applications Center), which remains a stepchild within the Air Force (AF) and is in serious need of modernization.

Recommendations: There are numerous aspects that deserve attention from each or all of the several agencies with mission responsibilities for nuclear monitoring, as follows:

- The Director of National Intelligence (DNI) should provide direction to the leading agencies in the IC to:
    - Increase the profile, support, and integration for the OSC's Counterproliferation (CP) Program to collect and disseminate information and analysis relevant to arms control and proliferation issues;
    - Assess/adapt new and expanded collection capabilities for nuclear monitoring, especially through multi-INT integration and enhanced processing;
    - Expand the use of open source and commercial information to focus search areas and reduce demand on national collection assets so that the collection system can keep up better with the expansion of targeted areas of interest;
        - Continue/expand the augmentation of data from national intelligence collection systems with imagery and radar from commercial systems;
        - Develop and apply quality assurance methods for crowd sourcing of commercial imagery results;
    - Ensure that DoD's activities for improving global indications and warning leverage existing sources of information and capabilities, and develop the analytics to produce actionable nuclear-related threat warnings;
    - Adapt the Treaty Monitoring Manager's role to one of a Proliferation Monitoring Manager, "home based" in NCPC, with orchestration and integration responsibilities to assess both horizontal and vertical proliferation.
- DOE/NNSA, DHS/DNDO, DoD/DTRA and the IC should build upon the existing memorandum of understanding (MOU) among these organizations to improve coordination and execution of their respective radiation detection programs to:
    - Conduct systems studies and engage operators early in development to improve transition of radiation detection advances to the field;
    - Ensure that developers and users agree in advance on system concepts, measures of success and levels of readiness for the principal technologies and operational scenarios of interest;
    - Focus new efforts on accelerating development of research with near-term payoffs, and investment in longer range technologies that can meet both technical <u>and</u> operational feasibility requirements;
    - Develop managed access to nuclear facilities and test ranges by all involved agencies at which detection technologies and operational approaches can be explored using real SNM;

  - Agree on investment strategies. There should be supporting inter-agency roadmaps to integrate efforts and focus crosstalk. Annual inter-agency reports to the NSS should be issued to track progress and enhance information flow.[4]
- DOE/NNSA, DTRA, and the IC should rebalance existing investments in order to grow new programs in R&D that expand activities and the supplier base to include adaptation of conventional warfighting ISR advances: e.g.,
  - Engage in planning and capabilities development, especially for data collection and fusion functions, for DoD's efforts to improve nuclear situational awareness;
  - Support transition of multi-INT fusion and exploitation tools to nuclear monitoring applications;
  - Ensure activities related to nuclear weapons and materials monitoring are guided by the "white team" function as discussed in the previous section and Chapter 4;
  - Make explicit the requirements for, and improvements needed in, HUMINT, SIGINT, cyber, OSINT, etc., to support monitoring and verification.
- NSS should monitor closely and persistently the resourcing to modernize the USAEDS with the help of the Vice Chairman of the Joint Chiefs of Staff (VCJCS), who should ensure its modernization, is supported in AF budgets.

Test to Iterate and Adapt: Key Findings and Recommendations

Findings: The comprehensive monitoring regime the Task Force proposes is a system of systems that must work together. It is too complicated to plan or assess analytically or with piecemeal testing, especially when used against an adaptive adversary and/or one with sophisticated denial and deception. Furthermore, experience shows that operators typically learn to use fielded systems differently and often better than system design/analysis would predict—an effect that would result from into iterative development and training.

Recommendations: DTRA, in partnership with DOE/NNSA and the IC, should develop comprehensive "iterate and adapt" national testing capabilities which:

- Provide a focal point for planning, iterating/adapting, and operating the system of systems;
- Help integrate technically disparate and organizationally disaggregated activities.

The national testing capabilities should include four interdependent parts:

- Ranges and facilities (real and simulated), almost all of which currently exist;

[4] An excellent recent example of this is the "Nuclear Defense Research and Development Roadmap. Fiscal Years 2013-2017" published by the National Science and Technology Council, April 2012.

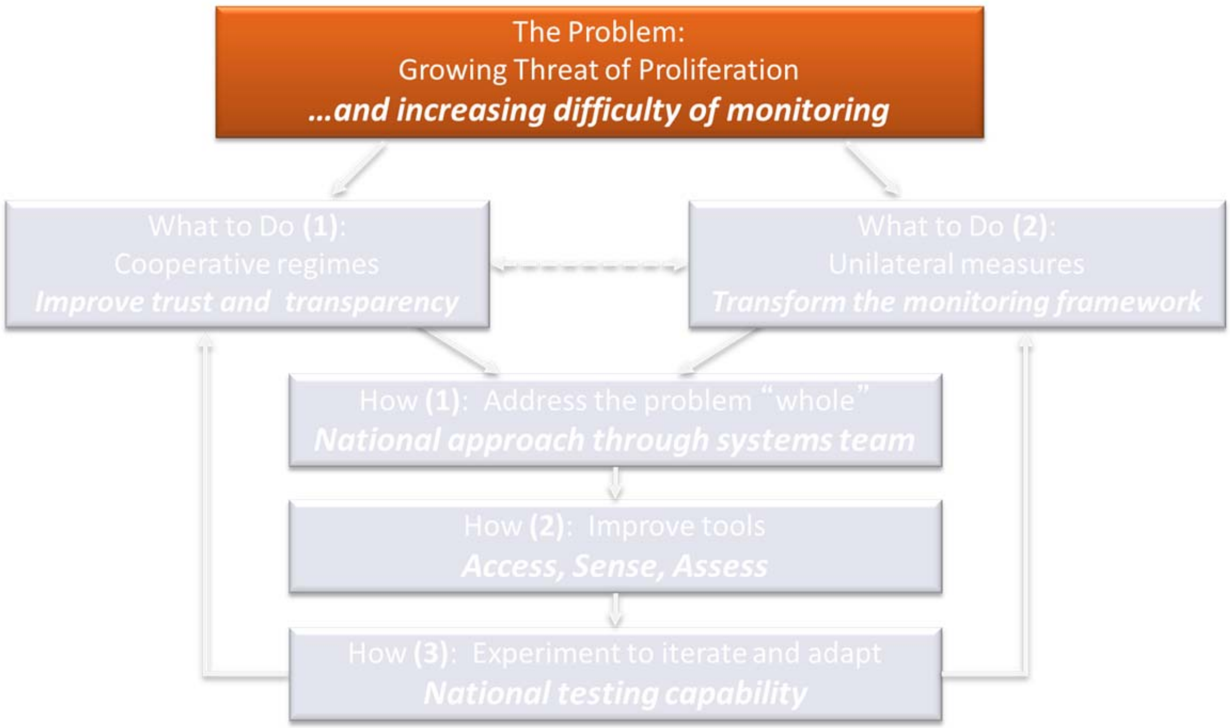
- Information/data management systems (e.g. data flows from and to sensors, information flows within analysis/fusion systems, and command/control data/information flows);
- A standing/ongoing Red Teaming activity;
- A White Team—a strong analytical component to assess the implications of test results and feedback into the cycle needed changes/improvements.

Support from the IC (principally NCPC and DOE) should be provided for the purpose of rebuilding a national nuclear threat technical assessment capability that anticipates "nth group" designs, effects, employment and deployment approaches and observables (per one of the recommendations for "Unilateral Measures").

Summary

The problem of managing the global nuclear environment to maintain stability will be with us for a very long time. The best bet for making progress is a sustained effort in which experience, competence, and relationships can be built over successive careers. The challenges are daunting and success will be difficult to come by, but prior experience tells us that persistence can lead to the outcomes we seek.

Chapter 1. The Problem – Growing Threat of Proliferation and Increasing Difficulty of Monitoring



1.1. Monitoring vs. Verification

The Terms of Reference—indeed the very name of the study—refer to monitoring and verification technologies. The Task Force focused, however, only on capabilities for monitoring because verification, traditionally and in the view of the Task Force, is principally the political judgment to which monitoring and other means contribute. Verification is also most often used in the context of adherence to, or violations of, treaties and/or formal or informal agreements. Monitoring, however, can and should be more broadly applied because of the nuclear future envisioned by the Task Force. In fact, monitoring for proliferation should be a top national security objective – and one that the nation is not yet organized or fully equipped to address.

1.2. The Nuclear Future – Not an Extrapolation of the Past

Too many factors have changed, and are changing, from our historic basis and experience in the Cold War, in a manner that should give national leadership pause for concern. The list starts with the fact that fundamental nuclear knowledge is much more widespread. Ubiquitous information access and widespread observational tools are increasing inherent transparency. At the same time, recognition of such increased transparency by potential or actual proliferants naturally leads to more sophisticated methods of denial and deception.

The actual or threatened acquisition of nuclear weapons by more actors, for a range of different reasons, is emerging in numbers not seen since the first two decades of the Cold War. Many of these actors are hostile to the U.S. and its allies, and they do not appear to be bound by established norms nor deterred by traditional means. In some cases of established nuclear powers, nuclear forces are seen as the most affordable and effective alternative to deter superior conventional forces; i.e., nuclear weapons are viewed as a legitimate warfighting capability, especially if their vital domestic or regional security interests are threatened. For example, Russia has publicly stated in doctrine and backed it up with training and exercises that they will use theater nuclear forces if necessary to deter aggression against the homeland.[5,6,7,8,9]

The pathways to proliferation are expanding. Networks of cooperation among countries that would otherwise have little reason to do so, such as the A.Q. Khan network or the Syria-North Korea and Iran-North Korea collaborations, cannot be considered as isolated events. Moreover, the growth in nuclear power worldwide offers more opportunity for "leakage" and/or hiding small programs, especially since current resources to support safeguards are already strained and will be increasingly challenged by cases of noncompliance.

In short, for the first time since the early decades of the nuclear era, the nation needs to be equally concerned about both "vertical" proliferation (the increase in capabilities of existing nuclear states) and "horizontal" proliferation (an increase in the number of states and non-state actors possessing or attempting to possess nuclear weapons).

The challenges for monitoring in this context are much more difficult. Historically, and even with New START, monitoring has focused on relatively few nations (only two in treaties with Russia) and locations. Moreover, the objects to be monitored have been numerous and easily identifiable (e.g., delivery platforms such as bombers, missiles, and submarines), the facilities supporting the enterprise visible and often declared, and nuclear materials inventories voluntarily declared.

---

[5] Nikolai Sokov, Russia's New National Security Concept: The Nuclear Angle, Center for Nonproliferation Studies Report, January 2000.
[6] Statement by Sergey Ivanov, available at http://www.mil.ru/articles/article3667.shtml
[7] Vladimir Putin, "Zakluychitelnoe Slovo na Soveshchanii s Rukovodyashim Sostovom Vooruzhennykh Sil Rossii", October 2, 2003 (available at htpp://www.president.kremlin.ru/text/appears/2003/10/53277.shtml).
[8] Yuriy Golotuyk, "I v Vozdukhe Tozhe Problemy" Vremya novostey, February 19, 2001.
[9] "Strategicheskaya Komandno-Shtabnaya Treniroivka VS Rossii", Nezavisimaya gazeta, February 17, 2001.

In the nuclear future as seen by the Task Force, monitoring will need to address more widespread foreign nuclear weapons related activities in a "messy" combination of negotiated, non-cooperative, and non-permissive environments. Any or all of the following could be factors in monitoring a particular nation or group of concern:

- Small inventories of weapons and materials, even as low as a single "significant quantity of fissile material;"
- Small nuclear enterprises designed to produce, store, and deploy only a small number of weapons – either as an end goal, or as the first steps of a proliferant, or a nuclear terrorist operation;
- Undeclared facilities and/or covert operations such as testing below detection thresholds;
- Use of non-traditional technologies, presenting at best ambiguous signatures, to acquire both materials and components;
- Theater nuclear forces and associated doctrine, exercises, and training complicated by the use of mobile, dual use delivery systems;
- Many more players to whom access by the U.S. or its allies will be limited or extremely difficult, some of whom will be globally networked with global access to relevant science and technology.

The stress on monitoring technologies is significant. Identifying and maintaining track on people, nuclear components and warheads now becomes a requirement, and in many cases, physical access will be limited. Moreover, the broad access to technology and the growing sophistication of cyber offenses by "them" as well as us will allow others to gain insights into our collection capabilities and methods. The challenges are further compounded by the many dimensions of the nuclear enterprise that need to be monitored, as illustrated in

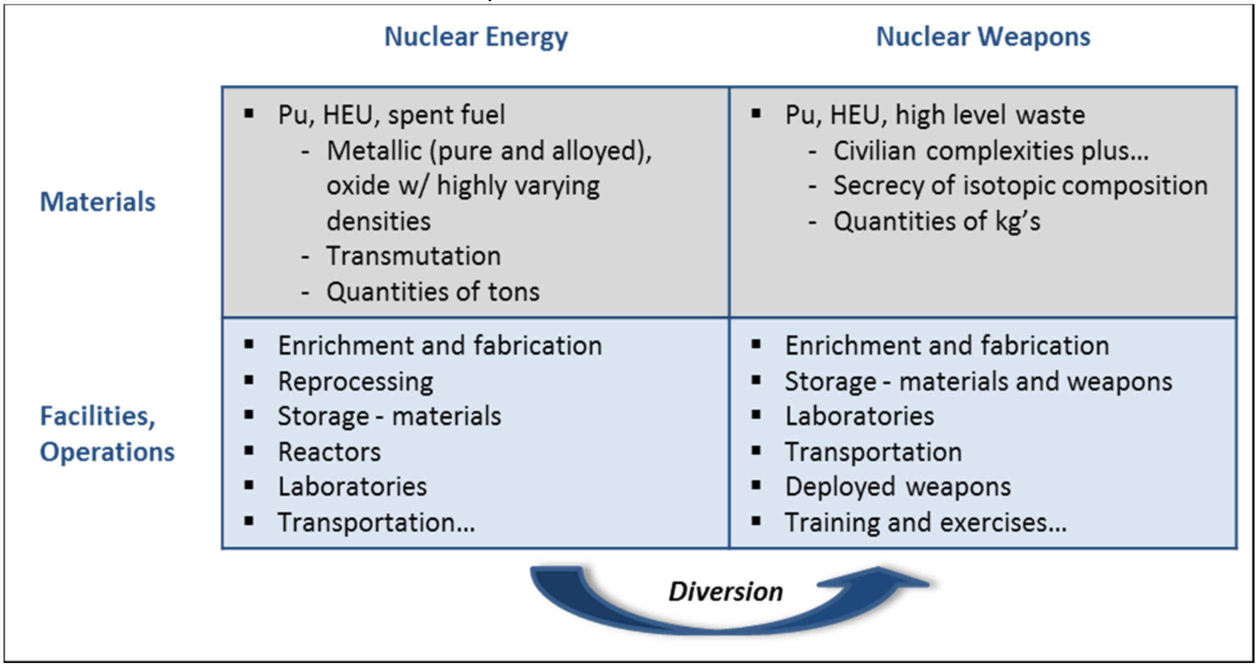


Figure 1-1.

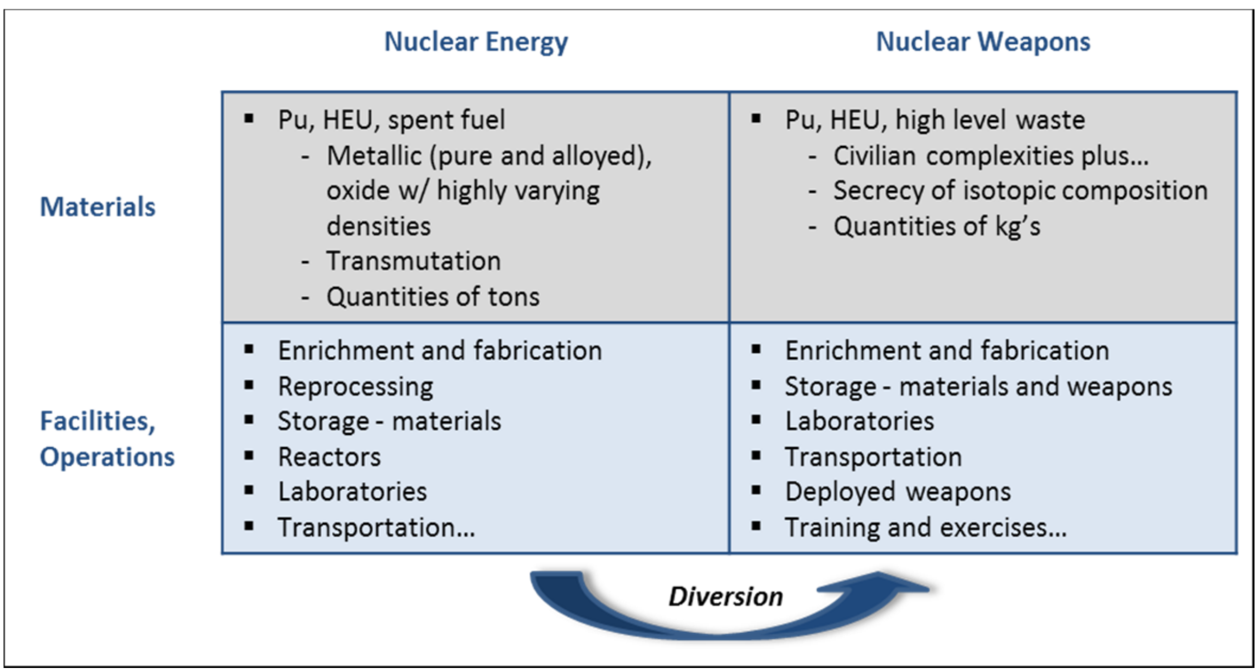


Figure 1-1 Challenges are Further Compounded by What Needs to be Monitored

The materials themselves in their many chemical forms, the operational configurations to which the materials are applied and associated facilities and infrastructure are all part of the enterprise that should be monitored. Nuclear energy operations, as well as nuclear weapons activities, should be carefully watched because of the potential for diversion of materials from energy to weapons, the ease of hiding low level weaponization activities within nominally civilian facilities, and/or the requirement for much lower quantities of weapons grade vs. reactor grade materials to obtain an operational weapons capability.

1.3. A Need for Comprehensive Monitoring

Given the potential reality of, and subsequent risks associated with, the nuclear future described above, the Task Force believes that the nation must "address the proliferation problem whole" because the global nuclear regime is itself an integral whole. Civil nuclear applications are a global enterprise, and military nuclear applications are increasingly networked. Military and civilian applications are connected, in part through the global nuclear science and technology (S&T) base. Actual or latent proliferation by one nation stimulates proliferation activities by others, especially neighbors.

In order to understand any one part of such a global interconnected enterprise (for example, to negotiate and/or monitor a particular treaty, or understand the threat posed by a nation that has proliferated), it is necessary to understand the whole. Understanding the whole entails monitoring the whole, and not all of that monitoring can be carried out through methods negotiated in treaties, at least not until the global treaty regime has become much more comprehensive. Negotiated monitoring for a particular treaty will have to be complemented by non-negotiated, "general purpose" monitoring, including unilateral monitoring. The Task Force acknowledges that such a relationship between negotiated and non-negotiated monitoring has been important in the past, but it will be even more important in the future. Moreover, the details (e.g., geography, access, suspected stage of proliferation, etc.) of where, and to what extent, each are applied will be important; one size will not fit all.

Figure 1-2 illustrates the point. Not only does the figure highlight the expanded and multi-dimensional nature of the proliferation monitoring problem, but it also introduces the opportunities for *synergy* among different types of monitoring for different purposes.

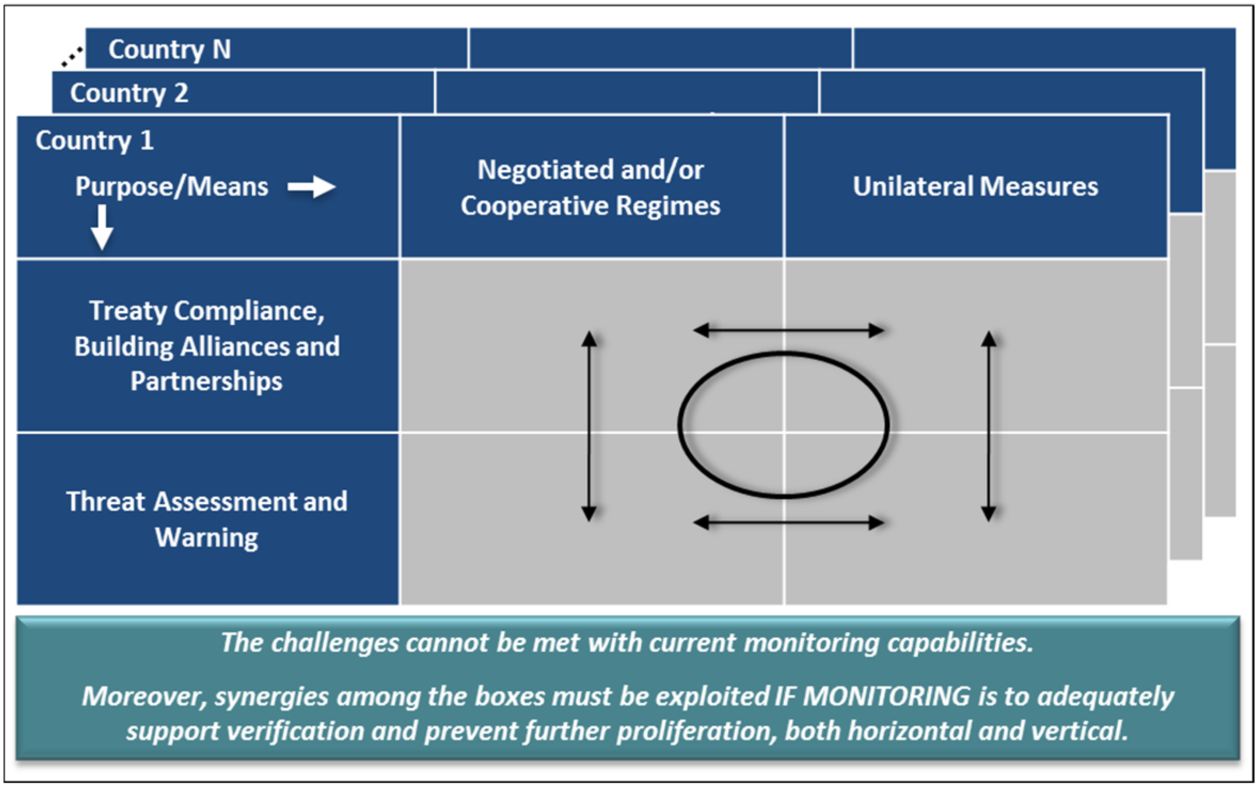


Figure 1-2 Scope – and Opportunities – of Future Monitoring Regimes

Managed as a whole, synergies can be developed in both the horizontal and vertical dimensions of the purpose vs. means matrix. Horizontally, for example, non-compliance with the provisions of a treaty might involve hiding assets or undertaking covert operations that non-negotiated/unilateral monitoring can uncover. Challenge inspections negotiated in a treaty can be triggered by non-negotiated monitoring data. Similarly, "general-purpose" monitoring for threat assessment (lower right) can be complemented by understanding treaty-limited items or behaviors learned through negotiated monitoring (lower left).

Vertically in Figure 1-2, an overall assessment of threats of proliferation or threats by proliferators constitutes the context in which future treaties should be proposed and negotiated. Conversely, observed non-compliance with a treaty can serve as a form of strategic warning in the threat assessment sense. As a more particular example, monitoring for "patterns of life" of nuclear operations in a particular nation (lower right) can indicate or reveal the presence of evasive/covert operations intended for non-compliance with treaties (upper right, moving to upper left).

Figure 1-2 also illustrates a separate monitoring approach for each of several nations to indicate, as discussed above, that nuclear activities can be both unique to each and increasingly networked. While complicating the overall challenge, this characteristic introduces more opportunities for synergies by integrating monitoring across several/all nations.[10]

1.4. Beyond Incremental Improvements…A Paradigm Shift

Because of the increasing challenges of controlling, limiting, and stabilizing the global nuclear regime and the increasing difficulty of monitoring it, the Task Force believes that efforts beyond incremental improvements of traditional approaches to monitoring will be required. Monitoring cannot continue to derive only from treaty and agreement dictates for "point" compliance to the numbers and types formally agreed upon and geographically bounded. Proliferation should become a continuous process for which persistent surveillance tailored to the environment of concern is needed. This leads to the need for a paradigm shift in which the boundaries are blurred between monitoring for compliance and monitoring for proliferation, between cooperative and unilateral measures. Monitoring will need to be continuous, adaptive, and continuously tested for its effectiveness against an array of differing, creative and adaptive proliferators.

The Task Force envisions a five-part framework, illustrated in Figure 1-3.

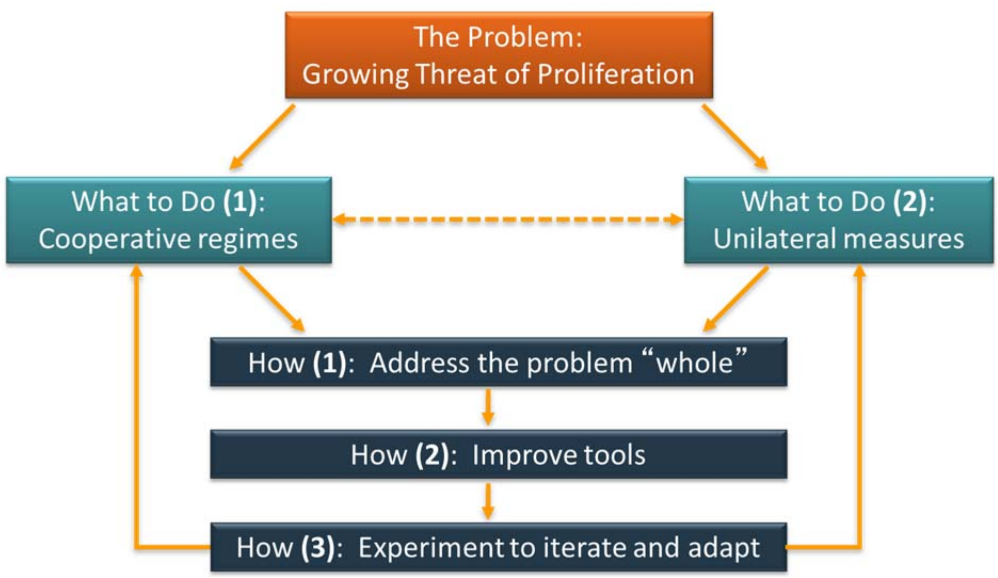


Figure 1-3 Meeting the Future Monitoring Challenge: Two "Whats" and Three "Hows"

Figure 1-3 highlights that it will be essential to expand the scope of monitoring by achieving greater international cooperation and transparency, and by developing and employing new U.S. monitoring architectures. Both will require that the monitoring problem be approached

[10] These kinds of connections and synergies in monitoring are developed in more detail for the case of monitoring of Theater Nuclear Forces (TNF) and dual capable (DC) systems later in the report [Chapter 6, section 6.2.5].

systematically and "whole;" improved through technical tools that enable access, sensing, and assessment; and continuously tested against evolving and adaptive proliferant strategies and techniques.

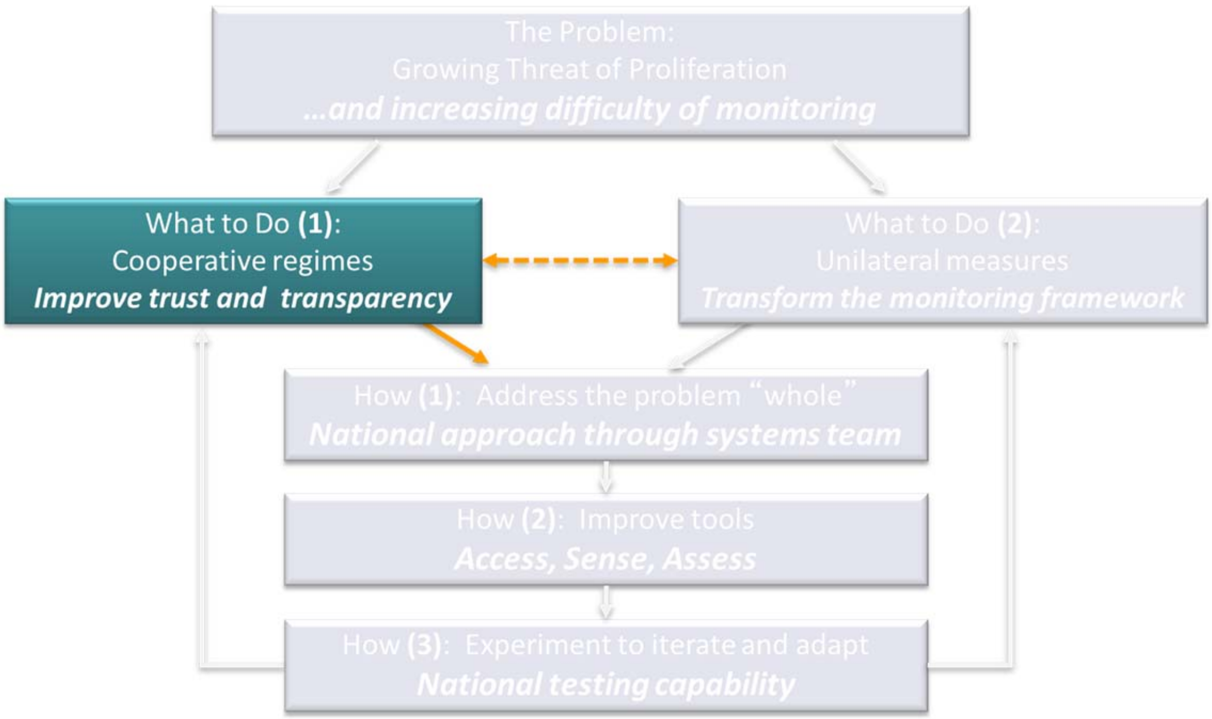
To achieve these goals, a major diplomatic effort to build trust and confidence will be required. Investments will also be needed to develop and field capabilities beyond the traditional emphases in treaty-monitoring technologies. Two key examples illustrate the point. First, the powerful tactical ISR developed for Iraq and Afghanistan – for example, for suppressing the improvised explosive device (IED) threat – should be adapted and extended for nuclear monitoring, especially where access is limited or denied. Such capabilities could also be negotiated for use in challenge inspections. Second, the "big data" technologies for extracting meaning from vast quantities of data that are being developed commercially in the information technology (IT) industry, and for other purposes in DoD and the IC, need to be extended and applied to nuclear monitoring.[11]

Nations seeking to proliferate and/or to evade the provisions of treaties (as well as non-nation state adversaries with nuclear ambitions) will be adaptive in hiding or obscuring what they are doing. Staying ahead of their adaptation must be an integral and deliberate part of U.S. efforts to develop and implement a comprehensive nuclear monitoring regime. A key element of staying ahead is continuously challenging our own assumptions. The Task Force believes this could best be accomplished through testing and experimentation in which monitoring capabilities would be challenged by red-teaming, with the red/blue interactions analyzed and refereed by a "white team." In this way, we can "try before we buy", and account for others' use of technology to thwart our own.[12]

In summary, the challenges of controlling and stabilizing the nuclear future, and the difficulty of monitoring global nuclear activities in that future, mean that the nation must plan for a long period of building both the political and technical groundwork for the next major steps in formal treaties or agreements, as well as for addressing proliferation more broadly where cooperation is unlikely for the foreseeable future. To drive the point home, the Task Force adopted the motto: "We can't let our treaties get ahead of our monitoring and verification headlights."

[11] These approaches are discussed in more detail in Chapter 3, section 3.4, and Chapter 5.
[12] The national testing capability is discussed in some detail in Chapter 6, sections 6.2 and 6.3.

Chapter 2. Cooperative Regimes: Improving Trust and Transparency



2.1. Introduction

There are many trends already at work toward openness and transparency in technology and in global institutions in general, in spite of resistance to and/or attempts to limit them in selected quarters. International trade and transportation, multinational corporations, international contract law, treaties intended to manage resources in the global commons, the Internet and the growing ubiquity of communications and information access are all cases in point. Each of these domains has largely developed its norms, standards, and/or policies independently and according to its own needs.

The increase in openness and transparency in this wide range of domains provides a foundation to build upon, extend, and integrate to raise the levels of trust among participants—most especially for monitoring proliferation related activities. However, because nuclear weapons are so central in security relations among nations, achieving higher levels of transparency and access needed for effective monitoring will require a comprehensive, sustained, policy-based diplomatic approach coordinated across the U.S. Government (USG) and with other nations, devoted expressly to advance the cause of openness and transparency writ large. While the U.S. has recognized the value of, and need for, such an approach almost since the development of nuclear weapons, it has had, at best, a mixed record of success in sustaining national efforts. This situation should be addressed with the highest priority, and the Task Force provides in this chapter one approach for how to do so.

2.2. A Well Established Starting Point: The Nonproliferation Treaty and Its Limitations

A baseline of nuclear transparency has been established with the Treaty on the Non-Proliferation of Nuclear Weapons (NPT).[13] However, the NPT regime remains under significant pressure—both from the expansion of nuclear power with the associated monitoring demands, and the continued intransigence of states violating their safeguard obligations.

In order to diversify their energy portfolios and meet growing demands for electricity, new states are venturing into civilian nuclear power. Most, if not all, of this expansion will be benign, but the dual-use nature of nuclear technology, at least with regard to SNM production, raises a number of concerns. Some of this growth will occur in areas of instability and/or regional tension. The recent events of the “Arab Spring” illustrate the potential for political volatility and range of possible outcomes.

Sensitive nuclear technologies, particularly those used in enrichment and reprocessing facilities, present unique monitoring and verification challenges. There are inherent difficulties monitoring complex, industrial size bulk handling facilities and processes. Expansion of nuclear power risks the illicit spread of these capabilities. The Kahn network illustrated the difficulties of controlling key technologies in a globalized and increasingly sophisticated manufacturing base. Collusion amongst proliferators enables states to bypass technological hurdles, serving to further complicate nonproliferation efforts.

In spite of these complexities, it is still decidedly easier to monitor declared material and facilities as the NPT (further enabled more recently by the Additional Protocol) has enabled for 40+ years, so that expanding the fraction of nuclear activities under “routine” inspection is desirable. Cooperative monitoring regimes provide a baseline of information while defining legitimate nuclear behavior. In recent years, linking nuclear security with Safeguards is providing a basis for engagement and cooperation between states to promote high standards for material protection, control and accounting. Cooperative monitoring also allows focusing of

[13] The NPT is a landmark international treaty whose objective is to prevent the spread of nuclear weapons and weapons technology, to promote cooperation in the peaceful uses of nuclear energy and to further the goal of achieving nuclear disarmament and general and complete disarmament. The Treaty represents the only binding commitment in a multilateral treaty to the goal of disarmament by the nuclear-weapon States. Opened for signature in 1968, the Treaty entered into force in 1970. On 11 May 1995, the Treaty was extended indefinitely. A total of 190 parties have joined the Treaty, including the five declared (at that time) nuclear-weapon States. More countries have ratified the NPT than any other arms limitation and disarmament agreement, a testament to the Treaty's significance. (Ref.: http://www.un.org/disarmament/WMD/Nuclear/NPT.shtml)

resources on "rest of world" coverage if/when concerns arise. International or multilateral verification activities provide independent data to support intervention efforts in cases of noncompliance.

The Safeguards system of the IAEA will need added resources and technical advances to deal with the effects of a global nuclear energy expansion to ensure a robust detection capability for any misuse. Should future arms reductions or other regimes or initiatives, such as Global Nuclear Lockdown and/or a Fissile Material Cutoff Treaty, require the IAEA to monitor a much more extensive set of facilities and/or materials, the existing Safeguards regime will have to shoulder an increase in the demand for strong but efficient monitoring and verification capabilities. Providing confidence that treaty obligations are being fulfilled while protecting sensitive information is a technical challenge common to both warhead verification and safeguards at commercial facilities, and one for which there are not yet widely accepted solutions.

2.3. Experience in Cooperation Outside the NPT: The Cooperative Threat Reduction Program

The CTR program was begun in 1993 in order to assist the Russians and the republics of the former Soviet Union to reduce the threat of a nuclear weapon accident or loss and meet their commitments to the original Strategic Arms Reduction Treaty (START). Also known as the Nunn-Lugar program,[14] the CTR program permitted the Ukraine, Belorussia and Kazakhstan to fulfill agreements to return their nuclear weapons to Russia and become nuclear weapons free states, reducing by three the number of governments that possessed operational nuclear weapons.

The program also enabled Russia to meet its commitments to START. The United States, by partnering with the Russian Defense Ministry to destroy missiles, bombers and submarines, helped ensure that the Russians reduced the numbers of delivery vehicles agreed to under the START Treaty. The CTR program also built facilities and provided security systems to store nuclear materials and secure operational nuclear weapons.[15] Funding was also provided to support Russian nuclear scientists with technical work in order to mitigate the concern that they might otherwise sell their expertise to other nations who are intent on building their own nuclear weapons capability. Participants on both sides agree that greater transparency and

[14] Then Senator Sam Nunn and Senator Richard Lugar initiated the program at the request of Secretary William Perry and Assistant Secretary of Defense Ashton Carter. Both Nunn and Lugar have remained active participants in the program over the years, visiting CTR sites in the former Soviet Union and guiding and encouraging aggressive conduct of CTR activities. They have also been instrumental in solving intergovernmental problems that otherwise would have delayed progress on the program.

[15] In addition, the CTR program assisted the Russians in making a best effort to meet its obligations under the Chemical Weapons Convention. The United States assisted the Russians in building chemical demilitarization facilities that destroyed thousands of chemical weapons. It has been expanded in recent years to secure biological agents of concern, as well as expand disease monitoring capabilities in selected international regions.

stability were achieved between the United States and Russia through the execution of the Nunn-Lugar program.

2.4. Toward an International Cooperation and Transparency Regime

Currently the IAEA monitors all declared stocks of SNM in states that are signatories to the NPT and occasionally SNM offered up as excess material in weapon states. The bilateral Safeguards agreements that provide the legal basis for safeguards implementation, require that the information collected be considered sensitive and not be shared with other states.[16] Extending protocols to include the monitoring of nuclear weapons and weapon components worldwide coupled to sharing of the information with all international parties who have agreed to cooperate should be the ultimate goal. In order to get to that point, a long period of trust building through a number of intermediate steps will be required. The Task Force examined the experience base to understand how to get started in such a process and then developed a proposal for a phased approach.

The Task Force started with an examination of the recent history of proposals and negotiations for how best to obtain mutual agreements on M&V technologies in the future. One of the best historic examples was the Cooperative Safe, Secure Dismantlement (SSD) talks of 1991-1994 (bilateral discussions between the United States and the Russian Federation). The talks had made significant progress towards a joint agreement for radiation detection equipment that could be used to establish the fact that an object presented for dismantlement was in fact a nuclear warhead.

Although these talks were terminated without a formal agreement being consummated, there were enthusiastic beliefs on both sides that they had "come close" to developing radiation detectors and related instruments and procedures that could adequately determine the amounts of SNM [either Highly-Enriched Uranium (HEU) or Plutonium (Pu)] with sufficient accuracy to establish that there were indeed weapon-like quantities present. The remaining barrier to be overcome was to ensure that sensitive information (such as specific design details of the devices presented) could not be transferred.

The approach being pursued during the SSD talks focused on the use of potential "Information Barriers," such as templates provided by the inspected party on CDs or magnetic disks at the point of inspection, which would then be used to convert the measured data into kilogram amounts of SNM, but which would not reveal geometric internal details of the device. That approach still had some difficulties prior to its being accepted, but there were serious efforts

[16] The IAEA does publish the plutonium holdings of nine countries, the five declared weapons states as well as Japan, Germany, Belgium and Switzerland. This information is provided on a voluntary basis by the participants consistent with the "Guidelines for the Management of Plutonium" (INFCIRC/549). Such declarations might be a useful starting point upon which to build a more comprehensive transparency regime.

being expended by both the United States and Russian participants to find acceptable solutions. Methods such as this one could be the first step to multilateral cooperation that could include non-nuclear weapons states.

Over the past decade, programs such as the United States-Russia Warhead Safety and Security Exchange (WSSX), and the United States-Russia-IAEA Tri-lateral Initiative have explored transparency methods and ways to protect sensitive information.

In a recent exchange meeting on this topic in January of 2011 between scientists of the Russian and United States National Academies, both sides expressed strong interest in finding ways to complete the search for mutual agreement on measurement devices that could overcome the difficulties listed above, convinced that these will be essential for verification of future nuclear agreements. Efforts are currently underway to pursue a United States-Russian agreement to allow such cooperative work to be reinvigorated. In addition, there was a meeting of United States and Russian nuclear weapons lab directors late in 2012, and both sides spoke favorably of finding a way to renew cooperative work, that was lost when the Lab-to-Lab efforts fell off during the Russian/Commonwealth of Independent States (CIS) reorganization.

During its deliberations, the Task Force learned there has been additional U.S. thinking and work that would utilize film recording, rather than direct counting apparatus. There are strong beliefs that the needed systems can be achieved by employing random scanning techniques which could average out geometrical details, while preserving the total assay/inventory of special nuclear material amounts.

The positive experience of these and other examples led members of the Task Force to conceive an overall approach, and to recommend that the U.S. pursue joint development efforts for "**Building Cooperation and Transparency**." The Task Force envisions a multi-year effort, which can pay large dividends in terms of a universal transparency that would improve strategic and tactical stability against nuclear war among all nuclear-weapons states, as well as achieve enhanced confidence building for nonproliferation efforts. We endorse these approaches, and outline some of the details for the proposed phased initiative below.

Realizing that there are no perfect transparency regimes, there are still many advantages that can result when nations can achieve full reciprocity in monitoring both nuclear weapons and nuclear materials that might otherwise be diverted for weapons use. All parties would benefit from the national security stability that would ensue from having transparent knowledge of the numbers/types of other nations' nuclear arsenals, while each nation in turn makes the knowledge of their own SNM and/or nuclear weapons inventories available to the others. The Task Force envisioned that the same techniques could be utilized by inspectors for routine inspections, dismantlement verification, and warhead destruction monitoring.

There are of course essential criteria that must be met before such a regime can be successful. Of primary importance, the security of storage sites and the security of stored weapons or materials should not be undermined or even weakened by the agreed upon inspection processes to be used. Similarly, successful transparency should reveal neither national secrets, such as specific locations of storage sites or security design techniques, nor vulnerabilities within the weapons designs. Achieving acceptance by all parties as to the permissible level of intrusiveness during the inspections, while preserving the effectiveness of the security measures employed by the inspected parties, will require independent agreement and confidence in these factors by all of the parties.

The Task Force fully understands that the task proposed will not be easy nor will it be accomplished soon. However, the Task Force does believe that the times are now propitious to move forward on a path to develop universal transparency regimes that can simultaneously fulfill these goals and requirements through an international process for achieving universal knowledge of nuclear weapon inventories and SNM inventories, and that the U.S. should lead in such an effort. Indeed the U.S. has already declassified the size of its current nuclear arsenal. The Task Force proposal has four phases, each with subparts that involve cooperative development efforts with a multiplicity of other states.

Phase 1. Bilateral Cooperative Developments/Evaluations with P-5 States. The journey should begin with a series of bilateral efforts among the five permanent members of the United Nations Security Council (P-5) nations (United States, Russia, UK, China, France) to jointly develop, evaluate, and improve monitoring equipment and recording methods to demonstrate the capabilities needed for warhead verification. Particular emphasis should be placed on achieving acceptable levels of “non-intrusiveness.” In order to win agreement for use of any approach by all of these parties, it will be important to prove that sensitive information will not be revealed—either directly or through collateral or surreptitious means. The model of the Joint Verification Experiment (JVE) provides an excellent template for how similar bilateral cooperative efforts, which the Task Force envisions here, could proceed. The JVE was carried out cooperatively between the United States and the U.S.S.R. in 1987 and 1988 for the purpose of creating mutually agreed upon methods for both on-site measurements and on-site verification systems in support of the series of bilateral Nuclear Testing Talks.[17]

When successfully demonstrated and accepted by the parties, these monitoring systems could be used for verification of nuclear weapons treaties, for authentication of declared stockpiles, for verification of dismantlement, and ultimately for verification of the destructions of warheads. At some point, the bilateral nature of this phase should move to multilateral cooperation across the P-5.

[17] The 25th Anniversary of the Joint Verification Experiment was commemorated jointly between the U.S. and Russia in the early fall of 2013 at the site of the experiment.

Phase 2. Extending the Development/Evaluations to all Nuclear Weapon States. The P-5 would embark on cooperative, bilateral efforts to demonstrate, adapt, and improve the systems through joint development efforts with all nations that currently possess any nuclear weapons. This would be a very sensitive endeavor, as previously there have been few if any contacts made with these nations (e.g., India, Pakistan) regarding measurements or monitoring of their nuclear weapons. The goal would be the same as for the previous phase: to demonstrate accurate and non-intrusive monitoring in order to win acceptance for use of demonstrated P-5 techniques or variants by all of these states. During this phase there will need to be a premium placed on the flexibility of implementing the monitoring techniques, since there are large variations in security and control measures, technical sophistication, and inspection methodologies. Initiation of this phase need not wait until Phase 1 is completed since this effort will likely require a lengthy period to establish mutual understanding and trust well before technology options or even discussed or tested.

Phase 3. Major Nations that Employ Nuclear Power Generation. The next phase shifts from nuclear weapons transparency to engaging Non-Nuclear Weapons States (NNWS). The particular focus should be on adapting existing international safeguards or new transparency techniques to achieve accurate and sharable determinations of the inventories of separated SNM (or weapons useable materials) in such states as Japan, Belgium, Netherlands, Germany, Canada, Taiwan, Ukraine, Kazakhstan, South Africa, and others who currently have or expect to generate in the future any separated quantities of material. Each nation must also believe that the techniques will be accurate, reciprocal, and non-intrusive in ways that would protect its commercial secrets, and would not compromise the security for storage of any of its materials. The efforts would be cooperative and bi- or (better) multi-lateral.

It is in this phase that the emphasis for Building Global Transparency of Nuclear Materials would become the dominant theme. At present, the IAEA retains the sensitive information as it carries out the verification activities on behalf of the member states. The shift from current protocols and practices under the NPT for such a Global Transparency regime would be making transparency information available as a quid pro quo for providing access to an international inspectorate.

Phase 4. The Evolution from Bi-lateral to Multilateral Implementation and a Prospective Non-Proliferation Treaty (NPT-x). Several studies have concluded that it is premature to pursue negotiation of a follow-on Non-Proliferation Treaty that would impose transparency on States possessing nuclear weapons and NNWS equally and add nuclear weapons disarmament transparency to the treaty. Completion of the three phases presented above, however, could set the stage for overcoming the current difficulties and be the basis for the trust and understanding needed to carry out both the periodic/continual monitoring of nuclear weapons worldwide, and the periodic/continual monitoring of SNM quantities of potential nuclear weapons materials worldwide.

The signatories of nuclear arms control or arms reductions agreements, joined by all of the nuclear weapons-possessing nations, would collectively and mutually negotiate the procedures, frequencies, prohibitions, etc. for carrying out materials and weapons transparency measures/inspections protecting against the spread of nuclear weapons expertise to NNWS. The ideal outcome would be agreement that the results of these inspections would be delivered to the IAEA as part of its routine monitoring and shared with all nations worldwide.
The Task Force believes that progress through Phase 4 will have a positive effect on worldwide arms stability as well as strengthen non-proliferation efforts. With everyone having a stake in the transparency processes coming into existence and successfully working, it might then be possible to require mandatory compliance for any holdout nations. The culmination of all of these efforts would be the achievement of a Cooperative Universal Transparency regime that would operate to ensure monitoring and verification of all nuclear weapons as well as inventories of SNM—over the whole world.

2.5. Developing New Monitoring Technologies to Support Expanded Demands

Cooperative monitoring has inherent limitations but offers unique benefits. Because inspections protocols are shared, the potential for deception and countermeasures is obvious. However, access rights afforded an international or multilateral inspectorate can extend well beyond those feasible by other means. As information gathering is done in the open, platforms that might be wholly impractical in a denied access context become feasible. Persistent surveillance opportunities are also expanded. The technical solutions pursued for cooperative monitoring must not infringe upon national technical capabilities, but the different design space and relaxed operational requirements can open up useful monitoring opportunities. Weapon design information must be protected and legitimate proprietary interests must be protected. Information barriers that allow reliable conclusions to be drawn by an inspecting party, while protecting design information and legitimate proprietary interests, must be developed and utilized.[18]

Research and development, ideally undertaken in partnership with other nuclear weapons and NNWS, along with the IAEA, must address several challenges, and in every case, take advantage of advances in information technologies. Priority should be placed on:

- **Information Barriers.** Information barriers that provide robust protection against unauthorized disclosures of sensitive information must be demonstrated. An ongoing level of effort is needed because vulnerabilities change over time as technology advances. More work is needed to ensure that the confidence required in a warhead verification measurement can be attained when such a barrier is employed.

[18] These issues have also been recognized by the State Department's International Security Advisory Board (ISAB), and near term technical steps for trust building with Russia proposed. See ISAB report "Verification Measures - Near Term Technical Steps," 2012; http://www.state.gov/t/avc/isab/200465.htm

Authentication is essential to the process if trust is to be achieved. However, it has been best understood in a data transmission context, and is less well developed for a cooperative monitoring context. Approaches to functional testing, joint development, and random selection along with advanced measurement techniques should all be explored. A clear understanding of the measurement protocol to be utilized, along with the development of appropriately tailored hardware/software, is needed to identify and mitigate vulnerabilities.

- **Persistent Surveillance and Perimeter Monitoring.** Measures to provide enhanced and persistent surveillance within facilities, to monitor movements in and out of facilities, and on a limited regional basis will be needed in both arms control and international safeguards applications. Whether declared items and materials are of weapons origin, or derive from civilian activities, the ability to remotely monitor and understand nuclear activities in near-real time is needed. Maintaining continuity of knowledge can deter violations and provide a basis for more efficient verification.

  New methods for monitoring facility perimeters and penetrations are needed to verify facility designs and monitor relevant material movements. Transfers from facility to facility over a wide but known area must also be tracked. These capabilities can be applied on a routine basis or as part of enhanced monitoring requirements authorized under U.N. Security Council resolutions in response to cases of noncompliance, e.g., the gas centrifuge facility at Natanz. Such monitoring approaches could benefit from recent lessons learned in developing ISR technical and architectural solutions to support conventional warfighting.[19]
- **Real-time Process Monitoring.** Within a facility, efforts to improve material assay capabilities should be augmented by on-line instrumentation and process monitoring to provide the detailed information necessary to understand complex facility operations at enrichment and reprocessing plants. The large quantities of data generated through such approaches must be analyzed to draw relevant conclusions in a timely manner. This requires effective algorithms that correctly identify activities of concern without hampering legitimate activities.
- **In-Field Inspection Tools.** While accurate material measurements will remain important, IAEA is increasingly focused on investigations of noncompliance and assessing the nature of a state's overall nuclear program. Since the Persian Gulf War and the revelations of the extent of the Iraqi nuclear program, the IAEA has shifted its attention to an examination of a state's actions as a whole. This has led to an increased need for investigatory tools that can be used for in-field measurements during an inspection, perhaps at previously undeclared locations. Providing as much information as possible to an inspector on past nuclear activities at a site, preferably while they still remain in the field, will grow in importance. Such forensic capability is also valuable in

[19] See Chapters 3 and 5 for further discussion on this topic.

verifying cases of nuclear roll-back (e.g., Libya) and potentially the verification of dismantling or decommissioning in an arms control context. To assist investigation efforts in cases of suspected noncompliance, new tools are needed to support inspections in the field. Portable analytical capabilities that are capable of providing rapid and accurate sample analyses to inspectors should be further developed. Improved capabilities in this area help ensure that follow-up activities can be swiftly identified, limiting opportunities for concealment attempts.

2.6. Considerations for U.S. Nuclear Modernization Programs

As future arms control efforts will likely result in expanded access at U.S. facilities, weapons, and platforms, approaches for meeting verification objectives while limiting overall intrusiveness will be needed. An informal survey by the Task Force indicated that DOE/NNSA is aware of the concern and has introduced the issue into the programs for the new production facilities it is building. For example, a team from DOE's nonproliferation program and from the State Department had a favorable review with the designers of the new Uranium Processing Facility in the weapons program. The Task Force did not learn of any comparable considerations integral to DoD's programs.

2.7. Open Skies Treaty – Another Opportunity to Build Upon?

The Task Force also considered the merits of extant treaties against the future proliferation environment and found them in need of updating to apply them to a broader proliferation agenda before significant investments are made. An example that was considered in detail was the upgrading of the capabilities of the United States Open Skies Treaty aircraft. Based on the quality of the sensors allowed by the treaty, the Task Force would not recommend such a course of action at this time. The sensor specifications permitted by the treaty are outdated when compared with the need. In fact, the existing treaty requirements can be fulfilled by sensor information readily available from commercial imagery without the expense of flight missions or sensor upgrades. Therefore the costs of such an upgrade of the aircraft, which would be significant, are not justified at this time. The Task Force believes, however, that the original principles of the treaty remain valuable and could serve as a template for expansion to other bilateral agreements, but the compliance protocols should be updated before any new aircraft upgrades are considered––in spite of the fact that the Russians are upgrading their system.

2.8. Recommendations: Cooperative Regimes

International Cooperation and Transparency. State/AVC (diplomatic), DOE/NNSA/NA-20 (technical), and DoD/DTRA (operational) should develop a joint long-term international engagement plan aimed at the ultimate goal of international cooperation and transparency, and cooperatively implement their respective/shared responsibilities.

The Task Force recommends a 4-phase approach for expanded cooperation, each step of which would gradually evolve to "internationalize the transparency inspections." The Task Force approach could be enabled by expansion of the role of IAEA for assuming responsibility for the transparency responsibilities that ultimately emerge:

1. Bilateral, cooperative developments and evaluations among P-5 states, building on experience in historic allied partnership programs, as well as the CTR program with Russia;
2. Extension to all nuclear weapon states;
3. Expansion to nuclear materials transparency among major states with nuclear power generation;
4. Negotiation of a future Non-Proliferation Treaty (NPT "X") to bring in all nuclear weapon and material programs into a cooperative, multi-lateral regime.

The three lead offices cited should establish a Multi-Agency Roadmap in partnership with other relevant players in the USG. The effort should be spearheaded by a (U.S.) Mission Manager[20] to drive the realization and coordination for this initiative throughout the development process.

Key steps in support of the engagement plan and roadmap include the following:

- The activities outlined in the Road Map should be given priority within the participating Agencies, including clear definition of the anticipated step-by-step approach to realize the initiative.
- The State Department should begin to consult with foreign representatives, in order to prepare for their participation, starting with a rough schedule for joint efforts, and devise measures of effectiveness to ensure success through the distinct phases (P-5, nuclear weapon states, SNM possessors, etc.)
- Blue Team and Red Team efforts[21] should begin and be coordinated from the outset, to ensure that the proposals brought forward can meet the requirements to protect our own (and others) sensitive information from being revealed, while meeting the goals of accurate SNM characterizations.
- Major efforts should be mounted to adapt the proposed technologies into use, in the U.S. and in countries worldwide, to ensure that security measures are not compromised for either warheads or materials. (This will entail creativity and flexibility by both the inspected and inspecting parties to ensure that robust security information protection and material protection measures are retained.)
- Focused consultations with the U.S. Congress will be needed to ensure that all foreign interactions and participations meet U.S. Atomic Energy Act protections and

[20] See Chapter 5 for a more complete discussion on the Mission Manager role.
[21] See Chapters 4 and 6 for a more complete discussion on the Blue and Red teaming.

classification constraints, including establishing new Congressional "123" Agreements[22] for participating nations as required.

- As the transparency effort emerges, it will be critical to ensure (1) a high level of confidence in, (2) acceptance for use of, and (3) expressions of support for, the efforts by all U.S. departments and agencies responsible for U.S nuclear weapons and for SNM inventories in government and private custody. (The Task Force notes that advance buy-in and enthusiastic support for eventual achievement of a Universal Transparency Regime is crucial to prevent "pocket-vetoes" within the U.S. interagency forums, and later in negotiating the international agreements.)
- Finally, the Task Force recommends that a line item budget be sought for this important multi-year initiative, with dedicated funding for developing the key technology pieces, for creation of the operating systems that will be proposed for joint international use, and the cooperative experiments and trials with foreign nations.

Research and Development. DOE/NNSA/NA-20 should pursue an international R&D program in automated monitoring and reporting systems supported by information barriers and authentication to enable more effective and extensive materials monitoring. Trusted information barriers, capabilities for real-time process monitoring and in-field inspection and analysis capabilities should be developed.

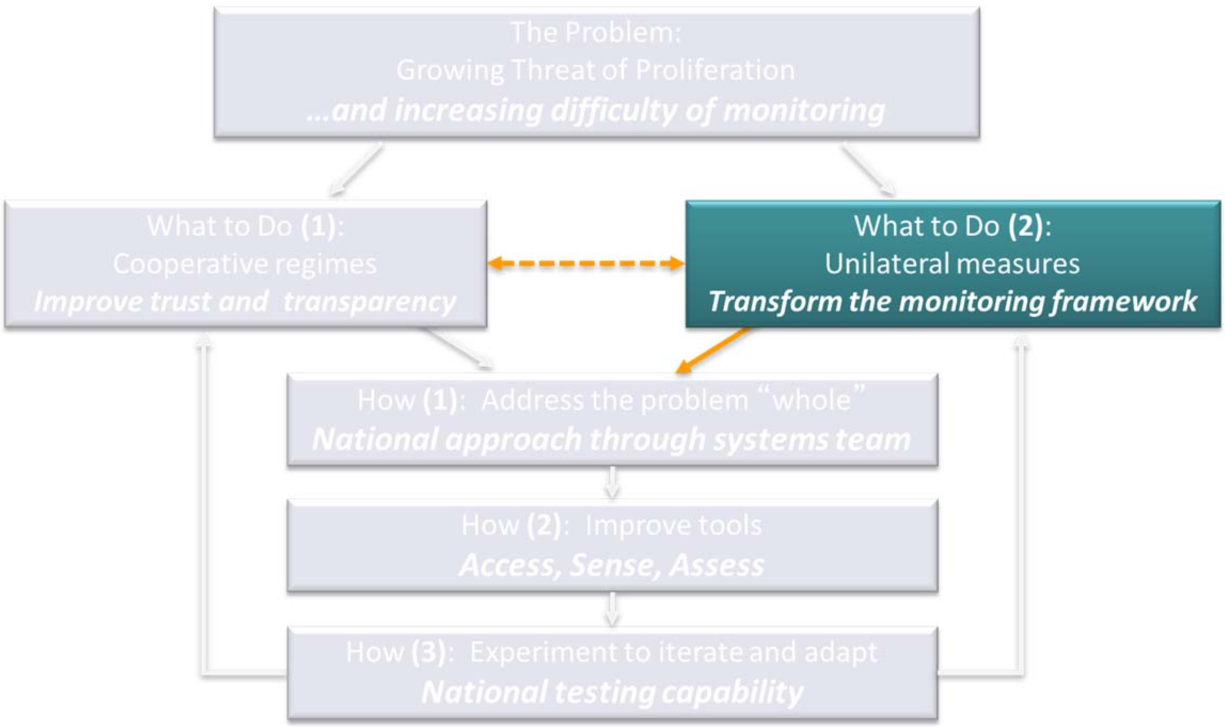
DoD/Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs ASD(NCB), DTRA, and DOE/NNSA/NA-10 should partner to develop cooperative options for asymmetric nuclear weapons security paradigms; e.g.,

- Sharable technical security principles, practices, and technologies for sites, materials, and components
- Site declaration and portal monitoring
- "Assurance Volume" concepts

U.S. Modernization Programs. In anticipation of treaties and agreements with more intrusive inspection regimes, State/AVC, DOE/NNSA, and DoD/AT&L should review current U.S. facility and weapon system modernization programs and instruct program managers, if necessary, to plan for accommodation of greater transparency measures. Methods for red teaming and performing vulnerability assessments should be developed and exercised routinely.

[22] Section 123 of the United States Atomic Energy Act of 1954, titled "Cooperation With Other Nations", establishes an agreement for cooperation as a prerequisite for nuclear deals between the US and any other nation. Such an agreement is called a 123 Agreement. To date, the U.S. has entered into roughly twenty-five 123 Agreements with various countries.

Chapter 3. Unilateral Measures: Transforming the Monitoring Framework



3.1. Introduction

Careful review of the ability to detect undesirable nuclear activities by non-nuclear states and non-state actors, as well as nuclear states experiencing internal instability or external threats, was a major part of the Task Force's effort. In general, prior reviews have come to two conclusions: that discovering such activities, if the perpetrator seeks to hide them, is a very difficult problem, and that the technical capabilities to do so are limited. This Task Force agrees with those conclusions, but believes there are some avenues of R&D worth pursuing to improve the current situation.

The national security community has faced such difficult problems before and generally found ways to achieve significant capability, if not entirely to solve them. Two examples are Anti-Submarine Warfare (ASW) and the recent problem of Countering Improvised Explosive Devices (Counter-IED). Both of these problems represented major threats and were difficult to solve, but a combination of technologies, some considered "out of the box," used in an end-to-end approach, was employed to achieve a satisfactory solution.

In its first phase during WWII, the ASW problem was significantly diminished by the advanced code breaking devices developed (the precursors of modern day computers), along with careful analysis of the patterns of operation by the German fleet. The second ASW problem, tracking the extremely quiet nuclear propelled and armed submarine developed during the Cold War, was addressed by the judicious blending of advanced large scale sonar arrays, discrete shadowing of threatening boats, and advanced algorithms to pull small signals from high clutter environments.

The IED problem has been addressed with a twofold attack: find the network and find the device. This has resulted in a significant mitigation of the threat. Both existing and new technologies have been brought to bear to address this problem. They can be categorized and characterized in the following six categories:

- **Persistence**: Holding the adversary at risk 24/7
- **Multi-INT integration**: One or more INTs to "find", one or more to "fix"
- **Advanced network analyses**: Tools to derive information from huge data sets
- **New cyber tools and techniques**: Cyber mining and geolocating to latitude and longitude
- **Improved SIGINT**: More signals, under more conditions

3.2. Characteristics of Monitoring Illicit Nuclear Activities

The Task Force agreed that <u>the guiding principle for monitoring to detect undesirable nuclear activity should be detection of activities as early in the planning and acquisition of a capability as possible</u> in order to provide the greatest number of options for slowing or reversing the effort. Difficulties arise from several factors—each one a challenge in itself, but in combination, as or more daunting than the ASW or Counter-IED problems. First, the number of actors and their geographic dispersion worldwide is large. Second, the observables are limited, typically ambiguous, and part of a high clutter environment of unrelated activities. Moreover, at low levels associated with small or nascent programs, key observables are easily masked and observation made more difficult without ready access by the full range of persistent intelligence systems. Third, and perhaps most significant, is that radiation phenomenology unique to SNM is not detectable at long standoff distances, further exacerbating the large area problem.

The signal-to-clutter characteristics are similar to those faced in ISR support to conventional warfighting and counterterrorism. The ISR architectural approach is based on a cueing principle that starts with general observations from multiple intelligence and surveillance sources and assigns ever more specific and precise assets to targets that appear to be of growing concern. Distinguishing characteristics of this approach are persistence, but not necessarily of the highest fidelity, widespread access to all the available data, allowing more "eyes on target" to detect anomalous behaviors or activities, and flexibility to rapidly reassign monitoring assets to "pop-up" areas of interest.

The Task Force believes there is promise in applying the conventional ISR paradigm to the proliferation monitoring problem. Unknown, however, is how well the ISR paradigm can be adapted to the spatial and temporal domains for monitoring suspect nuclear activities where long periods of observing normal patterns of life over large geographic areas will be punctuated by short duration anomalous events. Nonetheless, the impressive advances made in Iraqi Freedom and Enduring Freedom in support of locating both IEDs and the perpetrators warrant a serious effort to see how well these ISR technical and architectural approaches can be adapted to support proliferation monitoring.

3.3. A Cursory Examination of ISR Applied to Nuclear Monitoring

A closer examination of undesirable nuclear activities reveals two categories of focus for monitoring activities. Whether state or non-state actors, the two "headline" activities of concern are: 1) obtaining a nuclear device from existing stockpiles, or SNM from existing storage facilities; or 2) developing a nuclear device. In both of these cases, the primary objective should be to transition the initial monitoring problem (overwhelmingly large area and very small observable signature) into a more tractable one by either reducing the area that needs to be monitored or by establishing a more observable indicator of the activity.

The Task Force then dissected the problem into its simplest parts. The ways that a nuclear device could be obtained from an existing nuclear arsenal include:

- **Buying**: A large amount of money might induce the release of a few;
- **Stealing**: An insider could sneak one out of a facility;
- **Be given one**: Leaders of a weapon state could give one to a sympathetic or surrogate organization;
- **Recovering**: A lost device might be found;
- **Capturing**: A device may be taken from a storage facility or during transit.

The development of a nuclear device is in a relative sense conceptually simpler in that the developer must obtain or process SNM. Plutonium is more easily obtained, but weaponization more difficult. By contrast, HEU is more difficult to produce, but a device is relatively easy to fabricate.

With this simplified view of undesirable nuclear activities to be detected as early as possible, monitoring objectives can be stated as follows:

- Maintain an accurate accounting of existing nuclear material and devices in both declared and non-declared countries (see Chapter 2 for a phased path to achieve this objective);
- Detect and follow progress of suspected nuclear device development activity.

The Task Force then asked what the ASW and IED problems might teach us about this problem. The principal lesson is that detection using any single phenomenology or based on a single observable is not going to be successful. A multi-modal approach that goes after both primary and secondary observables is required.

Much of what was learned from the IED problem can be summarized as "find the network, find the device." Groups, not individual actors, carry out nuclear activities, much like the development and deployment of an IED. Coordination among several actors and organizations is required either to obtain a device or to develop one. Observing this coordination is the first indicator in the monitoring process and one for which many of the tools developed in dealing with IEDs should be well suited.

Exploiting the cyber domain should certainly be a big part of any nuclear monitoring effort. Both passive, depending on what is sent voluntarily, and active sources should be considered. Data gathered from the cyber domain establishes a rich and exploitable source for determining activities of individuals, groups and organizations needed to participate in either the procurement or development of a nuclear device. In fact, a set of new techniques, e.g. Advanced Graph Analysis (i.e., modeling relationships between data elements and data attributes as graphs to solve complex analytical problems), for exploiting these data have been developed and can be applied to the network of people possibly engaged in the activities associated with nuclear weapons.

Exploitation of the cyber domain to follow people, financial transactions, etc., is a critical first step in establishing a focus for technical monitoring based on other phenomenologies.[23] In other words, given the cyber cues, concentrated multi-INT collection and exploitation over a focused area is feasible. This is the basic process that has been used with success in recent areas of conflict where air and space collection platforms have generally enjoyed unfettered access. Moving forward, these same processes need to be applied in denied areas. Many of the new technology advances in data exfiltration, covert implantation, etc., hold promise for successful multi-INT collection and exploitation in non-permissive environments.

[23] The potential for OSINT (open source intelligence) as a focusing step is also promising and should be explored. See Chapter 5, Section 5.5.4 for a discussion.

3.4. Recommendations: Unilateral Measures

The guiding principle for monitoring to detect undesirable nuclear activity should be detection of activities as early in the planning and acquisition of a capability as possible in order to provide the greatest number of options for slowing or reversing the effort. New ISR technologies, demonstrated in recent conflicts, offer significant promise for monitoring undesirable nuclear activity throughout the world. The nature of the monitoring challenge, however, is such that these technologies are most effective when applied in an integrated architecture. To accomplish that goal, the Task Force recommends that:

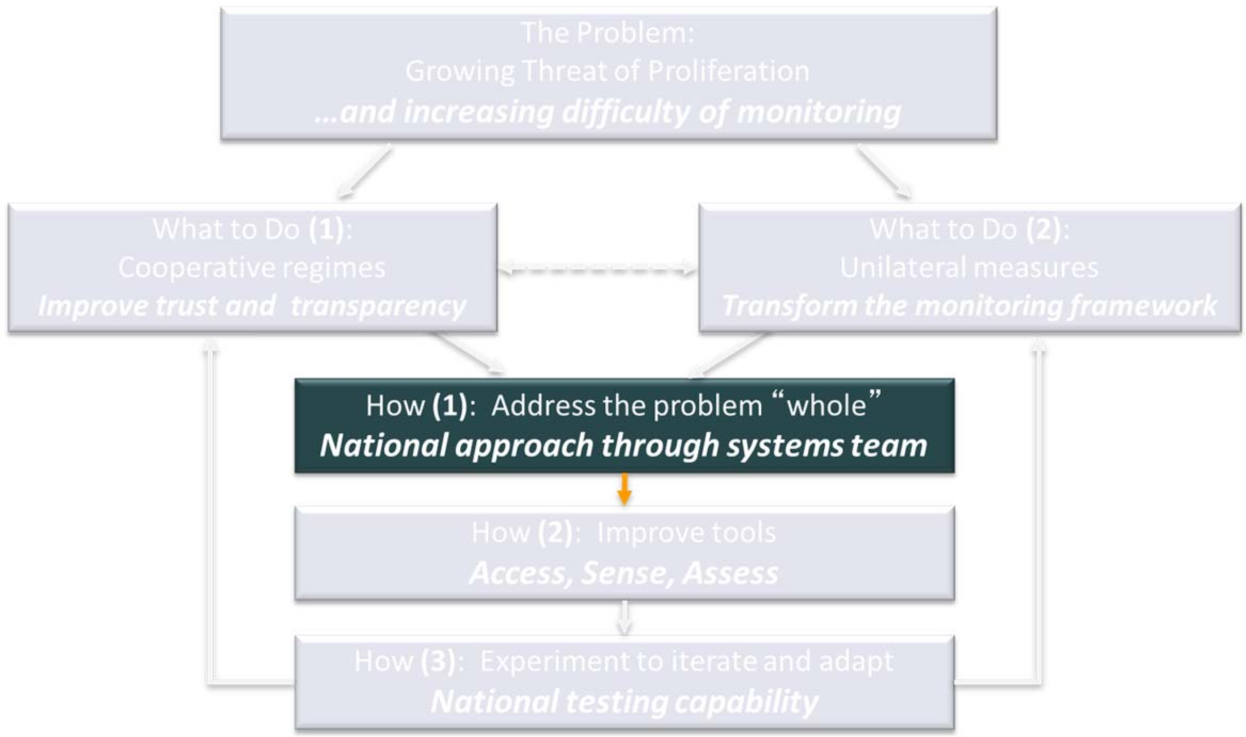
- The IC (led by the National Counterproliferation Center [NCPC]), DOE/NNSA, DoD/DTRA and Department of Homeland Security (DHS)/Domestic Nuclear Detection Office (DNDO), should develop a joint roadmap supported by the necessary systems analysis and engineering capabilities to implement an integrated, more comprehensive and responsive monitoring architecture for nuclear weapons activities worldwide, expanding upon the more general, but static approaches currently employed. As the legislated interagency lead for the Global Nuclear Detection Architecture (GNDA), DNDO should incorporate this more expansive monitoring architecture into the GNDA. The monitoring architecture should be structured to:
  - Create "corridors of observation" in multiple domains (geographic, commercial, individuals, financial…) based on open source and available multi-intelligence (INT) information;
  - Establish "patterns of life" within corridors that are suspicious;
  - Focus persistent monitoring assets on individuals and activities of greatest concern that emerge from patterns of life analyses;
  - Assemble and analyze data from all sources to support verification or identify previously unknown concerns;
  - Use results of analyses to iterate—i.e., to provide ever more focus for intelligence taskings, as well as provide guidance for needed improvements in technical and operational capabilities.

  It should also identify lead and support roles and responsibilities for its implementation.
- National Security Staff (NSS) should request that DoD integrate the architectural elements into a global awareness system that:
  - Builds on lessons and experiences of successful national security capabilities, such as the Counter IED Operations Integration Center (COIC), NSA's counter-terrorism capabilities, NCPC's counterproliferation efforts, and on DOE's Proliferation Risk Analysis Program;
  - Builds also upon the lessons and experience of the IC's Treaty Monitoring Manager[24], which at the height of arms control monitoring in the late '80s and

[24] The responsibilities of the Treaty Monitoring Manger are discussed more fully in the context of proliferation monitoring in Chapter 5.

    early '90s proved an effective vehicle for coordinating the work of multiple organizations and collection activities;
  - Uses the Monitoring and Verification (M&V) national testing capabilities (described and recommended in Chapter 6) as the key operational assessment vehicle to test a range of scenarios.
- The IC should recast DOE/IN's historic "nth country" analytical capabilities into an "nth group" effort, adapted to the wider range of actors and designs accompanying both vertical and horizontal proliferation.
  - The "nth group" program should serve as a community asset for helping to characterize proliferation pathways from available data and advancing technology, and posit pathways to guide collection priorities.

Chapter 4.
Address the Problem "Whole": A National Approach through a Systems Team



4.1. Introduction

Monitoring and verification for proliferation present a set of challenges that are difficult both technically and operationally. Progress and efficient use of resources in both domains should rely on solid, on-going analysis, but the analytical scope and complexity are no less challenging themselves. Many of the analytical challenges associated with M&V have been addressed in the past within the framework of historical treaties and agreements, which have often been unique to specific problem areas and definitions (such as detection limits, surveillance methods, and treaty details). As planners consider how the U.S. should address monitoring and verification missions in the future, new technologies, treaties, agreements, policies, and proliferators will change the landscape of capability requirements and continue to add complexity. The Task Force believes that experienced professionals in the area should not continue to address the problem as an extension of approaches used in the past treaties and agreements.

To better address the future monitoring challenge, the Task Force believes that there is a need to establish an enduring yet adaptable holistic methodology that encompasses the totality of the problem and solution space, along with the analytical capability for exercising that methodology, for guiding and facilitating the creation of roadmaps and plans for M&V

capabilities as well as for evaluating developing capabilities. In other words, addressing the future M&V challenges demands a systems approach. Moreover, execution of a systems approach would be most effectively accomplished through a "national" team to help provide a high degree of unanimity and coherence of purpose among the numerous and disparate agencies involved.

The Task Force also recognized that while easy to recommend a systems approach, it is much more difficult to do—and do well. We therefore challenged ourselves to see if we could provide an example and potential starting point for the community to understand the problem in its full breadth, depth, and extent, and to offer guidance on the path forward. This chapter provides an abridged version of those results, which are detailed more fully in Appendix A.

4.2. Elements of an M&V Analytical Methodology

Several key elements are proposed as necessary parts of an enduring M&V analytical methodology, as laid out in Figure 4-1.

- First, there is the "problem space," which consists of a set of frameworks that describe the M&V challenge independent of any proposed solutions. The problem space provides the basis that will serve as a common foundational understanding for solutions to be built upon and assessed for effectiveness.
- Second is the "solution space," in which proposed capability architectures are crafted. These architectures are collections of technologies, operations, and capabilities that work together to accomplish the goals and objectives identified to address the problem space.
- Third, there must be a Bridging Methodology which allows for the "back and forth" between the problem space and solution space; i.e., the tracking, integration, and trade-offs among objectives, requirements and architectural solutions to the problem.
- Finally, there must be a rigorous and repeatable portfolio decision methodology that allows for the values of the decision maker and his/her organization to be incorporated, and for defensible, tractable decisions to be made.

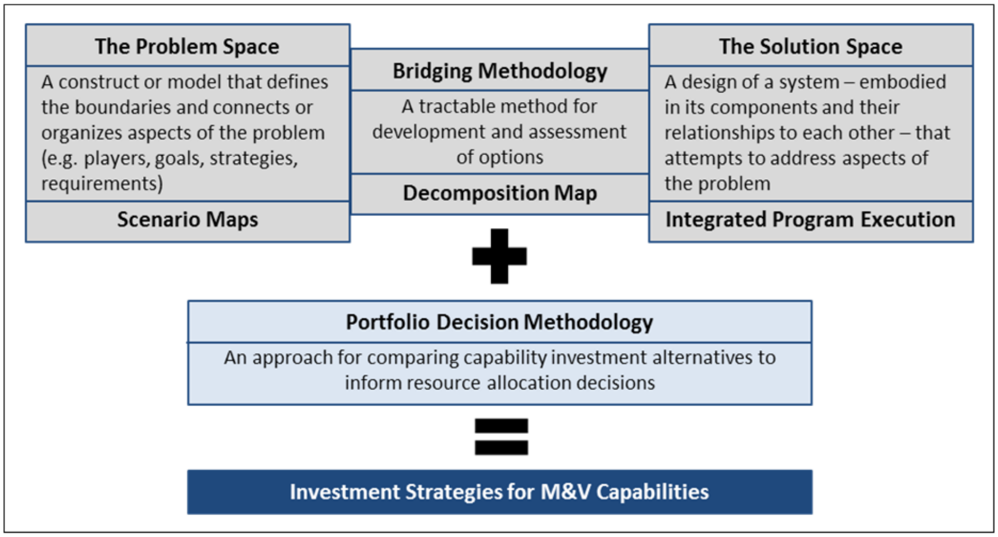


Figure 4-1 Elements of an M&V Analytical Methodology

A common issue in the development of analytical frameworks has been the tendency to frame the problem and solution together. The conflation of "problem space" and "solution space" brings with it several consequences:

- It tends to promote metrics and assessments that support optimized subsystem or component performance vs. system performance by assuming they are one and the same.
- It tends to lead analysts to fixate on a narrower problem (such as detector performance) rather than assessing those issues in the context of the larger whole.
- It does not enable a common understanding of the problem space itself, allowing solutions to be framed in whatever manner the solution proponent deems suitable.

All of these symptoms run counter to enabling the decision maker to achieve his/her ultimate goal: rendering and defending a provably effective investment strategy for M&V capability development. Separating the "problem space" from the "solution space" and analyzing them independently can therefore yield benefits by eliminating or mitigating these issues.

To illustrate the point, consider that detection systems have often been placed at the forefront of the national strategy for detecting the illicit movement of nuclear threats in proliferation regimes. While undoubtedly detectors play a role in the solution, the bulk of current analytical activities are focused on detector system performance. As a result, the M&V problem of detecting illicit movements is often miscast implicitly as a detector problem. This can lead to the line of thinking that more detectors with better detector performance parameters must logically provide reduced risk – a statement that may or may not be true. More importantly, other options that do not hinge on detector deployments may in fact provide more cost effective mechanisms for risk reductions.

4.3. Proposed Problem Space Description

While there are several possible frameworks for describing the M&V problem space, the Task Force chose to use one based on scenarios, defined here as follows:

> *A scenario is an evolution of the world through a series of incremental events from its current status towards an outcome of interest that is specified by the analyst.*

However, the Task Force did not adopt a scenario-based planning approach because of: the pitfalls of drawing conclusions from a too narrowly defined set of scenarios, especially if they represent the analysts' or decision makers' "favorites"; or conversely, the unwieldy nature of systematically analyzing too many scenarios. Instead the Task Force developed a scenario framework that attempts to encompass a large portion of the potential scenario space in order to address the totality of M&V problem complexity. A scenario framework for scenario generation and analysis is desirable primarily because it enables the examination of a family of scenarios, rather than a small set of independent and specific scenarios. It also provides a systematic method for decomposing scenarios into discrete nodes and linkages, and capturing the interdependencies between individual scenarios. Finally, it lays the foundation for a bridging methodology, or systematic mapping between the problem space and solutions space, that enables increased traceability between planner objectives and solution performance.

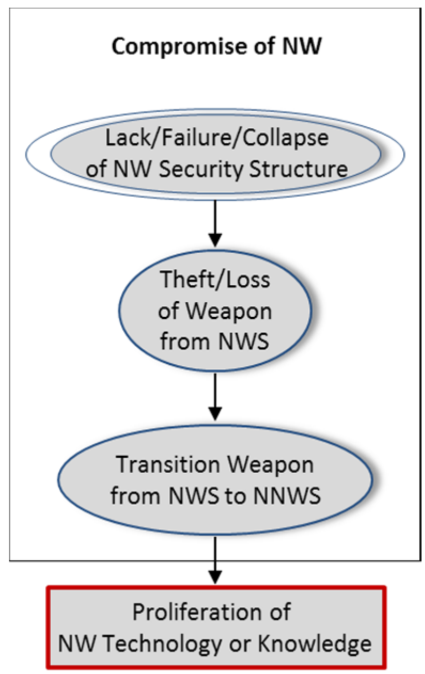


Figure 4-2 Example Node Sequence

The scenario framework developed by the Task Force for M&V started with the construction of a number of simple scenarios characterized by key nodes (events) and associated linkages. One such scenario, initiated by the collapse of a nuclear weapons state's security system, is illustrated in **Error! Reference source not found.**.

The Task Force proceeded to construct as exhaustive of a set of such scenarios as it could think of, using this node-linkage approach.[25] The effort yielded both a practically complete description of the M&V challenge, as well as the identification of shared nodes and pathways among scenarios. The complete scenario framework (plus a readable, large format version in Appendix A) is illustrated in Figure 4-2.

[25] This task force built upon previous work for OSD/NCB/NM by the DOE/NNSA laboratories: "*Analysis of Capability Options for the DoD Countering Nuclear Threats Mission: NNSA Tri-lab Phase 1 Summary,*" Sandia National Laboratories report SAND 2011-7985, November 2011.

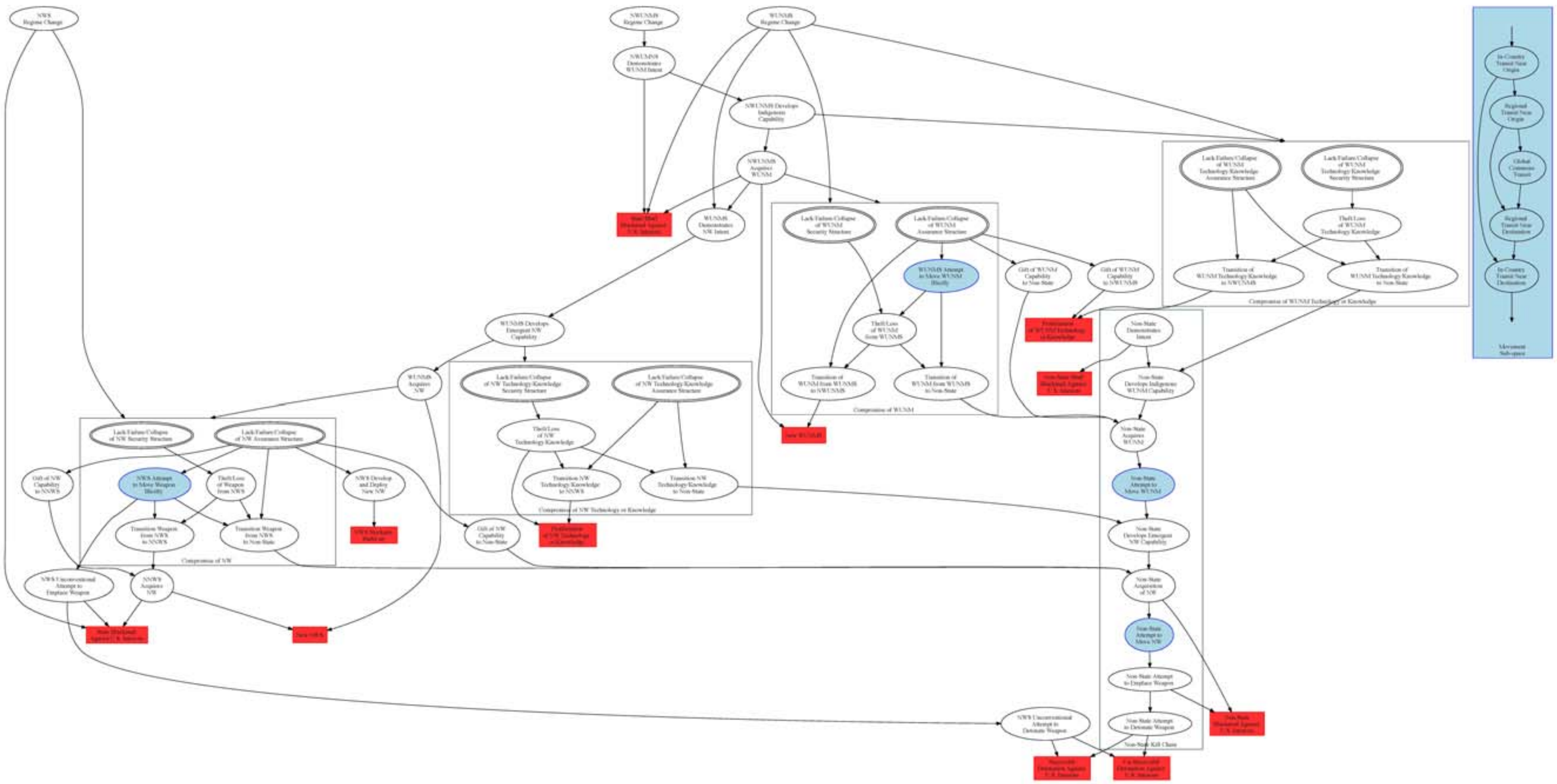


Figure 4-2 Scenario Framework of M&V

Blue-colored nodes indicate “macro” nodes, or nodes that are easily decomposed into a common set of sub-nodes. The “movement sub-space” is examined as an example. This sub-space corresponds to movement through the origin region, across international boundaries, through global commons, and into the target region. The movement sub-space is laid out in the blue box on the right hand side of the framework diagram.

4.3.1. Analysis Within the Scenario Framework

The scenario framework serves several roles. Most importantly, it exists as a common frame of reference for describing the M&V problem space. Narrower problem definitions, metrics, and objectives can be derived where appropriate through decomposition (discussed in Section 4.4.1). Scenarios for analysis can be generated by stringing sequences of nodes together. Any starting point and ending point can be selected, and a path through the network selected to connect them. From that string of nodes, a more complete narrative can be constructed.

The scenario framework can also allow for greater and more complete coverage in the design and analysis of solution architectures. A large family of scenarios can be analyzed by examining all nodes systematically node-by-node independent of end-to-end scenarios. An analyst can consider solution architectures that combat adversary success within a single node, and consider the collective impact it has on the complete scenario space by examining both upstream and downstream nodes. In addition, tradeoffs between architectures designed for different nodes can be compared in an end-to-end system performance sense. This will aid the assessment of the complete set of architecture components within a portfolio of defensive measures and allow for complex trades to be made. The scenario framework should be periodically reviewed and updated as appropriate based on real world experience and additional analytical studies.

While the scenario framework provides the structure for this kind of analysis, there is still the challenge of developing end-to-end metrics that are solution independent and common among all nodes. Further consideration of this issue is given in Section 4.5.1.

4.4. Bridging Methodologies

The method used to connect the problem and solution spaces is called a bridging methodology. It allows for a breakdown and prioritization of goals and objectives in the problem space into requirements and metrics for potential solution architectures. It also allows for the systematic aggregation of performance assessments and analyses into an overall picture of monitoring and verification architecture performance.

4.4.1. Proposed Decomposition Map Approach

The bridging method proposed by the Task Force is a decomposition approach that systematically maps problem space descriptions to prospective solution architect elements. The approach begins with the selection of any node in the scenario framework discussed in Section 4.3. The selected node is decomposed into sub-nodes required to add appropriate fidelity or resolution to the analysis. A system of decomposition layers is then constructed beneath the scenario nodes. Those layers, with increasing levels of specificity, are:

1. **Strategic Capability Areas** – This layer centers on core elements of the mission space associated with reducing risk.
2. **Functional Objectives** – Within each Strategic Capability Area, several functional objectives are articulated to capture high-level operational objectives that must be achieved.
3. **Tasks** – Each functional objective is further decomposed into a set of tasks. The tasks themselves are part of prospective solution architecture – i.e., tasks, just like objectives, are not universally defined, but proposed as part of a solution option.
4. **Assets** – Each task is accomplished through the employment of assets. Assets can include hardware, platforms, people, training, concepts of operations, and programs – essentially any capability that can be specifically invested in.

Each node in the scenario framework proposed in Section 4.3 will have at least one unique decomposition map associated with it in a fully formed analytical effort. There are only a limited number of unique investible assets that may be incorporated in prospective solution architectures, and many assets are likely applicable to several different functional objectives and tasks. These observations imply that most assets will aggregate requirements from multiple scenario nodes, strategic capability areas, functional objectives, and tasks. Assets must be assessed against each set, and synergies may be identified and leveraged when designing solution architectures. Optimistically, the same asset may have sufficient performance and applicability across multiple tasks, functional objectives, strategic capability areas, and scenario nodes.

4.4.2. Decomposition Map Example

The overall decomposition approach described in Section 4.4.1 may be best described through the example illustrated in Figure 4-3. The example decomposition map begins with a focus on the scenario node "Non-State Attempt to Move Weapon." The scenario node is decomposed into more specific scenario sub-nodes; in this case the analyst is concerned with "In Country Movement" of a nuclear weapon or asset.

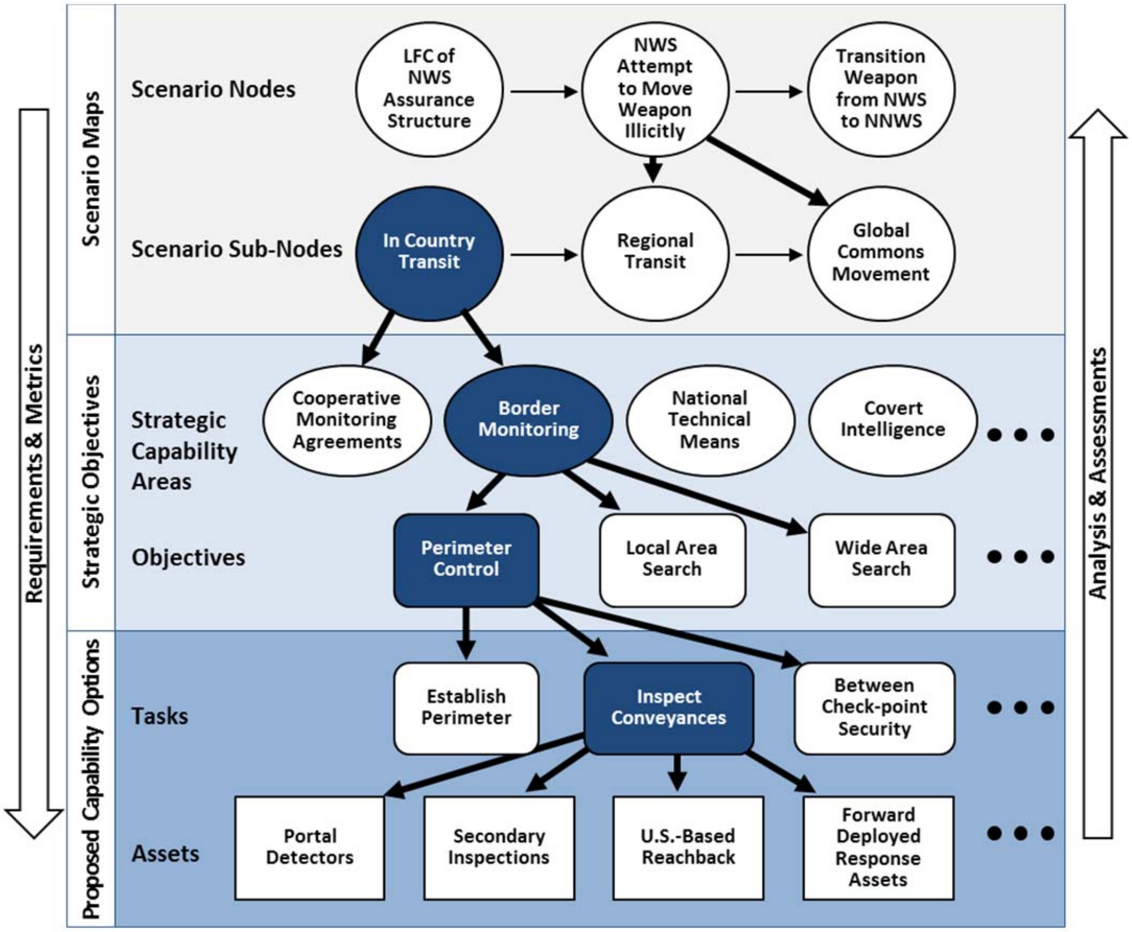


Figure 4-3 Example Decomposition Map

The next step of decomposition moves from the problem description (the top shaded area, labeled "Scenario Maps," in the decomposition map) into development of a solution architecture (the blue shaded area in the decomposition map). The scenario sub-nodes are decomposed into strategic capability areas dividing the problem space into discrete mission areas – in this case the strategic capability area of border monitoring is highlighted for further decomposition. Of several possible functional objectives for border monitoring, our example will consider perimeter control, which can be further decomposed into a set of tasks that must be accomplished in order fulfill that objective. These tasks and the assets associated with them represent a proposed solution architecture for accomplishing the objectives specified. For example, items that pass through that perimeter must be inspected to ensure that no nuclear contraband is passing across the perimeter.

As noted with the arrow on each side of the decomposition map, the requirements and metrics by which proposed assets are to be assessed have been derivatively defined from the previous layer. As assessments are made and analytical results obtained, they are aggregated into performance assessments of higher and higher layers. The derivation of a tractable set of metrics through this process is not a trivial task. Moving down the chain through strategic capability areas, functional objectives, tasks, and assets, metrics of increasing resolution and granularity are derived. At the asset level, the metrics center largely on performance specifications that are technology specific. These metrics are familiar in radiation detector assessments, for example, but on their own, are only implicitly related to the overall goals of risk-reduction. A metrics derivation process such as this places each metric in the context of the layer above it, explicitly linking it to overall architecture performance.

4.5. Portfolio Decision Methodologies

In order to render the analytical results that produce well-characterized architectural options from the approach described above into investment roadmaps, a decision framework must be established. While this section does not attempt to propose a decision framework, it does provide some considerations for doing so.

4.5.1. End-to-End Metrics

Risk (or risk minimization) is most often the implicit or explicit top-level metric for the decision maker. It provides a metric for endogenous trade-offs within the M&V problem space, allowing for the comparison of very different solution sets and examination of benefit between investments both within and across different components of the problem space itself. Utilizing risk as an end-to-end metric in the M&V problem space can also enable exogenous trades, as governments face economic challenges and must make tougher decisions about where to invest resources.

Utilization of risk as an end-to-end metric comes with a set of inherent challenges, however. Common criticisms of formal risk assessment methodologies in decision processes include:

1. **Conflating stochastic processes and adversary decisions** – Well characterized stochastic processes do not govern intelligent adversaries; instead, they make informed decisions. Although frequently used, probabilistic representations of adversary decisions are, for the most part, meaningless. However, characterization of uncertainty about adversary decisions in a probabilistic analysis can be beneficial, if carefully developed.
2. **Focusing on absolute values rather than relative impacts and sensitivities** – The absolute values of risk are, in most formulations, arbitrary, as they are built upon the assumptions and values of the analyst or decision maker for whom they are constructed. Additionally, the models upon which risk is calculated often cannot be truly validated.
3. **Inability to define "acceptable"** – A key component of making decisions in a risk-based framework is to define "acceptable" risks within the timeframe of the investment decision itself, something often difficult to achieve, especially when multiple equities are impacted.

4. **Examining risk trade-offs too narrowly** – In problems of high uncertainty, the error in risk calculations can be so large, that close trade-offs can be interpreted as essentially the same. Not having well-defined uncertainties can allow false comparisons to drive decision processes. At the same time, ignoring the uncertainty (or error bars) in the analysis denies they opportunity to prioritize potential efforts to improve understanding.
5. **Misuse of probability and statistics** – While it may seem like an elementary mistake, bad assumptions or interpretations, especially around dependence or independence, can lead to mathematical operations and inferences that may be numerically correct, yet meaningless—or worse, incorrectly calculated.

Given the difficulties that can make a robust risk definition in the M&V space difficult, it is possible to use measures that are proximate to risk when performing analyses. For example, other studies have proposed and formalized the replacement of probability in the classical formulation of risk with the use of assessments of the difficulty an adversary would face in executing a successful attack[26], when working with risk assessments of intelligent adversaries. Additionally, understanding the readiness level of an adversary and the expected time to attack can also serve as a useful risk proxy. Regardless of the exact risk metric or proxy used, risk (or some formulation of risk proxies) is a “necessary evil” as it allows for disparate approaches to be transacted together in cost-benefit trade-offs, and provides a consistent metric and method for analysis as new information and options become clear.

4.5.2. Balancing Risk

A key role of a portfolio decision methodology is to identify investments in capabilities that balance risks given the values of the decision maker. Investment risk includes not only cost and technical risk, but also institutional decision factors. Institutional decision factors are elements such as championship, mission, acceptance, and other factors that may prevent investments from being successful if not present. While not often considered in formal decision processes, they can have a large effect on the outcomes of decisions to acquire capabilities. These factors should be accounted for in any M&V portfolio decision methodology.

As an analyst considers capability options, a balanced portfolio may be very different given the values and risk tolerance of the decision maker and the investing agency. For example, R&D focused organizations may have a set of values that is more risk tolerant, and a balanced investment portfolio may be skewed towards the long-term, high risk, high payoff projects. At the same time, an operational component may seek primarily commercial-off-the-shelf solutions and a balanced investment portfolio may be skewed towards incremental, low risk improvements. Formal and quantitative methods for assessing the risk tolerance and the

[26] Wyss, Hinton, et al, Risk-Based Cost Benefit Analysis for Security Assessment and Investment Prioritization, Sandia National Laboratories, 2011

values of decision makers exist and should be extended in formulating an M&V portfolio decision methodology.

4.6. Proposed Analytical Capability

4.6.1. The White Team

The complexity of the M&V problem requires a different analytical approach, one example of which is the scenario framework described above. In turn, the complexity of that analytical approach points to the need for a focused and sustained effort to develop and exercise the framework, the bridging methodology, requirements and metrics. The recommended approach is an analytically focused team sponsored by the appropriate government agency(ies), and populated with technical and policy experts. This team is neither a "red team" nor a "blue team," but rather an independent and unbiased body, focused on a high-level and comprehensive analytical effort to tee up options for decision makers with a clear eyed assessment of the pros and cons of each option. As such, the team should exist independently of operational or acquisition organizations. It could and should, however, utilize findings, analysis, and data from both red and blue teams. This team, which the Task Force labeled the "White Team," would have a charter that includes:

- Fully developing and stewarding the problem framework, a bridging methodology, the associated strategic requirements, and metrics;
- Participating in test-bed activities, providing data requirements to further analyses, and specifying test cases;
- Presenting policy and acquisition options to implementing agencies for decisions;
- Working with trusted international partners to examine and exchange best of breed strategies and architectures.

As steward for the problem framework and the bridging function, the white team must integrate from the comprehensive understanding of the problem space to the pool of candidate solutions. The white team should accomplish this through not only its own intellectual endeavors, but also by working closely with a "Solution Provider Team," comprised of laboratories, contractors, research institutions, and academia, who together can provide a rich set of candidate solutions. These are the organizations that should be at the forefront of technologies, systems, and their integration into operations. The solutions provider team has the charter of:

- Proposing technical and non-technical solutions in response to strategic objectives and requirements, as well as the focus for R&D when existing solutions are inadequate;
- Preparing performance analyses to serve as first pass component specific studies to feed the White Team (the "ho-ho" test);
- Working with trusted international partners to develop best of breed solutions.

While the individual members of the solution provider team may have real or perceived biases or conflicts of interest, the overall solution provider team will have a more balanced perspective, and any recommendation from them must pass through the independent filter of the White Team.

4.6.2. Implementing the White Team

Two factors are required for implementing the White Team: 1) the identification of a cadre of analysts who see a strong opportunity for a valued career experience, if not profession; and 2) the establishment of an institutional mechanism that can ensure the team's access and impact across the interagency.

Regarding the first factor, the Task Force discovered that the experienced systems analysis workforce of the Cold War has largely disappeared, just as it has in other areas related to nuclear weapons. Moreover, although there have been significant successes in nonproliferation and counterproliferation analysis, these approaches have tended to focus on problems bounded by treaties and agreements, or by specific actors of interest. They do not easily scale to meet emerging challenges across the globe. The Task Force has attempted to portray how much more complex the environment is today and into the foreseeable future. As a result, new approaches and new tools are called for. The leading agencies therefore should understand that part of their charters should be the re-growth of knowledgeable professionals, especially systems analysts, to support threat assessment, trade-off studies and experiments, and investment prioritization.

The second factor for a successful White Team is the institutional home and support that it will require in order to maintain both investment and operational functions throughout the interagency. The Task Force debated a number of mechanisms:

- Establishing a "czar"
- Appointing an executive agent
- Instituting a "holding company" model, similar to the On-Site Inspection Agency
- Assigning a mission manager (whose role is discussed in the next chapter)
- Identifying a coalition of the willing, coordinated through an Interagency Coordinating Committee
- Utilizing the "Ungroup" model, which worked so effectively as an ad hoc, high level interagency group through the negotiation and implementation of the original START treaty and other arms control agreements.

Each option has its pros and cons within the context of the monitoring and verification problem, and none seemed well suited or sufficiently innovative to address the problem as the Task Force sees it; something more unique would be needed, at least initially, in order to protect the White Team while it establishes itself. The Task Force modeled its idea after the Phase One Engineering Team (POET), which was established within a couple of years after the standup of the Strategic Defense Initiative Organization (SDIO) at DoD in the early 1980s. The POET was populated by successive generations of some of the top talent from the Federally Funded Research and Development Centers (FFRDCs) and national laboratories; individuals were independent of specific acquisition programs. The POET reported directly to the SDIO director and had sufficient influence to establish the baseline threat assessment and balanced architecture options, as well as more specific assessments of proposed technical capabilities.

Adapting the POET model into an interagency environment will require some variant of either a lead agency with accountability to partnering agencies (e.g., a “board of directors”), or governance by a special interagency board, chaired by the appropriate lead in the NSS or selected on a rotating basis among the participating agencies. The Task Force realizes that this approach is highly unusual, but also believes that other options fall short given the complexity of the problem, the need to think through new and innovative solutions, and the number of agencies and interfaces that are needed to make progress.

4.7. Recommendations: Addressing the Problem Whole

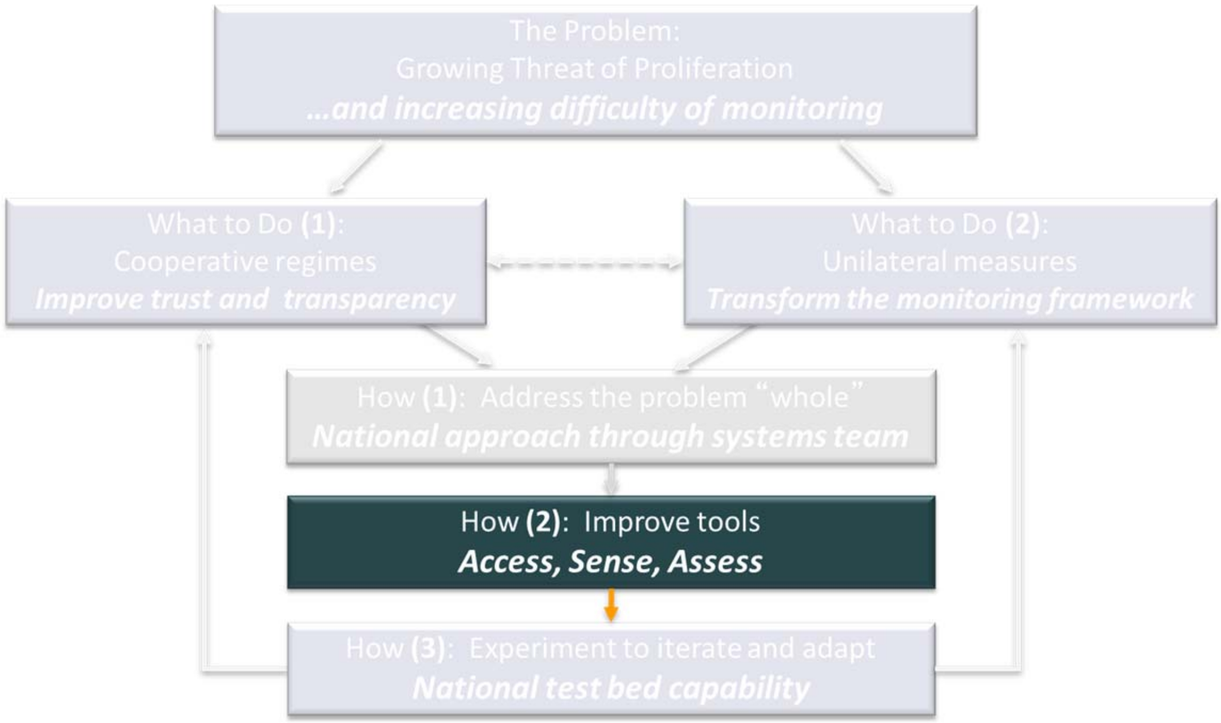
As the lead agencies, State/ASD/AVC, DoD/ASD/NCB, DOE/NNSA and IC/NCPC should create the processes and oversee the following steps:

- Establish the “White Team” whose charter is to characterize the comprehensive Monitoring and Verification Framework, relating threat events and actions to monitoring requirements, both cooperative and unilateral.
    - The White Team should be assigned to a “home” agency, but supported and governed by an interagency “board” whose members have sufficient authority to influence any needed changes in strategy and program directions at their home agencies.
- Ensure a common understanding among agency leads for addressing all aspects of the framework, including policy, diplomacy, operations, and RDT&E.
    - It is critical that those agencies involved in implementing M&V capabilities maintain a high degree of unanimity on how M&V problems and challenges are characterized, and how they will be addressed in order for the White Team to be both effective and sustainable. The adoption of common frameworks (such as that proposed in this chapter and report) can contribute to developing a common understanding of national strategy, goals, and pathways to accomplishing those goals.

The foundation established with the two steps above leads to the following implementation steps, again under the charge of the leading agencies:

- Adapt or create integrated implementation plans**.** No single agency has purview over the totality of the responsibilities in the M&V mission, but integration "across the seams" is required.
  - The NSS, with support from OSTP, should assess progress annually.
- Establish an institutionalized interagency planning process that evolves with the threat.
  - The nature of the M&V problem and solution spaces has changed considerably over the past decades. Undoubtedly, the challenges and proposed solutions will continue to evolve in the coming years. Therefore, not only must the analytical framework used by the White Team evolve, but the plans and priorities across the government must evolve as well.
- Enlist a wide range of contributors.
  - Historic contributors such as the DOE national laboratories remain critical to addressing the nonproliferation problem. However, the Task Force believes that the agencies should enlist a wider array of performers (other labs, contractors, academia) to address the full complexity of this problem space that will call for new, as well as improved, tools.

Chapter 5.
Improve the Tools: Access, Sense, Assess



5.1. Introduction

The second "how" in the Task Force's assessment, illustrated in Figure 5-1, addresses the "tool box" to support proliferation monitoring and verification. Figure 5-1 conveys the three principal areas for effective monitoring, each of which is in need of improvement:

- **Access**—global in a range of possible environments;
- **Sensing**—through radiation detection, post-event collection and analysis, and application of new modalities;
- **Assessment**—involving exploitation of massive and disparate data sources.

Further, as illustrated in Figure 5-1 and discussed earlier in Chapter 1, integration and iteration of monitoring results, within and across the full scope of monitoring environments, will be required if monitoring is to support verification.

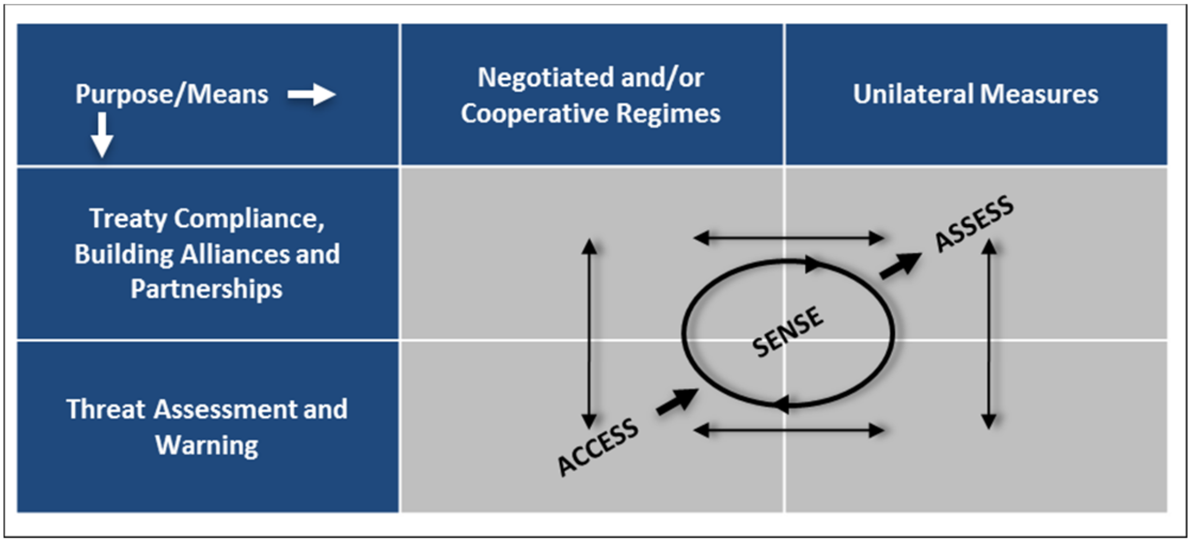


Figure 5-1 Improve Tools: Both Cooperative and Unilateral Measures Rely on Monitoring Tools to "Access-Sense-Assess-Iterate"

5.2. Access Globally

Improving access is essential for making progress against the low and/or obscured signal of incipient proliferators. A principal benefit of expanded cooperative regimes, as discussed in Chapter 2, is the access it affords. However, many scenarios could require access in areas where access is difficult. Improvements across the board are needed.

5.3. Sensing: Radiation Detection

The detection of radiation emitted by enriched uranium or plutonium coupled with the identification of the source of the radiation has been regarded as the gold standard for monitoring SNM in process, in transit, and in storage; as material to be manufactured, as components for, or integrated in reactors or weapons, as spent or retired material. The radiation usually comes in the form of gamma rays and thermal or fast neutrons. There are a number of different detector systems in use and many more under active research and development. This section of the report describes the range of technologies and applications being pursued, as well as the role of the several government agencies that develop or use radiation detectors.

5.3.1. Applications and Limitations

There is a wide range of potential applications for radiation detectors in the general area of monitoring and verification. Such detectors play an integral role in treaty verification. They are an essential element of on-site inspections for treaties and IAEA–type inspections. They are used to confirm nuclear material types and inventories under bilateral or multilateral agreements below the formal level of treaties. They are required for scanning at border crossings and ports, and are the confirming step in any search for suspected hidden SNM or weapons.

The detector technology of choice is dictated by several factors. Most importantly, the laws of physics and the limits of engineering art set bounds on what can be detected in various operational scenarios (see Figure 5-2). Detection and identification are relatively straightforward when access to potential sources of SNM is relatively unconstrained by distance or time. However, this is usually not the case. More often the detector system, including data processing and display, needs to be portable, relatively low cost, and easily operated in stressing environments with limited access. In every important application there is a trade-off that must be made among all of the possible characteristics that would be possessed by the ideal detector.

Material	Shielding	Distance (m)*	Distance (m)*
		Neutrons	*Gammas*
12kg HEU	3cm Tungsten	0.2	<0.4
4kg Pu (weapons grade)	3cm Tungsten	25	<0.6
** The distance quoted is that at which the passive signal equals the nominal background rate for handheld/backpack detectors.*			

Figure 5-2 Physics of SNM Detection

5.3.2. Detection of Special Nuclear Materials (SNM)

Detection of SNM can be accomplished passively by measuring natural radiation from the isotope in question, or actively by bombarding the isotope with radiation probes and measuring the resulting emissions. Passive detection is often limited by the low intensities of naturally occurring radiation from the source, the interference produced by background radiation, and the obscuring effects of shielding (including self-shielding in the object). Active detection usually has a much higher signal to noise ratio but requires complex interrogation equipment (frequently large and expensive) and often involves radiation safety issues. In addition to the passive or active question, detector design entails choices on a wide range of characteristics: cost, size, portability, radiation probe (for active detection), sensitivity, efficiency, energy resolution, discrimination, directional capability, imaging features, and features tied to the operational scenario of interest.

5.3.3. Status of R&D for Various Applications

The science and practice of radiation detection is many decades old and the most commonly used detector materials have changed little for much of that period. The field was somewhat rejuvenated after the end of the Cold War with the potential for new treaties as well as the goal of accounting for SNM throughout the world. The events of September 11 accelerated the need for new detectors and in particular, broadened the need for technologies that could detect hidden SNM in a variety of environments. Many of those new approaches and instruments are still in the development stage, but it is likely that a modernized set of detectors will be deployed during the coming decade. In all cases, these represent quantitative but evolutionary improvements in capability rather than revolutionary new techniques that overcome longstanding range limitations. Nonetheless they will greatly enhance the ability to monitor ports, border crossings, and vehicle cargoes for hidden SNM. What remains elusive is practical detection schemes at ranges greater than 100m and identification of illicit activities involving SNM.

There are copious reports summarizing the state of the art and future research directions in radiation detection.[27,28,29] Instead of repeating and summarizing the extensive discussions found in those documents, the Task Force chose to summarize the status of radiation detection technology for the main applications of interest and refer the reader to those documents for much of the background technical information.

Close-in Monitoring of SNM. Applications include on-site and IAEA-type inspections where close-in access is possible. In this case, there is a need for improved measurement systems for identification and quantification of SNM in a variety of material types and configurations. Examples of promising research areas include high-resolution gamma-ray spectrometers operating at room temperature; improved neutron coincidence counting and neutron multiplicity measurements; correlated measurements of fission gammas and neutrons; and advanced micro-calorimetry.

Hidden SNM at Ports, Borders, and in Vehicle Cargoes. As noted previously, a tremendous effort to develop radiation detection equipment for these applications has occurred since September 11. Passive gamma and neutron instrumentation has been deployed overseas (e.g., as part of DOE's Megaports program). The Department of Homeland Security has deployed fixed-site radiation detection and radiography equipment at U.S. ports and borders. Portable radiation search equipment has been shared with partners through the Proliferation Security Initiative. The next generation of radiation detection instruments with improved performance for these applications is in the pipeline of testing and qualification for deployment over the next several years.

Operations in Contested Areas. A variety of passive gamma and neutron radiation detectors are now available for operations in denied areas, primarily for troop protection where the presence of radiation is anticipated. Portable radiation detection equipment for aircraft and ground vehicles has been demonstrated under battlefield conditions. The concept of operations

For example:

[27] NNSA, "Special Nuclear Materials Detection Program: Radiation Sensors and Sources Roadmap," NA22-OPD-01-2010 (recommended as one of the most comprehensive)

[28] Congressional Research Service, "Detection of Nuclear Weapons and Materials:Science, Technologies, Obervations," R40154, June 4, 2010

[29] JASONS, "Concealed Nuclear Weapons," JSR-03-130(2003); "Active Interrogation," JSR-09-2-2 (2009); "Lifetime Extension Program (LEP) Executive Summary," JSR-09-334E (2009)

for these systems relies on external cueing that radiation sources could be expected in the immediate vicinity of operations. The next generation of radiation detection systems for this application may include large-array gamma and neutron detectors, passive neutron and gamma ray spectral imagers, and possibly active neutron and photon (bremsstrahlung) interrogation sources. If successfully developed and deployed—and the Task Force cautions that much work will be needed to do so—such active systems could extend the useable detection range out to ~100 meters depending on the quantities of SNM and associated shielding of the objects in question.

Finding Loose Nukes or Identifying Theater Nuclear Weapons. These continue to be the most challenging problems for detection and identification of SNM sources. As noted elsewhere in this report, radiation detection by itself will play a limited part in the solution to these challenges. A networked search and discovery architecture that includes non-radiation sensors along with near-real-time data and information fusion and dissemination will need to be developed. Radiation sensors would be engaged only during the end game when a likely location for a hidden weapon or SNM has been identified. At that point, radiation sensors would be used to identify and characterize the source before interdiction by personnel or destruction by kinetic munitions.

Longer Range Detection. Active interrogation for stand-off detection using high energy photons to stimulate fission has demonstrated detection of delayed neutrons. Interrogation distances up to 100m have been demonstrated, but detection distances have been limited to tens of meters. Long range (100m to kilometers) stand-off radiation detection and identification of SNM must await future breakthroughs. There is little chance of a deployed technical solution in the next 10 years.

5.3.4. Agency Responsibilities and Inter-Agency Coordination

The agencies with principal responsibilities for technical development as well as operational deployment of radiation detection systems are the Departments of Defense, Energy, and Homeland Security. The DoD must protect its bases and other sites, be prepared for detecting radiation sources in hostile environments, carry out on-site inspections and (ideally) detect SNM from standoff distances (> 100 m). The DOE has a myriad of different programs that involve radiation detection including non-proliferation, monitoring of material in the nuclear fuel cycle, operations at international borders and ports, and searches for suspected loose material or weapons. The DHS has the lead role in U.S.-based operations including borders and ports and for activities in public U.S. environments. There is a four-part MOU among those three agencies plus the DNI for coordination of nuclear detection R&D, and an interagency working group (IWG) led by the President's OSTP. These mechanisms help provide substantial information exchange and communication among the workers in the field and has been successful in avoiding unnecessary duplication of effort, but the diversity of technical and operational needs makes it difficult to set (or infer) overall research and development priorities. Novel concepts and new materials are continually being proposed and should be evaluated within each of the major government programs because it is possible that one may produce breakthroughs in cost and/or performance, but the Task Force found none that were sufficiently mature to warrant a major ramp-up in investments.

The major shortcomings across the federal efforts are two: (1) there is no integrated mechanism for setting R&D priorities across the programs or for allocating funding along such lines; and (2) operational requirements to measure the readiness of a given technology or operational system for transition to a specific application are often lacking, such that much of the radiation detection technology that is developed is never transferred to operational use. The task force believes that a more unified "national" technology roadmap can aid both the individual agencies and the efficiency of the overall federal programs. In addition, understanding the interplay between possible radiation detection capabilities and the broad range of possible (other) monitoring technologies, operations, and scenarios should be improved within both the R&D and operational communities.

5.3.5. Key Findings: Radiation Detection

The task force did not try to down-select or set research and development priorities among the various technologies since the wide range of applications often calls for differing solutions. Rather, it focused on identifying mechanisms that would enable the various agencies to do their work more effectively and also produce a better overall federal approach to radiation detection. Our specific findings are as follows:

- Operational requirements to measure the practicality and readiness of a given technology or operational system for transition to a specific application are too often lacking. As a result, much of the radiation detection technology that is developed is never transferred to operational use.
- Technology and concept of operations (CONOPs) are both workable problems for New START treaty verification. Intrusiveness and information protection must be addressed.
- Beyond New Start, the requirement for monitoring will begin to emphasize individual warhead or bomb counting; solutions that simultaneously verify the presence of a warhead without revealing sensitive classified design information will be needed.
- There are technically plausible approaches at ports and borders for detecting plutonium and radiological materials; shielded uranium requires continuing research. Several systems are currently in the pipeline for deployment during the next several years. All methods involve trades among CONOPs and cost-benefit choices, which must be resolved before deployment.
- Radiation detection will have a limited role in finding loose SNM or theater nuclear weapons; however, when a suspect object is found, radiation detectors should be able to identify and characterize it.
- Managed access at national nuclear facilities and test ranges is needed for technical and operational development of radiation detectors.

- There is little chance of a deployed technical solution for longer range (>100 m) detection of SNM in the next 10 years.

5.4. Sensing: Post Event

The Task Force was originally asked to look into capabilities for nuclear forensics but decided not to pursue the topic, with one exception, because of a focused National Academies committee which was completing its work during the course of this study.[30] The one exception was an assessment of the USAEDS, operated by the Air Force since the late 1940s. The full system, comprised of a global satellite surveillance constellation and a seismic-hydroacoustic network, coupled to the International (seismic) Monitoring System, also includes an airborne sampling system that is vectored to the area of a suspected explosion to collect radioactive debris.[31] The samples are returned to ground laboratories for detailed radiochemical analysis. The analysis can take days to weeks.

5.5. Sensing: Additional Modalities

Chapter 3 introduced the need for a significantly expanded monitoring architecture to address the challenges of both horizontal and vertical proliferation. The task force highlights here some of the particular sensing capabilities that should be assessed and/or integrated into the overall architecture.

5.5.1. The “INTs”

Many of the various intelligence collection capabilities (HUMINT, IMINT, MASINT, OSINT, SIGINT, etc.) have historically played a strong role in the detection and assessment of larger nuclear programs. Applications outside the nuclear proliferation domain in which signal-to-clutter is extremely small have been significantly improved, especially from an exploitation standpoint, during the last decade of warfighting. Crossing back into the nuclear realm and focusing on small, easily hidden or nascent programs will be important to meet the monitoring challenges identified in this report.

5.5.2. Scientific and Commercial Imagery

A major scientific and economic trend exploitable for increasing the capacity and persistence of monitoring coverage worldwide is the spread of satellite sensing capability throughout the world and into the commercial sector. Governments and nongovernmental organizations in over 50 countries now operate nearly 1,000 active satellites in earth orbit. Two hundred of those satellites are engaged in earth observation. This collection of satellites has several attributes of potential utility to monitoring:

[30] “Nuclear Forensics: A Capability at Risk,” A. Carnesale (committee chair), National Research Council, 2010.

[31] The airborne component of the system was deployed and proved invaluable in the aftermath of the Fukishima nuclear reactor disaster.

- Observation of earth from satellites is no longer just within the purview of compartmented defense and intelligence programs. Information is collected by a growing number of states and companies and shared widely for academic and commercial purposes. This makes information from space, which is relevant to arms control monitoring and proliferation concerns, more easily shareable and accepted in international fora.
- International monitoring bodies themselves are increasingly engaged in the use of imagery from space. The IAEA, for example, has established a Satellite Imagery Analysis Unit. IAEA presentations note that commercial satellite imagery is now routinely used as an integral part of the safeguards system by which IAEA seeks to monitor independently the correctness and completeness of the declarations made by states about their nuclear materials and activities.
- There is a growing body of academic and non-governmental organization (NGO) literature that uses imagery from commercial or declassified sources to analyze activities or installations of proliferation concern. This literature identifies methodologies for the employment of information from satellite systems to improve monitoring regimes and has provided crowd-sourcing techniques for the detection of activities and places of monitoring concern. These methodologies employ readily available visualization tools and historical imagery available from websites such as Google Earth. Some observers, with some hyperbole, have referred to these techniques as “a new era in global transparency.”
- Despite the funding vagaries of the commercial satellite industry, the number of commercial remote sensing platforms seems likely to grow. This growth will be accelerated by increases in hosted payloads, in cube- and mini-sats, and in new business enterprises offering innovative lift for payloads, including suborbital spaceplanes.

This proliferation of commercial remote sensing satellites does have some limitations and drawbacks:

- The increase in the volume of data and the reports of nongovernmental entities analyzing commercial imagery may introduce additional noise into U.S. and international monitoring systems. Some experts are concerned that bad data and bad analysis could increasingly tarnish or mask more reliable data. Moreover, these experts are concerned that such data and analysis would divert government professionals from more important tasks in the quest to corroborate or refute commercially derived claims.
- The greater availability and dissemination of data will constrain the ability of the United States to keep its options open in dealing with potential violations of international agreements or other threatening behavior. The distinction between the gathering of information through monitoring and the making of political judgments in the verification process will erode, and raw information gathered by commercial or international sources may become matters of public discourse that could hamper quiet resolution of noncompliant or ambiguous activities more difficult.

On balance, however, it is the judgment from the task force that more information from remote sensing systems, both commercial and dedicated national assets, is better than less information. The increase in information from commercial systems adds to the importance of recommendations, made in Chapter 3, to improve the United States ability to process and analyze information proactively and to find weak signals of threat or noncompliance even within the most cluttered and noisy environments. The ready availability of commercial imagery and other open source data also increases the ability of the United States to share or discuss data with international partners in ways that serve to protect the most perishable of intelligence sources and methods.

5.5.3. Open Source Center (OSC)

The OSC provides accessible reporting on foreign political, military, economic, and technical developments in over 80 languages and from more than 160 countries. The OSC, largely based on the former Foreign Broadcast information Service, uses open sources such as radio, television, newspapers, news agencies, databases and the World Wide Web. Within the OSC is the Counterproliferation Program (CPP) office charged to track priority CP issues through various public media. Since the establishment of the CPP in 2007, the OSC has provided, by many accounts, excellent support with limited resources to the IC's counterproliferation mission.

Open Source (OSINT)/Social Media/Networking is the area that is undergoing perhaps the most revolutionary change within the IC and across the globe. "The poor man's intelligence community" is now available to anyone with access to the Internet. The continual launch of commercial space-based sensors of every phenomenology (e.g., electro-optical, multi-spectral imaging, hyperspectral imaging, synthetic aperture radar, and eventually full motion video) has meant an explosion in source data originating from outside the national security community – which is often difficult to process, exploit and disseminate. Nonetheless, these and other geospatial (or geospatially-enabled) data are becoming increasingly available around the world, and are helping to shape and reshape GEOINT and Open Source as new modes of high-value "intelligence." Cell phones, Smartphones, tablets and other like devices are increasingly able to sense location, giving rise to a new class of applications. In this class of applications, the line between Open Source and GEOINT will become more blurred. Eventually, as all open source information becomes more anchored in place and time, one will see Open Source transform how GEOINT is prosecuted and used.

5.6. Assessment: Data Exploitation

The Task Force focused on two emerging enablers for exploiting the increasingly vast amounts of data available at the heart of the assessment function: big data analytics and crowd sourcing.

5.6.1. Big Data Analytics

A popular term for an area that is growing rapidly in R&D investments, big data refers to collections of data sets so large and complex that until recently they were impossible to exploit with available tools. One can successfully argue that the era of big data arrived quite a while ago for the intelligence and military communities with the collection of data from sensor and other sources of information that overwhelmed the capacity to exploit all, or even most, of it. Technologies are rapidly evolving commercially to enable the storage, access, computational processing, etc., of such large data sets, but will require different "data centric" architectures and more importantly, new analytical tools for exploitation. A major tradeoff—or limitation—is emerging in big data analytics with the realization that the transmission latency among storage devices in a cloud based architecture is overwhelming the processing time for computational operations. As such, the analytics need to stay near the data; i.e., in a "back to the future" sense, large banks of co-located processors will form the big data processing architecture of the near future in those cases where the data is growing and/or changing rapidly. The strategic monitoring capability argued for in this report is one such example.

5.6.2. Crowdsourcing of Commercial Imagery

The use of crowdsourcing for nuclear monitoring offers the potential of increasing analytical capabilities without necessarily a substantial increase in the funding for specially designated offices for counterproliferation analysis. For example, the Task Force believes that crowd-sourcing of commercial imagery is one avenue that should be pursued. Imagery analysts focusing on counterproliferation at the National Geospatial-Intelligence Agency (NGA) and other organizations could focus their efforts on the higher priority and time-sensitive CP requirements, while crowdsourcing could be implemented for less critical imagery analysis requirements. The viability of the concept has been tested in several recent examples.[32,33,34]

The use of crowdsourcing of commercial imagery analysis does come with one major concern identified above in the discussion of the use of commercial and scientific imagery, namely the quality of both the data and analysis. A vital part of any commercial imagery crowdsourcing process has to be a thorough "quality assurance" process. There have already been major analytical errors made by untrained imagery analysts who have published openly.

A recent article in the Washington Post about work done by Georgetown University students analyzing the network of tunnels in China to hide their missile and nuclear arsenal is a good

[32] DARPA Red Balloon Challenge (http://archive.darpa.mil/networkchallenge/)

[33] M. Fisher, "Google Maps Reveals Exact Site of North Korea's Nuclear Test, Plus Nearby Test Facility and Gulag," Washington Post, February 12, 2013

[34] C. Hansell, Cristina; William C. Potter; "Engaging China and Russia on Nuclear Disarmament," Monterey Institute of International Studies, April 2009

example of both the pros and cons of crowdsourcing.[35] Using open source information for the past several years—the Internet, local Chinese news reports, Google Earth and online photos posted by Chinese citizens—the students have published a far-reaching paper that challenges assumptions made by the IC on China's nuclear weapons capability. However, there is an extensive debate on the accuracy of this report, compiled by untrained intelligence analysts without access to classified data, which could have serious political and military implications. Many nonproliferation experts question the veracity of the report, citing how a semi-fictionalized Chinese TV series is used as one of the intelligence sources.

Whether the report is completely accurate or not, this event provides a "proof-of-concept" on how crowd sourcing can be used to augment limited analytical capacity. The IC should establish a process which codifies crowd sourcing as an additional area for research related to nuclear treaty monitoring issues, and ensure that a non-prejudicial process is established whereby open source and mainstream intelligence assessments can be reconciled.

5.6.3. Iteration: Proliferation Monitoring Management

Figure 5-1 illustrates the importance of integration and iteration in the access-sense-assess cycle. The Task Force notes that this responsibility should fall to the DNI, who bears a special responsibility for pursuing and integrating sensitive intelligence sources and methods, open-source information, and data provided through arms control-related information exchanges and inspections. In carrying out this role, the DNI can draw upon the lessons and experiences of the Intelligence Community's Treaty Monitoring Manager.

At the height of arms control monitoring in the late 1980s and early 1990s, the position of Treaty Monitoring Manager (TMM) was an effective vehicle for coordinating the work of multiple organizations and collection activities. As noted earlier in this report, the number of actors of both horizontal and vertical proliferation concern, and the increased geographic scope of activities of concern, have become too large to understand and anticipate developments of potential threat to the United States within treaty sanctioned regimes alone. The Task Force believes the TMM model could be effectively adapted to a Proliferation Monitoring Manager position with responsibilities to proactively orchestrate the collection, fusion, analysis, and dissemination of information vital to understanding the overall horizontal and vertical proliferation threats to the United States and its allies, as well as providing information relevant to verification judgments about the compliance of state parties to international agreements. This position, working with other National Intelligence Issue Managers, should explicitly act to create synergies among collection modalities and information means and to disaggregate tough overall monitoring problems into manageable problem sets. The Proliferation Monitoring Manager, as the Treaty Monitoring Manager has historically done, would play the leading role in the U.S. Government for orchestrating the timing and focus of the most sensitive intelligence

[35] W. Wan, "Georgetown Students Shed Light on China's Tunnel System for Nuclear Weapons," *Washington Post,* November 29, 2011

collection with negotiated and overt activities such as inspections, data exchanges, cooperative measures, and diplomatic demarches.

The Task Force believes that the position of Proliferation Monitoring Manager should reside in the NCPC. The Center reports to the DNI, is engaged and effective in the interagency process, and has the appropriate nonproliferation and counterproliferation coordination responsibilities. The charter for NCPC states that "it shall be the primary organization within the Intelligence Community for managing, coordinating, and integrating planning, collection, exploitation, analysis, interdiction and other activities relating to weapons of mass destruction, related delivery systems, materials and technologies, and intelligence support to United States Government efforts and policies to impede such proliferation." In pursuit of the goals of its charter, the Center has helped enable and focus military, diplomatic, and international cooperative activities and has a close relationship to those that have special authorities like CIA. NCPC draws on detailees from around the IC, the interagency, and military commands, which would facilitate the Proliferation Monitoring Manager's ability to orchestrate activities across multiple agencies, approaches, and perspectives. Elements of the Center have experience in, and a bias toward, the type of actions that this task force report advocates.

5.7. Recommendations: Improving the Tools

The "tool box" does not lack for opportunities for improvement. The Task Force recommends a number of them across the access-sense-assess-iterate spectrum.

Improving Access. The responsible agencies in the IC and DoD should rebalance existing investments and/or grow new programs in R&D to develop improved approaches for obtaining access across an array of scenarios and environments.

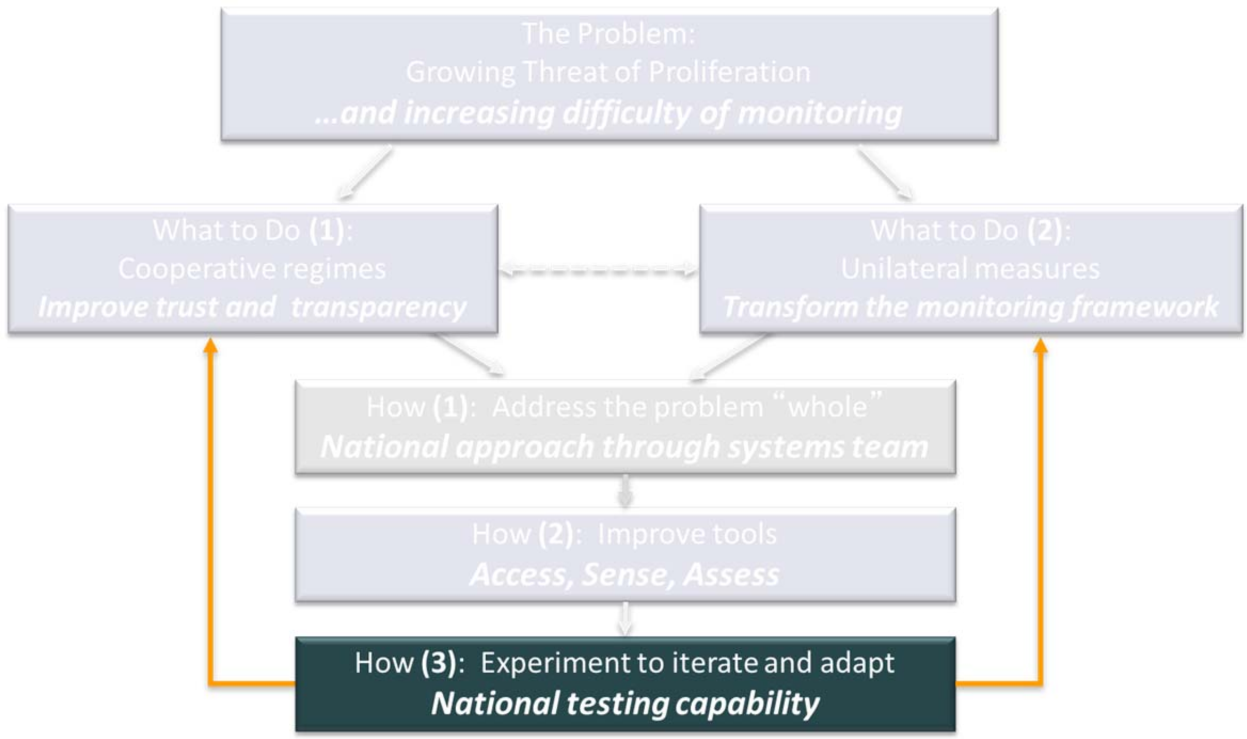
Expanded Sensing and Assessment. There are numerous aspects that deserve attention from each or all of the several agencies with mission responsibilities for nuclear monitoring, as follows:

- The DNI should provide direction to the leading agencies in the IC to:
    - Increase the profile, support, and integration for the OSC's Counterproliferation (CP) Program to collect and disseminate information and analysis relevant to arms control and proliferation issues;
    - Assess/adapt new and expanded collection capabilities for nuclear monitoring, especially through multi-INT integration and enhanced processing;
    - Expand the use of open source and commercial information to focus search areas and reduce demand on national collection assets so that the collection system can keep up better with the expansion of targeted areas of interest;
        - Continue/expand the augmentation of data from national intelligence collection systems with imagery and radar from commercial systems;

        - Develop and apply quality assurance methods for crowd sourcing of commercial imagery results;
    - Ensure that DoD's activities for improving global indications and warning leverage existing sources of information and capabilities, and develop the analytics to produce actionable nuclear-related threat warnings;
    - Adapt the Treaty Monitoring Manager's role to one of a Proliferation Monitoring Manager, "home based" in NCPC, with orchestration and integration responsibilities to assess both horizontal and vertical proliferation.
- DOE/NNSA, DHS/DNDO, DoD/DTRA and the IC should build upon the existing MOU to improve coordination and execution of their respective radiation detection programs to:
    - Conduct systems studies and engage operators early in development to improve transition of radiation detection advances to the field;
    - Ensure that developers and users agree in advance on system concepts, measures of success and levels of readiness for the principal technologies and operational scenarios of interest;
    - Focus new efforts on accelerating development of research with near-term payoffs, and investment in longer range technologies that can meet both technical <u>and</u> operational feasibility requirements;
    - Develop managed access to nuclear facilities and test ranges by all involved agencies at which detection technologies and operational approaches can be explored using real SNM;
    - Agree on investment strategies. There should be supporting inter-agency roadmaps to integrate efforts and focus crosstalk. Annual inter-agency reports to the NSS should be issued to track progress and enhance information flow.[36]
- DOE/NNSA, DTRA, and the IC should rebalance existing investments to grow new programs in R&D that expand activities and the supplier base to include adaptation of conventional warfighting ISR advances: e.g.,
    - Engage in planning and capabilities development, especially for data collection and fusion functions, for DoD's efforts to improve nuclear situational awareness;
    - Support transition of multi-INT fusion and exploitation tools to nuclear monitoring applications;
    - Ensure activities related to nuclear weapons and materials monitoring are guided by the "White Team" function as discussed in the previous section and Chapter 4;
    - Make explicit the requirements for, and improvements needed in, HUMINT, SIGINT, cyber, OSINT, etc., to support monitoring and verification.
- NSS should monitor closely and persistently the resourcing to modernize the USAEDS with the help of the VCJCS-, who should ensure its modernization is supported in AF budgets.

[36] An excellent recent example of this is the "Nuclear Defense Research and Development Roadmap. Fiscal Years 2013-2017," National Science and Technology Council, April 2012.

Chapter 6.
Experiment to Iterate and Adapt: National Testing Capability



6.1. Introduction

The last of the "hows" important to comprehensive and effective proliferation monitoring is the ability to experiment with both existing and new capabilities in response to—or ideally, in anticipation of—an increasingly wider range of proliferant strategies and tactics. The Task Force addressed three inter-related topics related to experimentation: 1) a national testing capability for supporting experimentation; 2) a sample problem description of monitoring dual-capable nuclear forces (including warhead counting for arms control treaties) where the need for experimentation seems clear; and 3) use of the testing capability to develop capabilities for monitoring dual-capable systems.

6.2. National Testing Capabilities

Any argument for a national testing capability should provide answers to five important questions: (1) Why are national M&V testing capabilities needed? (2) What should they consist of? (3) What would be done using them? (4) Why do we think the national approach would work? (5) What should be done to get started?

6.2.1. Why is a National Testing Capability for Monitoring and Verification Needed?

There are many inter-related reasons. The comprehensive monitoring regime the Task Force proposes is a system of systems that must work together, and is too complicated to plan/assess on paper and/or with piecemeal testing. Furthermore, experience shows that operators typically learn to use actual monitoring systems differently and often better than system design/analysis would predict. Two examples illustrate the point:

- Past experience in radiation detection operations; e.g., Operation Morning Light (the 1978 deployment to search for and recover debris from a reactor-powered Soviet RORSAT that re-entered in northern Canada); and Navy experience in detection of shipboard nuclear weapons. In both cases, operators learned to reject clutter and spurious signals by identifying patterns inherent in their own operations and/or in the larger context. For example, in Morning Light, radiation signatures from the low-grade uranium-ore deposits that are ubiquitous in Northern Canada confounded the search operations in the first days. But operators identified the source of the spurious signals, and learned that the radiation signatures from these deposits rose and declined more slowly, as the search platforms flew across the terrain, than the radiation signatures of the point-targets they were looking for, and could be sorted out on that basis;
- Recent experience in the development of new-generation tactical ISR in the Counter IED fight discussed elsewhere in this report; learning from operational experience in Iraq/Afghanistan ("on the job training"), has been coupled with iteration in experiments in various DoD testing and training facilities (e.g., the National Training Center [NTC]) to not only train deploying units but also to anticipate next steps in adversary tactics, techniques and procedures (TTPs).

The need to learn from experimentation and experience is even greater in the areas addressed by this Task Force, where an adaptive adversary and/or one with sophisticated denial and deception is likely to be involved.

The advantages of a testing capability are many and compelling. It would or could:

- Provide a focal point for planning, iterating/adapting, and operating the system of systems;
- Help integrate the technically disparate and organizationally disaggregated activities that comprise the national monitoring system;
- Better couple developers and users and provide an experimental basis for net assessment and risk management;
- Provide ground-truth performance metrics for technologies and operations, in part as a basis for future spirals;
- Stimulate sorely needed new ideas;
- Expose "subcritical" programs because planning experiments would force development of concrete requirements and CONOPs;

- Elevate attention to red-teaming of monitoring systems.

On a broader scale, it could help build international understanding and cooperation on monitoring systems. In particular, testing operations could be a vehicle for confidence building and transparency assessment and promotion, and could also contribute to dissuasion and deterrence.

6.2.2. What Would a Testing Capability Consist Of?

The testing capability would have four interdependent parts: 1) the ranges and facilities (real and virtual); 2) the information/data management systems (data flows from and to sensors, information flows within the analysis/fusion systems, and command/control data/information flows); 3) a standing "White Team"; and 4) a standing Red Teaming activity.

The ranges and facilities would consist of a distributed, netted set of:

- Operating real-world facilities (e.g. PANTEX, a power reactor, port of New York, SFO, the URENCO enrichment plant);
- Real test facilities (e.g. NTC, Nevada National Security Site [NNSS]) with space for large-scale operations and/or use of radioactive materials;
- Simulated facilities/operations.

This set of facilities and networks would eventually cover the full range of nuclear threat and treaty-related capabilities and activities, including: labs, production, industrial base, distributed weapons and materials storage, deployment, distributed field operations. The set would also be broad enough to bring into play "patterns of life" in peace, crisis, and perhaps war. The facilities should include remote areas, areas like "the South Bronx", air, and at-sea operations. There should be the capability to use real SNM. Some facilities and ranges might be overseas, including facilities that would be the actual subject of monitoring in future treaties.

Information and data flows are the second crucial part of the testing capability because they comprise the essence of monitoring. The monitoring system itself is about information; monitoring the data/information flows in treaty-partner and/or adversary systems and operations is a crucial function of the monitoring system. The testing capability must thus include both blue and (hypothesized actual or simulated) red information/data management systems and networks. Such information/data systems—real or simulated—can be very expensive, and their development and iteration very time-consuming. Fortunately, rapid prototyping, testing capabilities, and iteration for such data management systems have been developed for other applications. It appears possible to readily adapt such testing for the information management aspects of the nuclear monitoring testing capability. Moreover, the testing capability systems can evolve to become the actual operational systems.

The third integral part of the testing capability would be a standing analytical "White Team" that would use the scenario-generator and scenario-to-asset planning approach (see Chapter 4) to guide exercises/experiments, assess implications of testing and training results, and identify needed changes/improvements for the next cycle. It would provide a simulation capability and translate test results to deployed monitoring operations. The information management aspects of the White Team activities would eventually become part of the real world ops center for the comprehensive nuclear monitoring system of systems.

The fourth essential element of the testing capability would be a standing Red Teaming activity. Red teaming would include active R&D on means by which adversaries could (or do) evade threat-assessment monitoring and by which treaty partners might evade treaties and treaty-monitoring, including by deception and denial. A key step would be to rebuild a national nuclear threat assessment capability, principally but not exclusively with the National Labs, that anticipates "nth group" weapon designs, development, and production approaches (as discussed in Chapter 3). The services and certain combatant commands (COCOMs) could explore ways in which nth-countries might deploy, operate, and employ nuclear and dual-capable weapon systems and forces. The White Team would referee red-teaming, for example by specifying the levels of technology, or degree of knowledge of U.S. systems, that might be attributed to various actual or simulated adversaries.

6.2.3. What Would Be Done Using the Testing Capability?

The testing capability would eventually cover the full range of experiment, test, demonstrate, exercise, and train, through multiple cycles of learn-iterate-adapt. The testing capability could be used to explore very specific detailed topics, like improved CONOPS for a particular type of advanced sensor, and very general questions, like the interplay between transparency and stability. Each experiment would use a few or many of the types of facilities and capabilities that are part of the testing capability. The exercises, tests, etc., would explore the full scope of current and possible future monitoring applications: nonproliferation, counter-proliferation, countering nuclear terrorism, IAEA monitoring applications, Comprehensive Nuclear-Test-Ban Treaty (CTBT) monitoring, cooperative threat reduction, routine and challenge on-site inspections, negotiated over-flights (Open Skies done right – see Chapter 2), and confidence-building measures.

The exercises and experiments would be sponsored by all relevant USG agencies, occasionally singly but more often jointly. In certain important cases there would be international participation, partly for confidence-building purposes or ideally, as an integral part of the phased strategy for cooperative regimes discussed in Chapter 2. There would be red- and blue-teaming, in multiple forms.

6.2.4. Why Does the Task Force Think the Testing Capability Would Work?

Almost all successful developments of major systems of systems have used testing capability development and iteration. DoD in particular has a long history of using testing and experimentation, augmented by simulation, to develop successful systems. The near real time experiment-iterate-adapt cycle for countering IEDs simultaneously developed technical capabilities (e.g., ODIN & MAD DAWG) with CONOPs. Earlier, during the Cold War, there were key developments in which test-beds used in conjunction with operational experience led to important improvements in theater weapons, forces, and their CONOPS. These included:

- “Shockwave” in the North Atlantic Treaty Organization (NATO) Central Region during the 1970s and 1980s (see the next section of this chapter for a more complete description);
- SORAK (N.E. Asian theater)[37];
- Pershing IA and ground launched cruise missile (GLCM) endurance experimentation during the 1980s[38];
- Horizontal and vertical dispersion of dual-capable aircraft (DCA) to improve theater nuclear force (TNF)-DCA force endurance.

Major force component assessments and requirements have also been developed using test-bed approaches, including the Navy’s submarine survivability program and the Air-Land battle command robustness.

The nonproliferation and arms control community is not a stranger to such approaches, although systems integration and experimentation are not as common. For example, Sandia’s Technical On-Site Inspection (TOSI) site was used effectively to develop on-site inspection approaches.

6.2.5. What Should Be Done to Get Started?

The first application of the testing capability should be one for which progress would address a major shortfall in current capabilities and possibly open the door for new arms control agreements. Monitoring dual-capable/TNF weapon systems was selected as a leading example for these reasons. The challenges for monitoring TNF systems are discussed in the next section, followed by ideas for getting started on learning how to monitor them using the testing capability in Section 6.4.

[37] SORAK was a South Korean experimentation concept developed in the late 1970’s and early 1980’s based on Shock Wave. It was sponsored by Commander-in-Chief, U.S. Pacific Command (CINCPAC) and supported by DARPA, as part of the joint United States- South Korean exercise Ulchi Focus Lens. The concept was intended to create an all source testing capability to observe operations.

[38] Pershing II and GLCM operations were driven by the need for survivability in moving units out of peacetime garrison in crisis and in move-and-hide tactics in the field in crisis and war. These operations were developed iteratively using red-teamed test-bed exercises coupled with simulations, both in CONUS and in Europe.

6.3. Monitoring Dual-Capable Nuclear Forces, Including Warhead Counting for Arms Control Treaties

Monitoring dual-capable (nuclear and conventional) systems is of interest in its own right, but it also epitomizes other monitoring problems. It illustrates the synergies among the four elements of the Task Force's basic 2x2 matrix of Figure 1-2, which encompasses the full scope of the monitoring regime; i.e., monitoring for the purpose of treaty-compliance and monitoring for threat assessment, within the context of both negotiated and/or cooperative monitoring agreements and non-negotiated/unilateral monitoring.

All nations that have nuclear weapons, except for the UK, have dual-capable (DC) weapons, and many of these nations, including recent proliferators, have only dual-capable nuclear systems. It is likely that most potential future proliferators (Iran, etc.) will use dual-capable platforms for their initial, if not longer term, nuclear capability.

There is a wide range of dual-capable weapon-system types:

- Air forces: gravity bombs, air-launched cruise missiles, air-to-air missiles, defense suppression missiles.
- Ground forces: anti-armor infantry weapons, tube artillery, surface-to-surface missiles, air defense missiles, demolition munitions; some are dual-role (e.g., surface-to-air and surface-to-surface).
- Naval forces: surface-to-surface missiles, air defense missiles, ASW weapons, torpedoes
- Special forces weapons

We have also seen that some nuclear warheads may be dual-use (i.e., strategic and TNF), adaptable both ways.

It is important to take into account that most proliferators will rely on "hiddenness" and uncertainty in general, for their nuclear systems survivability. The survivability provided by hiddenness and uncertainty tends to enhance crisis stability but exacerbates the difficulty of monitoring and verification for both arms control and threat assessment. The net effect may be that the risk of miscalculation by current or potential future adversaries increases, and overall strategic stability over the long term decreases. How transparency, certainty and uncertainty, and stability interact, for good or ill, is an important issue that deserves more systematic thought than it has received to date. Dual capability is an integral part of this question, because of the uncertainty about whether any given delivery platform may be armed with, or destined to be armed with, a nuclear weapon.

To be effective, monitoring of dual-capable forces must cover the full spectrum of activities: design, production, storage, and deployment; during both peacetime and crisis/war operations; for both nuclear warheads and DC systems. Understanding this complete set of activities—i.e., the "pattern of life" for dual capable systems—illuminates each individual part, including parts that may be relevant to treaties, but also paints a much broader picture of nuclear capability. An increasingly serious problem is that U.S. de-emphasis of dual-capable systems narrows our frame of reference for monitoring and verification of others. The result is a limited range of opportunities to test monitoring systems against our own dual-capable systems, and the roster of people who understand the possible patterns of life of DC systems, based on their own experience with them, is shrinking rapidly. It is a central theme of this report that there are synergies that should be amplified and exploited between monitoring for arms control purposes and for threat assessment, and between negotiated/cooperative monitoring and monitoring means that are not negotiated and not explicitly cooperative. These synergies are illustrated, in more specific terms, in the case of monitoring for dual-capable systems, in Figure 6-.

Means → / Purpose ↓	Negotiated and cooperative Close access (peacetime)	Unilateral Measures Integrating NTM, Theater Intel, Tactical ISR (peace, crisis, war)
Treaty Compliance, Building Alliances and Partnerships Non-compliance ↓	**Countering TNF warheads:** ▪ Inspections at agreed locations ▪ Tagging ▪ Area/perimeter constraints ▪ Challenge inspections ▪ Other measures??? ←	**Locating and counting warheads not declared or not at agreed locations**
Strategic warning Threat Assessment	Understanding intent ↔	**Understand sequence from design to use:** ▪ Warheads (design, production, industrial mobilization) ▪ Systems (design, production, industrial mobilization potential) ▪ Doctrine and exercises ▪ OOB Operations—peace, crisis, war ▪ Conventional, Nuclear

Figure 6-1 Dual Capable (DC) Theater Nuclear Forces (TNF) - An Example to Illustrate Synergies in our Approach

One can observe that:

- Knowledge of warhead inventories gained from treaty monitoring contributes to threat assessment. Verified or even suspected non-compliance with treaty limits would represent a form of strategic warning in the threat assessment context.
- The objective of threat assessment is to know everything relevant about the force structure, order of battle, development life-cycle and operational patterns of life in peace, crisis, and war, for both warheads and systems. Much of this knowledge would

also be needed in order to assess whether warheads were being withheld from the treaty-prescribed counting-process.

- Negotiated limits on numbers of warheads narrow the range of uncertainties in understanding of the overall TNF/DC posture for threat assessment purposes.

Some of the monitoring means that might be involved in the space of Figure 6- are shown in Figure 6-, a version of the same basic framework.

Means → / Purpose ↓	Negotiated and cooperative Close access (peacetime)	Unilateral Measures Integrating NTM, Theater Intel, Tactical ISR (peace, crisis, war)
Treaty Compliance, Building Alliances and Partnerships Non-compliance ↓	▪ Count declared w/hs at declared sites ▪ Verify absence at non-allowed sites ▪ Monitor agreed boundaries ▪ Challenge inspections ▪ Specified overflights	▪ NTM/NMM ▪ Shockwave-like operations ▪ ODIN-like systems ▪ Covert UGS ▪ Covert tagging ▪ Crowd-sourcing ▪ Attaches ▪ …
Strategic warning Threat Assessment		▪ Haystack-like analysis ▪ "Patterns of life" ▪ Nth Country's nuclear designs

Figure 6-2 Dual Capable (DC) Theater Nuclear Forces (TNF) - Some Specific M&V Approaches for Monitoring

In the upper left corner of this graphic, the Task Force posited five possible elements of a treaty involving counting TNF warheads. On the right side, a few candidate monitoring means for both complementing the treaty-allowed monitoring means and for monitoring for threat assessment are listed. While the Figure suggests a clear distinction between methods applicable to Treaty Compliance (top row) and Threat Assessment (bottom row), in reality, the methods are applicable across both.

"Shockwave" (mentioned in the previous section) was a comprehensive, successful, TNF-related threat-monitoring/understanding effort that ran from about 1978 to about 1985. It is discussed here as an effective antecedent of future, comprehensive TNF threat-monitoring systems which would benefit from improved technologies and possibly from negotiated limits and monitoring. The purpose of Shockwave was to understand improvements in the ability of the Soviet/Warsaw Pact (WP) to execute a swift, successful campaign inside U.S. and NATO timelines for nuclear employment, and thus to aid selection among U.S. and NATO options to counter those improvements. It used a wide range of U.S. national, theater, and tactical monitoring means, from both the Army and Air Force, as well as similar Allied means where appropriate. The Defense Advanced Research Projects Agency (DARPA) and the Defense Nuclear Agency (DNA) were major players in developing new monitoring capabilities. Exercises using NATO forces were used to elicit responses in later WP exercises that could be observed by Shockwave assets. The effort was led by successive SACEURs, with integration at both Supreme Headquarters Allied Powers Europe (SHAPE) and United States European Command (EUCOM) headquarters. Over the 7-8 years it was run, Shockwave was highly successful. In fact, it serves as a premier example of how persistent, comprehensive monitoring for threat-assessment purposes can pay off.

Shockwave involved development and use of persistent (for its time), relatively wide-area (for its time), aircraft-based, multi-sensor, monitoring systems, combined with many other approaches to gaining understanding. There is a direct evolutionary path from those systems to the kinds of systems used, recently and currently, for more-persistent, wider-area monitoring to suppress the IED threat in Iraq and Afghanistan. One such recent system was ODIN. ODIN-like systems, in turn, could be adapted and extended for a future, Shockwave-like effort for monitoring dual-capable systems (as well as for other purposes, including wide-area search for "loose nukes"). Integrated with such systems could be a wide range of other things including covert unattended ground sensors, covert tagging, and crowd-sourcing for gaining patterns-of-life information. The ODIN concept has been conceptually adapted for nuclear monitoring; the operational concept demands close access for detection consistent with the discussion on radiation detection in Chapter 5.

We have focused here on monitoring of dual-capable systems both because they are relevant in their own right, for future treaties and for threat assessment, and because other M&V problems share aspects of the DC/TNF M&V problem. For example:

- Monitoring the IAEA Additional Protocol, which would allow access to undeclared nuclear facilities, is similar to the problem of finding undeclared warheads;
- Awareness of the early stages of proliferation and monitoring weapon production are similar to understanding the dual-capable weapon system development and deployment life cycle.

6.4. Use of the Testing Capability for the TNF-DC Problem

The ODIN system of systems became effective for IED suppression because its users were forced to learn from experience in the real world, including from many initial failures where people died. Nuclear monitoring systems for both treaty-monitoring and threat-assessment will not have the same plethora of daily, high-stakes, real-world events from which to learn. An essential part of developing and iterating these systems toward success must be providing frequent learning experiences using the test-bed approach we discussed above. We close by returning to that subject.

As introduced earlier in this chapter, the first use of the national M&V test-bed should be for both arms-control and threat-assessment monitoring of dual-capable systems. The key is to start small in both the scope of the facilities/ranges involved and the complexity of the scenarios, and then grow in both dimensions as national monitoring capabilities grow and need to be integrated. The goal should also be to start soon—the problem space is too complex to be designed perfectly a priori.

As a first step, DTRA should analyze use of wide-area, persistent ISR/reconnaissance, surveillance, and target acquisition (RSTA) for monitoring of dual-capable systems to support both treaty-monitoring and threat-assessment. Pros and cons should be developed comparing various applications of this first step, including for example, future warhead-counting treaties, assessment of Russian dual-capable systems in general, and assessment of China's DC systems along the Taiwan Straits.

Based on that analysis, the next step should be to plan, jointly among DoD, DOE, and the IC, a first, relatively simple experiment in detail; for example, using an ODIN-like system to find a single dual-capable platform operating in "move-and-hide" mode, at NTC and/or NNSS. (The latter would allow experimentation with real SNM signatures.) This would be a relatively low cost initial effort, but it would get started on an important problem. Even this first small step should involve red-teaming, and should be planned by the White-Team using the scenario-generator described in Chapter 4. Various sensor mixes and adaptive sensor/platform CONOPs, posited by a "solutions team" also described in Chapter 4, should be explored. The product should be a well-understood design for one component of the future nuclear monitoring system of systems, along with options for operating that component.

Following success with this single-focused monitoring application, the experimentation campaign should add two, three, and more elements of the "pattern of life" for the red nuclear enterprise. The results should not only inform CONOPs development, but also identify intelligence gaps where collection assets might be focused.

For all of the above, it will be important to partner with at least one geographical COCOM, and to be guided by a steering group of military and technical experts who have made such undertakings a success in the past.

6.5. Recommendations: National Monitoring Testing Capability

The Task Force believes that even with substantial investment in all other elements of its proposed "whats" and "hows", the U.S. will likely see only marginal improvement in monitoring capabilities without the national testing capability. While the idea of "testing capability" could suggest an expensive undertaking, the Task Force has been careful, as it has in other parts of this report, to make recommendations that build upon existing capabilities or shift investment priorities within existing portfolios. In the case of the testing capability, the communities should make maximum use of existing capabilities in ranges, equipment, and development programs (both hardware and software) that already exist. It is the integration and application of such capabilities to the "paradigm shift" in monitoring that is important for learning and making progress in addressing the proliferation problem. In fact, the Task Force believes that its "get started" plan can be undertaken without substantial new investment outside of intellectual capital. To that end, the Task Force recommends that:

- DoD/DTRA, in partnership with DOE/NNSA and the IC, develop a comprehensive "iterate and adapt" national testing capability which:
  - Provides a focal point for planning, iterating/adapting, and operating the system of systems;
  - Helps integrate technically disparate and organizationally disaggregated activities.
- The testing capability should include the following elements:
  - Red and blue teaming, in multiple forms, to include engagement of allies in various red and blue roles;
  - Realistic physical and virtual environments;
  - White Team (as recommended in Chapter 4); i.e., a strong analytical component to assess the implications of test results and feedback into the cycle needed changes/improvements.
  - Support from DOE, working with NCPC, to rebuild a national nuclear threat technical assessment capability, principally but not exclusively with the National Labs, that anticipates "nth group" designs, effects, employment and deployment approaches and observables.

Chapter 7. Summary and Conclusions

The Task Force's mandate was broad, as specified in the Terms of Reference. As such, many topics did not receive the in-depth look that would help executing organizations with more explicit recommendations on priorities and get started actions. For example, the Task Force fell short in providing explicit recommendations for:

- Defining specific steps for the long term cooperative engagement plan;
- Assessing more thoroughly the opportunities and "dry holes" in applying conventional warfighting ISR capabilities;
- Assessing the current and desired information flows and integration for early detection of proliferation;
- Recommending in greater detail improvements in collection and analysis carried out by the IC as part of the overall monitoring plan;
- Advancing materials monitoring and safeguarding technologies;
- Creating and sustaining the "White Team";
- Developing a national RDT&E program for improving and fielding radiation detection systems;
- Defining the specific requirements and implementation path beyond the initial step recommended in the report for a national testing capability.

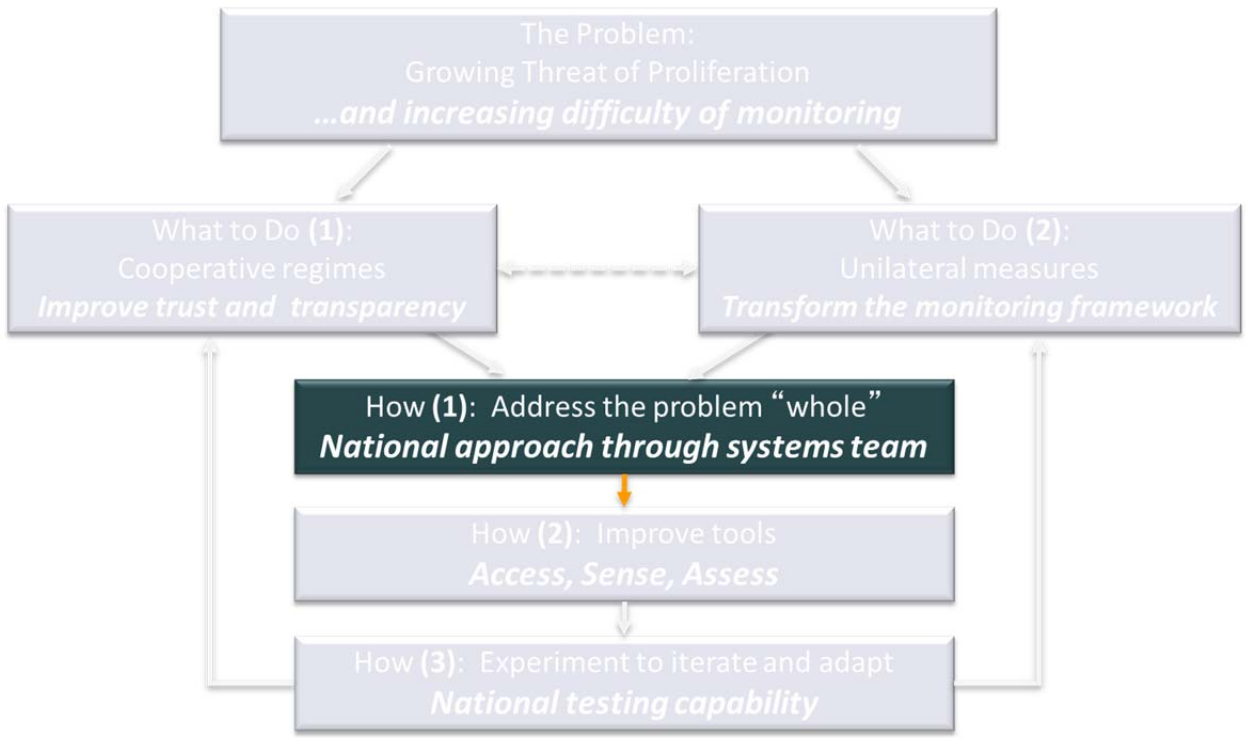
That said, the Task Force believes the comprehensive look it provided is both needed and timely. The topic has not been previously addressed in anticipation of the nuclear monitoring and verification demands that the nation is likely to face in the future. While difficult to predict, that future seems poised to present challenges unlike any faced with the experience base derived from historic nonproliferation and arms control treaty regimes. This is due to a number of reasons highlighted throughout the report, but what to do about it forced the Task Force to ask whether simply doing better at what we already know how to do would be sufficient. The answer the Task Force came to was "no". Instead a combination of evolution and innovation is called for.

In that context, the Task Force admonishes leadership not to repeat shortcomings of the past where monitoring technology and verification efforts were tied to the treaty or the proliferation problem immediately at hand, and then declined when that problem had been addressed or had diminished in perceived importance. The problem of managing the global nuclear environment for stability will be with us for a very long time. The best bet for making progress is a sustained effort in which experienced and competent professionals can devote their careers to the quest and pass on their wisdom to successive generations.

Success in this long and important effort is not guaranteed, considering the difficulty of the future monitoring challenges. But progress can be made, building on successes of the past against equally daunting problems, and on experience with prudent hedging strategies and programs.

—APPENDICES—

Appendix A. Unabridged Description of a Proposed M&V Analytical Methodology



Chapter 4 presented a candidate analytical methodology for prioritizing among the many operational and acquisition options to advance the nation's monitoring and verification capabilities. A more complete description is provided in this appendix.

A.1. Elements of an M&V Analytical Methodology

There are several key elements proposed as a necessary part of an enduring M&V analytical methodology, as laid out in Figure A-1.

- First, there is the "problem space", which consists of a set of frameworks that describe the M&V challenge independent of any proposed solutions. This is a critical component in the proposed approach, as it provides the basis that will serve as a common foundational understanding for solutions to be built upon and assessed for fitness.
- Second, there exists a "solution space", in which proposed capability architectures are crafted. These architectures are collections of technologies, operations, and capabilities

that work together to accomplish the goals and objectives identified through examination of the problem space.

- Third, there must be a Bridging Methodology which allows for the "back and forth" between requirements and objectives that any solution must meet, as dictated by the frameworks that describe the problem, and architecture features and assessments of the solution space that are mapped into the analyst's understanding of the problem itself.
- Finally, there must be a rigorous and repeatable portfolio decision methodology that allows for the values of the decision maker and his/her organization to be incorporated, and for defensible, tractable decisions to be made.

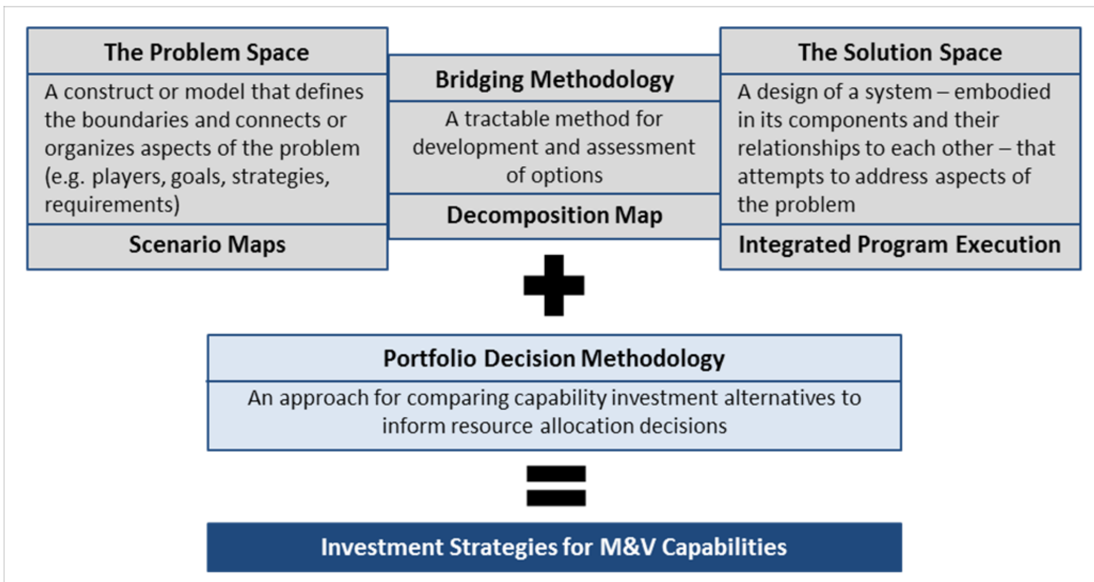


Figure A-1 Elements of an M&V Analytical Methodology

A common issue in the development of analytical frameworks has been the tendency to frame the problem and solution together. The conflation of "problem space" and "solution space" brings with it several consequences. First, it tends to promote metrics and assessments that maximize elemental solution parameters such as detector performance, rather than system performance against the actual threat space, by assuming that they are proximate. Second, it tends to lead analysts to fixate on a narrower problem (such as detector performance) rather than assessing those issues in the context of the larger whole. Third, it does not enable a common understanding of the problem space itself, allowing solutions to be framed in whatever manner the solution proponent deems suitable. The entire set of symptoms run counter to enabling the decision maker to achieve his/her ultimate goal: rendering and defending a provably effective investment strategy for M&V capability development. Separating the "problem space" from the "solution space" and analyzing them independently can therefore yield benefits by eliminating or mitigating these issues.

To illustrate the point, consider that detection systems have often been placed at the forefront of the national strategy for detecting the illicit movement of nuclear threats in proliferation regimes. While undoubtedly detectors play a role in the solution, the bulk of current analytical activities are focused on detector system performance. As a result, the M&V problem of detecting illicit movements is often miscast implicitly as a detector problem. This can lead to the line of thinking that more detectors with better detector performance parameters must logically provide reduced risk – a statement that may or may not be true. More importantly, other options that do not hinge on detector deployments may in fact provide more cost effective mechanisms for risk reductions.

A.2. Proposed Problem Space Description

While there are several possible frameworks for describing the M&V problem space, the Task Force chose to use one based on scenarios. This section describes the scenario framework and its application for describing the M&V problem space. For the purposes of this effort, the following definition of scenario is used:

> *A scenario is an evolution of the world through a series of incremental events from its current status towards an outcome of interest that is specified by the analyst*[39].

Utilizing scenarios for the evaluation of potential solution sets to complex problem spaces is by no means a new idea. Neither is using scenario sets as an organizing framework for defensive architecture development across a disparate set of stakeholders. In a report that attempted to pave the way for improving U.S. capabilities to combat biological terrorism, Danzig suggested that a common set of planning scenarios be adopted by the community concerned with bio-terrorism, along with a set of metrics, and proposed four scenarios for consideration.[40] This approach had several attractive potential benefits. First, it laid out scenarios that were wholly distinct from any proposed solutions, ownership, or mission space, but instead focused on a concise model of the problem of bioterrorism itself. Second, it began to establish a consistent framework for the development and use of metrics and measures of performance. Finally, it

[39] Dunn, Lewis, *Global Shocks and Surprise: Shaping the 2030 Nuclear Future*, presented to the Joint Sandia Laboratories – University of California "Pathways to Alternative Nuclear Futures Workshop," September 2009; http://sandia.gov/nuclear_pathways/. In this paper, Dunn referred to scenarios as "shock- free surprises" that are distinct from truly "shocking surprises". Shocking surprises refer to events that may radically alter priorities of a decision maker, and that an analyst may not foresee as feasible. An M&V analytical methodology should not be exclusive of "shocking surprises."

[40] Danzig, Richard, *Catastrophic Bioterrorism – What Is To Be Done?*, Center for Technology and National Security Policy, August 2003. In this paper, Danzig stated that individual efforts tend to be unrelated to any overarching strategy, and measures of effectiveness are difficult to formulate. Danzig also observed that relevant tools and capabilities were not viewed as alternatives, or as complements, but rather as individual programs, each operating independently with resource allocations being made more in accord with bureaucratic position and power, rather than in response to the problem.

highlighted the stewardship of problem definition as a necessary and important element in the set of capabilities to combat the problem itself.

Scenario based planning approaches can also have shortcomings if not appropriately implemented. For example, while useful for highlighting specific trade-offs, a limited set of scenarios can generally only cover a small subset of the variables that an analyst might want to explore, thereby artificially narrowing the problem space. Utilizing a wide set of end-to-end scenarios can become cumbersome and difficult to assess systematically. Additionally, conclusions drawn from a narrowly defined set of specific scenarios can be fragile to "what-if" challenges, where the scenario details beyond those explored in the analysis are modulated, casting uncertainty on the results and raising the risk of invalidation. Scenario authors also run the risk of fixating on "favorite" scenarios, or those that mirror their own preferences and biases, which can prevent systematic and objective thinking. Finally, a non-systematic scenario approach can exacerbate the problem of mapping scenario details and analysis to a structured decision methodology.

Rather than utilizing a small set of well-defined scenarios with the risks and shortcomings noted above, the Task Force developed a scenario framework that attempts to encompass a large portion of the potential scenario space in order to address the totality of M&V problem complexity. A scenario framework for scenario generation and analysis is desirable primarily because it enables the examination of a family of scenarios, rather than a small set of independent and specific scenarios. It also provides a systematic method for decomposing scenarios into discrete nodes and linkages, and capturing the interdependencies between individual scenarios. Finally, it lays the foundation for a bridging methodology, or systematic mapping between the problem space and solutions space, that enables increased traceability between planner objectives and solution performance.

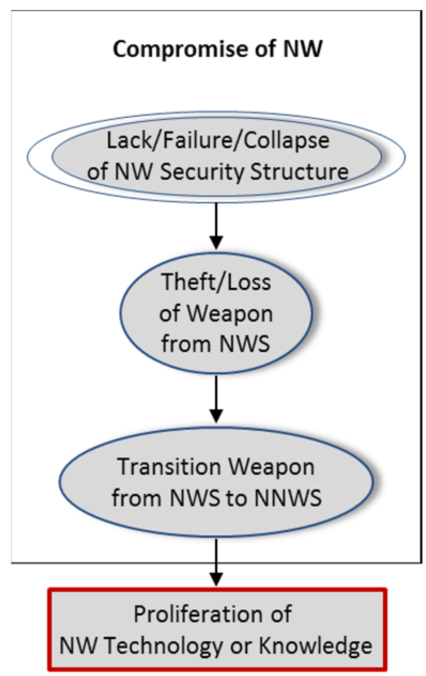


Figure A-2 Example Node Sequence

In constructing an example scenario framework, the study team began with a simple premise: a scenario is a linear series of events can be broken down into discrete nodes and associated linkages, and systematically analyzed, node by node. **Error! Reference source not found.** shows a simple sequence of nodes within the framework to illustrate these concepts. In this example, the failure of a nation's NW security structure (e.g. compromise of storage site security, material stolen by an insider) begets an evolution of subsequent scenario actions. Such a failure could lead to the theft or loss of a weapon from the custody of a nuclear weapon state. This theft could lead to the transition of a weapon to a non-nuclear weapon state, thereby proliferating not only weapons possession, but also technology and knowledge.

Each scenario node could play an elemental role in many other scenarios – e.g., the theft of a weapon could be a common step in several distinct scenarios. The nodes are therefore linked in a network of connections that becomes a framework for systematically developing and analyzing an entire family of scenarios in the M&V problem space. Figure A-2 illustrates the complete scenario framework, rotated to fit the page, while Appendix B provides a larger view of the framework.

As shown in Figure A-3, scenarios generally evolve as one traces from top to bottom, following the directed graph towards consequences. The left side demonstrates scenarios that can lead to movement of weapons themselves from NWS to other actors. The center details scenarios that can lead to the proliferation of NW technology and knowledge, and the right hand side covers compromise of weapons usable nuclear material (WUNM) and associated technology. The long vertical chain in the middle-right illustrates the evolution of non-state actors towards unconventional attack with nuclear weapons. Consequences in the scenario framework include blackmail, attack, or simply the emergence of a new nuclear-armed state.

Within the scenario framework, blue-colored nodes indicate “macro” nodes, or nodes that are easily decomposed into a common set of sub-nodes. For the purposes of this work, the only set of sub-nodes explored is the “movement sub-space.” This sub-space corresponds to movement through the origin region, across international boundaries, through global commons, and into the target region. The movement sub-space is laid out in the blue box on the right hand side of the framework diagram.

Real-world events could easily be interpreted as a signal that a scenario in the framework is playing out, although there is actually no nefarious activity. It is very important to consider these degenerate scenarios, in addition to actual threat scenarios, when analyzing potential solutions as it is likely the bulk of actual signals and information will be from situations that are not actually leading to nuclear attacks. For example, the nuisance alarm problem in radiation detectors that are monitoring commerce streams plays a large role in the overall cost, effectiveness, and operation of those systems. Operational and analytical understanding of such false positives leads to an understanding of the full suite of information and analysis required for high confidence detection.

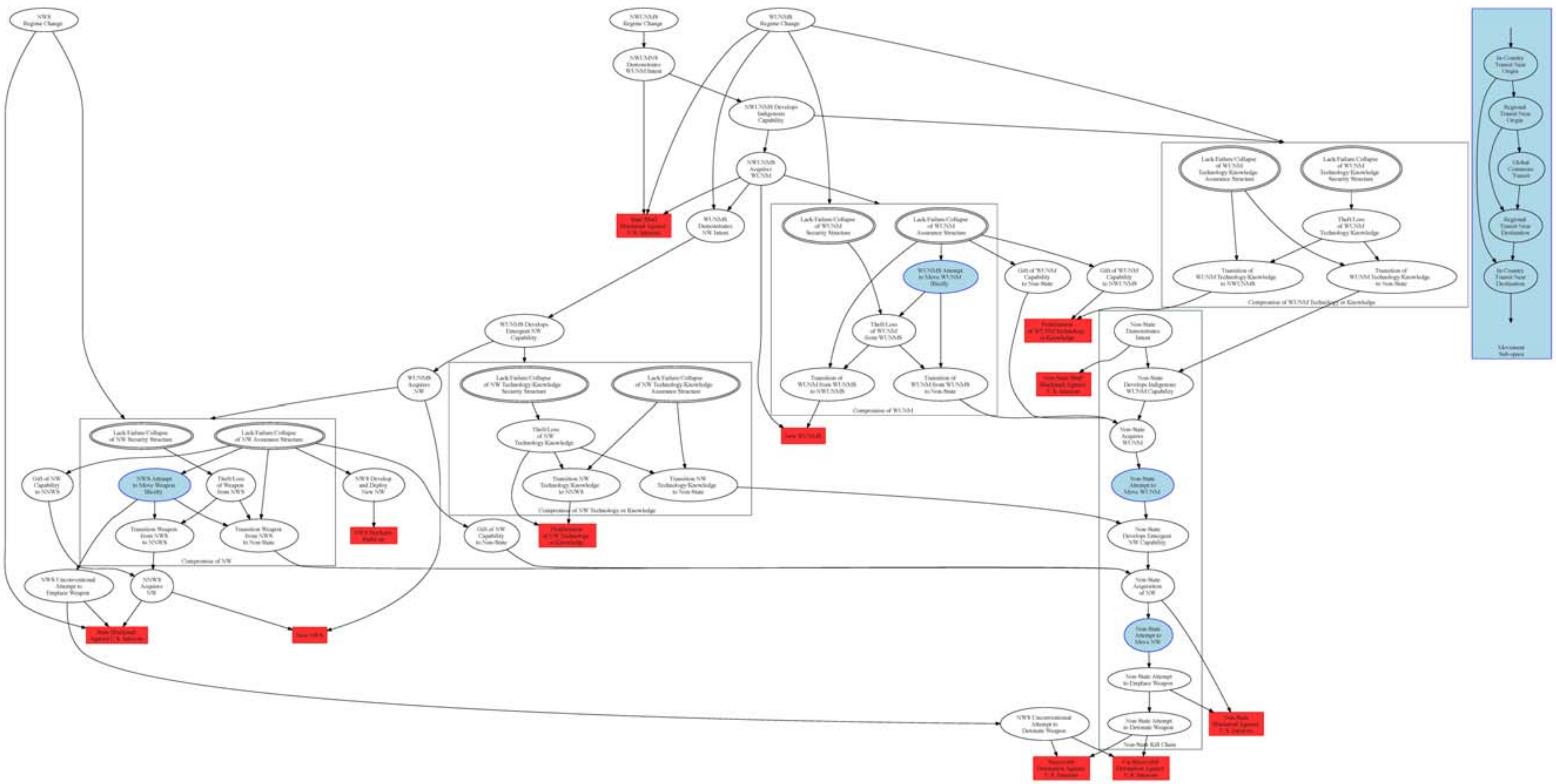


Figure A-2 Proposed Scenario Framework

A.3. Analysis Within the Scenario Framework

Analytically, the scenario framework serves several roles. Most importantly, it exists as a common frame of reference for describing the M&V problem space. Narrower problem definitions, metrics, and objectives can be derived where appropriate through decomposition (discussed more in Section A.5). Scenarios for analysis can be generated by stringing sequences of nodes together. Any starting point and ending point can be selected, and a path through the network selected to connect them. From that string of nodes, a more complete narrative can be constructed.

The scenario framework can also allow for greater and more complete coverage in the design and analysis of solution architectures. A large family of scenarios can be analyzed by examining all nodes systematically node-by-node independent of end-to-end scenarios. An analyst can consider solution architectures that combat adversary success within a single node, and consider the collective impact it has on the complete scenario space by examining both upstream and downstream nodes. Additionally, tradeoffs between architectures designed for different nodes can be compared in an end-to-end system performance sense. This will aid the assessment of the complete set of architecture components within a portfolio of defensive measures and allow for complex trades to be made. While the scenario framework provides the structure for this kind of analysis, there is still the challenge of developing end-to-end metrics that are solution independent and common among all nodes. Further consideration of this issue is given in Section A.8.

Finally, it should be noted that the scenario framework is not proposed to be the sole description of the problem space for the M&V mission. Rather, it is one useful construct for describing the problem space that lends itself to the analysis that is discussed in this chapter. As is often the case with large complex problems that have a myriad of stakeholders who might have competing objectives, there are likely many representations of the problem space that are all germane to evaluating potential solutions. While it is recommended that the scenario framework be considered as a unifying representation of the problem space for analysts and decision makers, it is also recognized that other representations exist and are useful. Such work should continue, but the need for integrating them into a common set of problem space models remains. Likewise it is recommended that the scenario framework be periodically reviewed and updated as appropriate based on real world experience and additional analytical studies.

A.4. Bridging Methodologies

While the scenario framework proposed in Section A.2 can provide a common frame for understanding the M&V problem space, any problem framework must be connected to potential solution options in order to be ultimately useful to capability investment decision makers, or policy makers and treaty negotiators. The method used to connect the problem and solution spaces is called a bridging methodology for the purposes of this report. A bridging methodology approach allows for a breakdown and prioritization of goals and objectives in the problem space into requirements and metrics for potential solution architectures. It will also allow for the systematic aggregation of performance assessments and analyses into an overall picture of monitoring and verification architecture performance.

A.5. Proposed Decomposition Map Approach

The bridging method proposed by the Task Force is a decomposition approach that maps between problem space descriptions and prospective solution architect elements. This subsection describes the decomposition approach in general; the next one provides an example to illustrate its application.

As envisioned, the proposed approach begins with the selection of any node in the scenario framework discussed in Section A.2. The selected node is decomposed into any sub-nodes required to add appropriate fidelity or resolution to the analysis. A system of decomposition layers is then constructed beneath the scenario nodes. Those four layers are:

1. **Strategic Capability Areas** – This layer, while arbitrary, provides a convenient organizational structure when considering the universe of potential capability investments. As defined in this report, the strategic capability areas center on core elements of the mission space associated with reducing risk.
2. **Functional Objectives** – Within each Strategic Capability Area, several functional objectives can be articulated. These objectives are intended to capture high-level operational objectives that must be achieved. The articulation of these objectives must be performed by the decision maker, as there is no universal set. The metrics used to assess performance against those objectives must be derived by the analysts from the articulation of risk in the problem space.
3. **Tasks** – Each functional objective can be further decomposed into a set of tasks. The tasks themselves are part of prospective solution architecture – i.e., tasks, just like objectives, are not universally defined, but proposed as part of a solution option. Each task defines a specific component of a functional objective, to be accomplished through the application of assets. The measures of performance used to assess the performance of a task are formulated derivatively from the metrics used to assess performance against the functional objectives.
4. **Assets** – Each task is accomplished through the employment of assets. Assets can include hardware, platforms, people, training, concepts of operations, and programs – essentially any capability that can be specifically invested in. Requirements and metrics for assets are established derivatively from the tasks. The mix of appropriate assets for consideration is dependent on the tasks proposed as part of prospective solution architectures.

As assessments of performance of existing or proposed solution architectures and components are completed through analytical work, the results must be first cast in the framework of the decomposition map, and then captured as part of the overall solution architecture assessment. Areas of disagreement in assessments, or those areas that are not well covered (or over-covered) by current analytical results can be readily identified. In this way, a decomposition map can also serve to guide the overall effort of an M&V analytical capability, such as that described in Section A.6.

Each node in the scenario framework proposed in Section A.2 will have at least one unique decomposition map associated with it in a fully formed analytical effort. There are only a limited number of unique investible assets that may be incorporated in prospective solution architectures, and many assets are likely applicable to several different functional objectives and tasks. These observations imply that most assets will aggregate requirements from multiple scenario nodes, strategic capability areas, functional objectives, and tasks. Assets must be assessed against each set, and synergies may be identified and leveraged when designing solution architectures.

Optimistically, the same asset may have sufficient performance and applicability across multiple tasks, functional objectives, strategic capability areas, and scenario nodes. This implies that if a consistent accounting of performance and benefits is made, through a systematic methodology as proposed here, then benefits across the problem space can be better understood, and investments in one area may have the effect of reducing risk in areas outside the scenario node currently being investigated. In this way, one might imagine a fully executed analytical model of the M&V mission areas as a large multi-layered network – on one face exists the problem description (i.e. the scenario framework), and on the opposite face proposed solution architectures in the form of a set of investible assets. The layers in between are highly connected and consist of the layers articulated in the description of the bridging methodology described above.

A.6. Decomposition Map Example

The overall decomposition approach described in Section A.5 may be best described through the example illustrated in Figure A-3. The example decomposition map begins with a focus on the scenario node “Non-State Attempt to Move Weapon”. The scenario node is decomposed into more specific scenario sub-nodes; in this case the analyst is concerned with “In Country Movement” of a nuclear weapon or asset.

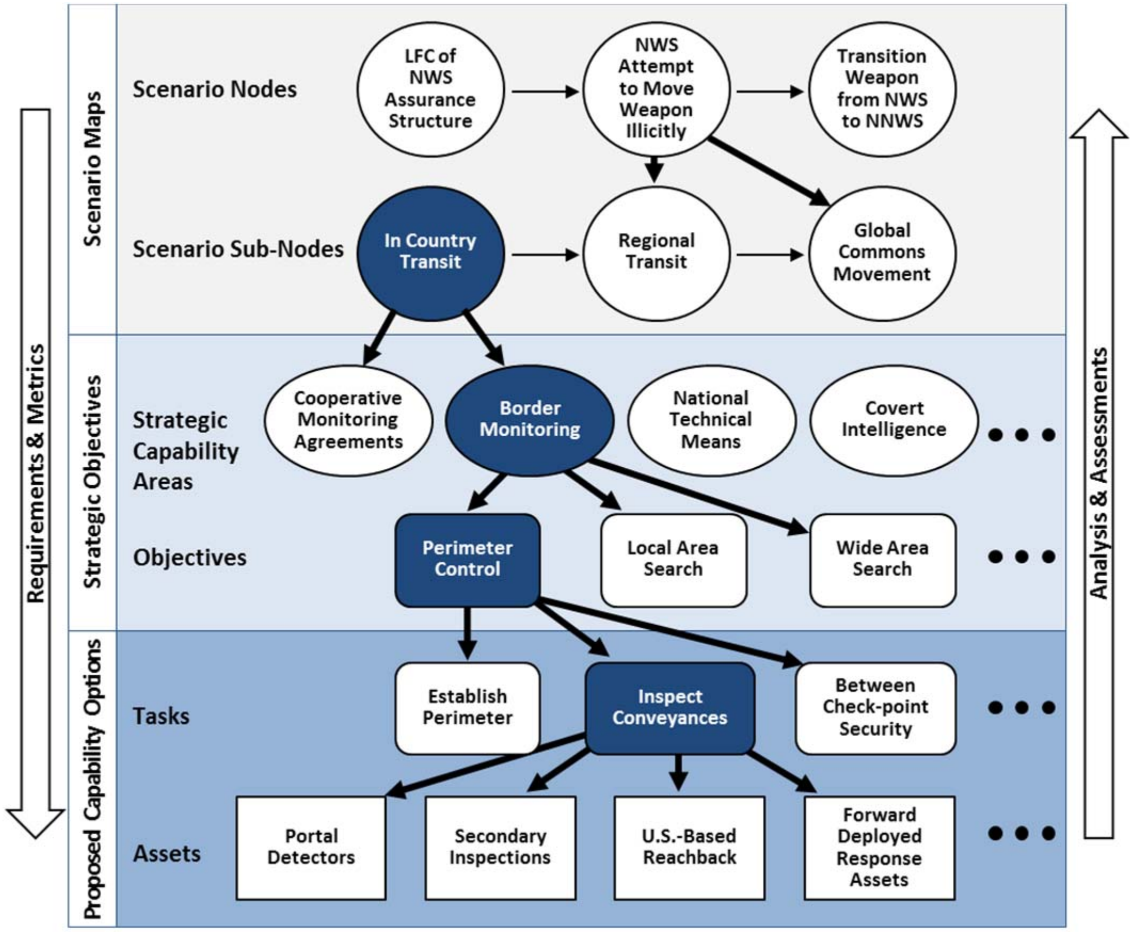


Figure A-3 Example Decomposition Map

The next step of decomposition moves from the problem description (the red shaded area in the decomposition map) towards the articulation of a solution architecture (the blue shaded area in the decomposition map). The scenario sub-nodes are decomposed into strategic capability areas dividing the problem space into discrete mission areas – in this case border monitoring is highlighted. In addition to other functional objectives, it may be desirable as part of border monitoring to control a perimeter around an area of interest, preventing nuclear materials or devices of interest from moving across that perimeter (it may also be desirable to allow innocent traffic to cross the perimeter, as in border control scenarios). Additionally, the capability to search small areas thoroughly, and search large areas efficiently may be important functional objectives.

The functional objective, "Perimeter Control" can be further decomposed into a set of tasks that must be accomplished in order fulfill that objective. These tasks and the assets associated with them represent a proposed solution architecture for accomplishing the objectives specified. For example, the perimeter must be established and maintained. Additionally, items that pass through that perimeter must be inspected to ensure that no nuclear contraband is passing through the perimeter. A secure zone between inspection points must be maintained to ensure that no nuclear contraband is passing around those inspection points. (Additional tasks may need to be performed, but are not included here.)

In this example, it is proposed that radiation detectors, in addition to persistent surveillance assets might be used to help establish a perimeter through monitoring and surveillance of perimeter zones. Boots on the ground and vehicles are proposed for enforcing perimeter incursions presenting a show of force along the perimeter itself. Similarly, additional assets can be laid out and their relationships to mission objectives captured. The requirements and metrics by which proposed assets are to be assessed have been derivatively defined from the previous layer. As assessments are made and analytical results obtained, those are aggregated into performance assessments of higher and higher layers.

The derivation of a tractable set of metrics through this process is not a trivial task, nor should it be. Risk is often considered the top-level metric (with further discussion in the next section). Moving down the chain through strategic capability areas, functional objectives, tasks, and assets, metrics of increasing resolution and granularity are derived. At the asset level, the metrics center largely on performance specifications that are technology specific. These metrics are familiar in radiation detector assessments, but on their own, are only implicitly related to the overall goals of risk-reduction. A metrics derivation process such as this places each metric in the context of the layer above it, explicitly linking it to overall architecture performance.

A.7. Portfolio Decision Methodologies

The scenario framework, the bridging methodology, and the risk considerations proposed above lay out a systematic method for developing and assessing M&V solution architecture options. In order to render those results into investment roadmaps to develop capabilities, a decision framework must be established. While this section does not attempt to propose a decision framework, it does provide some considerations for doing so.

A.8. End-to-End Metrics

A significant challenge in adopting the approach that has been laid out above has been the articulation of an end-to-end metric that can be used to understand overall solution architecture performance against the problem space. Ultimately, it is that metric that matters most to decision makers. Risk provides a clear metric for endogenous trade-offs within the M&V problem space, allowing for the comparison of very different solution sets and examination of benefit between investments both within, and across, different components of the problem space itself. Utilizing risk as an end-to-end metric in the M&V problem space can also enable exogenous trades, as governments face economic challenges and must make tougher decisions about where to invest resources.

Utilization of risk as an end-to-end problem space metric comes with a set of inherent challenges as well. Common criticisms of formal risk assessment methodologies in decision processes include:

- **Conflating stochastic processes and adversary decisions** – Rigorous risk assessment methodologies rely on estimates of the probabilities of events of concern. In systems where outcomes are determined by truly random processes, this works quite well, especially when the system is well characterized. However, well characterized stochastic processes do not govern intelligent adversaries; instead, they make informed decisions. Although frequently used, probabilistic representations of adversary decisions are, for the most part, meaningless. However, characterization of uncertainty about adversary decisions in a probabilistic analysis can be beneficial, if carefully developed.
- **Focusing on absolute values rather than relative impacts and sensitivities** – The absolute values of risk are, in most formulations, arbitrary, as they are built upon the assumptions and values of the analyst or decision maker for whom they are constructed. Additionally, the models upon which risk is calculated often cannot be truly validated. Therefore, the absolute values of risk are less important and somewhat meaningless, while the differences and relative comparisons can be more telling.
- **Inability to define "acceptable"** – A key component of making decisions in a risk-based framework is to define acceptable risks within the timeframe of the investment decision itself. If "acceptable" cannot be defined, the goal becomes to simply minimize risk, expending all resources, rather than achieve minimum risk using appropriate resources.
- **Examining risk trade-offs too narrowly** – One of the most common criticisms of implementations of risk-based approaches is the lack of definition around uncertainties. Especially in problems of high uncertainty, the error in risk calculations can be so large, that close trade-offs can be interpreted as essentially the same. Not having well defined uncertainties can allow false comparisons to drive decision processes. At the same time, ignoring the uncertainty (or error bars) in the analysis denies they opportunity to prioritize potential efforts to improve understanding.
- **Misuse of probability and statistics** – While it may seem like an elementary mistake, bad assumptions or interpretations, especially around dependence or independence, can lead to mathematical operations and inferences that may be numerically correct, yet meaningless—or worse, incorrectly calculated.

In the face of those challenges, it is certainly possible, although difficult, to articulate a risk metric that serves as an end-to-end metric within the M&V problem space for evaluating proposed solution architectures. It may not be necessary to always use the classical definitions of risk as the primary measure. Most risk studies use the arithmetic product of probabilities of occurrence and consequences as the standard definition of risk. However, the strictest interpretation of risk may not always be the most useful or accurate. Instead, it is possible to use measures that are proximate to risk when performing analyses. For example, other studies have proposed and formalized using assessments of the difficulty an adversary would face in executing a successful attack[41] to replace probability in the classical formulation of risk, when working with risk assessments of intelligent adversaries. Additionally, understanding the readiness level of an adversary and the expected time to attack can also serve as a useful risk proxy. Regardless of the exact risk metric or proxy used, risk (or some formulation of risk proxies) is likely to be a "necessary evil" as it allows for disparate approaches to be transacted together in cost-benefit trade-offs, and provides a consistent metric and method for analysis as new information and options become clear.

A.9. Balancing Risk

A key role of a portfolio decision methodology is to identify investments in capabilities that balance risks given the values of the decision maker. Investment risk does not only include cost and technical risk, but also institutional decision factors. Institutional decision factors are elements such as championship, mission, acceptance, and other factors that may prevent investments from being successful if not present. While not often considered in formal decision processes, they can have a large effect on the outcomes of decisions to acquire capabilities. Accounting for these factors in an M&V portfolio decision methodology is recommended.

A method for achieving a "balanced" capability portfolio can be desirable to some decision makers. For the purposes of this work, "balance" is defined as having an appropriate mix of capability investments to maximize risk reduction in the outcomes, while being prudent about the investment risks associated with each portfolio asset. As an analyst considers capability options, a balanced portfolio may be very different given the values and risk tolerance of the decision maker and the investing agency. For example, R&D focused organizations may have a set of values that is more risk tolerant, and a balanced investment portfolio may be skewed towards the long-term, high risk, high payoff projects. At the same time, an operational component may seek primarily commercial-off-the-shelf solutions and a balanced investment portfolio may be skewed towards incremental, low risk improvements. Formal and quantitative methods for assessing the risk tolerance and the values of decision makers exist and should be extended in formulating an M&V portfolio decision methodology.

[41] Wyss, Hinton, et al, Risk-Based Cost Benefit Analysis for Security Assessment and Investment Prioritization, Sandia National Laboratories, 2011.

Appendix B. Terms of Reference

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

APR 2 6 2010

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board (DSB) Task Force on the Assessment of Nuclear Treaty Monitoring and Verification Technologies

During the coming years, the United States is expected to engage in a series of treaty negotiations on nuclear weapons and nuclear forces. In addition, the rapid growth in nuclear power worldwide will likely stress the implementation practices of existing material control agreements, as well as poise more nations with the ability to acquire nuclear weapons of their own. Monitoring and verification measures are an integral part of all the existing, modified, or new agreements. Potential requirements for new or expanded monitoring and verification requirements place a renewed focus – after almost 2 decades of limited investment – on the adequacy of the Nation's technical tools to support monitoring and verification, both as part of the cooperative verification regimes of the treaties and through national intelligence.

You are to form a DSB Task Force to accomplish the following:

1. Research and summarize anticipated directions in nonproliferation and arms control agreements and the environments in which they might be implemented (for example, the level of transparency and cooperation that will be desired/required in post-Cold War arms control agreements, including treaties among nuclear states in addition to the United States and Russia);

2. Project the demands and challenges placed on existing agreements enforced by the International Atomic Energy Agency with the growth in nuclear power over the next 15 to 20 years, and assess the adequacy of current practices and resources to maintain confidence that inspected nations remain non-proliferators;

3. Assess current and programmed technical capabilities and gaps to support the anticipated monitoring and verification regimes;

4. Address what could be adapted from technical advances made for a number of other existing monitoring purposes, such as those developed for applications related to the following:

a. Close-in and/or unmanned intelligence, surveillance, and reconnaissance systems to support conventional warfighting and counter-improvised explosive device operations;

b. Stockpile stewardship;

c. Nuclear forensics and attribution;

d. Nuclear weapons effects; and

e. Nuclear defense and interdiction programs.

5. Propose new initiatives, including identification of the technologies, research, development and testing program, and red/blue teaming requirements to fully vet new concepts; and

6. Perform a net assessment to understand the potential limitations and regrets associated with possible technical implementation paths.

The Task Force should recommend a comprehensive set of time-phased technical programs that could be conducted by the Department of Defense, the Department of Energy, the Intelligence Community, or a combination of these agencies, with consideration of what other agencies might also require (e.g., Department of State), contribute (e.g., Department of Homeland Security), or enable (e.g., Office of Science Technology and Policy).

The study will be co-sponsored by me as the Under Secretary of Defense for Acquisition, Technology and Logistics; the Administrator of the National Nuclear Security Administration (NNSA); and the Director of National Intelligence (DNI). Dr. Miriam John and Dr. Donald Kerr will serve as Chairpersons of the Task Force. Mr. Rhys Williams of NNSA, Dr. Tom Hopkins from DATSD(NCB), and Mr. Michael Toomey of ODNI will serve as co-Executive Secretaries, and Major Michael Warner, USAF, will serve as the DSB Secretariat Representative.

The Task Force will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5105.4, the "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of title 18, U.S. Code, section 208, nor will it cause any member to be placed in the position of acting as a procurement official.

Ashton B. Carter

2

Appendix C. Task Force Membership

Co-Chairs

Dr. Miriam John	Independent Consultant
Hon. (Dr.) Donald Kerr	Independent Consultant

Executive Secretaries

Dr. Tom Hopkins	Office of the Secretary of Defense
Mr. Michael Toomey	Office of the Director of National Intelligence
Dr. Rhys Williams	National Nuclear Security Administration

Members

Dr. Joseph V. Braddock	Independent Consultant
Mr. John A. Lauder	Arete Associates
Dr. Anthony Pensa	Lincoln Laboratory
Hon. F. Whitten Peters	Williams & Connolly
Amb. (Dr.) Paul Robinson	Independent Consultant
Dr. Alexander C. Livanos	Northrop Grumman Corporation
Mr. Darryl Sargent	Draper Laboratory
Dr. James Tagnelia	Independent Consultant
Dr. Bruce Tarter	Lawrence Livermore National Laboratory
Mr. Lou Von Thaer	General Dynamics
Dr. Richard L. Wagner, Jr.	Independent Consultant
Dr. Joan Woodard	Independent Consultant

Senior Advisors

Dr. Craig Fields	Independent Consultant
Hon. (Dr.) John S. Foster, Jr.	Independent Consultant
Hon. (Dr.) William Schneider Jr.	Independent Consultant

Government Advisors

Mr. Richard Benson	Air Force
Mr. Bob Blum	Department of State
Mr. Doug Bruder	Defense Threat Reduction Agency
Mr. Don Cobb	Defense Threat Reduction Agency
Dr. Pat Falcone	White House, Office of Science & Technology Policy
Mr. Dick Gullickson	Defense Threat Reduction Agency
Mr. T.R. Koncher	Department of State
Mr. George Look	National Security Council
Mr. David O'Brien	Air Force
Dr. Joan Pierre	Defense Threat Reduction Agency

Mr. R.C. Porter	Defense Intelligence Agency
Dr. Caroline Purdy	Department of Homeland Security
Mr. Luis Salcedo	Navy
Mr. Kurt Seimon	National Nuclear Security Administration
Ms. Donna Smith	National Nuclear Security Administration
Lt. Col. John Smith, USAF	Office of the Secretary of Defense
Mr. Tom Troyano	Office of the Secretary of Defense
Mr. Larry Turnbull	UCIA

Laboratory Advisors

Dr. Kory Budlong-Sylvester	Los Alamos National Laboratory
Dr. Mona Dreicer	Lawrence Livermore National Laboratory
Ms. Nancy Jo Nicholas	Los Alamos National Laboratory
Mr. Jason Reinhardt	Sandia National Laboratory
Dr. Sheila Vaidya	Lawrence Livermore National Laboratory
Mr. Bruce Walker	Sandia National Laboratory

DSB Secretariat

Mr. Brian Hughes	Defense Science Board
Lt. Col. Michael Warner, USAF	Defense Science Board
CDR Doug Reinbold, USN	Defense Science Board

Contract Support

Mr. Chris Grisafe	SAIC
Ms. Tammy-jean Beatty	SAIC

Appendix D. Task Force Meeting Schedule

Date	Briefing Title	Briefer	Affiliation
7/1/2010	DSB Intro Task Force Brief	Maj. Mike Warner	DSB
7/1/2010	Arms Control and Nonproliferation Priorities in the Administration	Mr. George Look	NSC
7/1/2010	New Arms Control Challenges: The Role of Intelligence in Verification and Monitoring	Mr. John Lauder	Task Force Member
7/1/2010	Monitoring R&D Program	Mr. Dick Gullickson	DTRA
7/1/2010	International Monitoring System	Mr. Don Phillips	Space and Missile Defense Command
7/1/2010	U.S. Atomic Energy Detection System	Dr. David O'Brien	AFTAC
7/1/2010	Does Monitoring Matter?	Dr. Joe Braddock	Task Force Member
7/2/2010	Intelligence Science Board	Dr. Joan Woodard	Task Force Member
7/2/2010	Limitations on UGT monitoring	Dr. Jay Zucca	LLNL
7/2/2010	Space and Seismic Monitoring R&D programs	Mr. Randy Bell	NNSA
7/22/2010	Where the Materials Are in the world	Ms. Jamison Manternach	DOE
7/22/2010	DOE Global Threat Reduction Initiative	Mr. Ken Sheely	DOE
7/22/2010	Technologies for Sustainability of Next Generation Russian Programs	Mr. Mike O'Brien	LLNL
7/22/2010	Program Brief: International Material Protection	Mr. John Gerrard	DOE
7/22/2010	IAEA Safeguards	Dr. Kory Budlong-Sylvester	LANL
7/22/2010	Cooperative Threat Programs	Amb. Bonnie Jenkins	DOS
7/22/2010	Insights on Global Threat Reduction	Dr. Joe Braddock	Task Force Member
7/23/2010	Materials Protection	Ms. Laura Holgate	National Security Council
7/23/2010	Global Nuclear Lockdown	Mr. Tom Skillman	DoD
7/23/2010	Value of Monitoring and Verification	Hon. John P. Stenbit	Private Consultant
7/23/2010	Importance of Understanding NW Effects in Support of Verification	Dr. Joan Woodard	Task Force Member

8/24/2010	Role of TRMG and New START	Dr. Robert Blum and Mr. Ed Fortier	DOS
8/24/2010	CTBT NIE	Mr. Brian Lessenberry	NIC
8/24/2010	Nuclear Explosion Monitoring Challenges for the Next Decade	Dr. Larry Turnbull	JAEIC
8/24/2010	Test Monitoring Limitations	Mr. Don Linger	DTRA
8/24/2010	Russia's Stockpile	Ms. Marysusan Lynch	Office of Russian and European Analysis
8/24/2010	Rest of the World Stockpile and the Threat	Mr. John Galascione	WINPAC
8/24/2010	Importance of Understanding NW Effects in Support of Verification	Dr. Joan Woodard	Task Force Member
8/25/2010	Assessing Foreign Nuclear Programs	Mr. Bruce Held	Lab Advisor
8/25/2010	Nuclear Denial and Deception	Dr. Larry Gershwin	
8/25/2010	Nuclear Terrorism	Ms. Tara Swersie	NCTC
8/25/2010	Insights on Global Threat Reduction	Dr. Joe Braddock	Task Force Member
8/25/2010	Task Force Briefing v1	Dr. Mim John	Co-Chair
8/25/2010	Delivery Systems Chart	Dr. Mona Dreicer	Lab Advisor
9/13/2010	Future Issues for Safeguards	Amb Greg Schulte	DOS
9/13/2010	NK Nuclear Activity, CP Issues Worldwide and New START/NIE	Amb Joseph DeTrani and Mr. Bob Walpole	NCPC
9/13/2010	Open Skies	Mr. Scott Simmons; Mr. Dennis Connaughton; CDR Darin Liston; Mr. Don Spence & Mr. Michael Bett; Mr. Bob Harmon	DIA, DTRA, DOS, NGA
9/13/2010	Training for On-Site Inspections	Mr. Hunter Lutinski & Mr. Mark Beddoes	DTRA
9/13/2010	Next Generation Safe Guards	Mr. Steven LaMontagne	
9/13/2010	Task Force Briefing v2	Dr. Mim John	Co-Chair
9/14/2010	Monitoring & Verification for Arms Control (Password is: DSB)	Dr. Mona Dreicer	Lab Advisor
9/14/2010	START 3/Technology Development 1990-Present	Mr. John Dunn	NNSA
9/14/2010	U.S.-UK Technical Cooperation to Support Arms Reduction Initiatives	Ms. Michele Smith, NNSA	NNSA

9/14/2010	Nuclear Power	Dr. Kory Budlong-Sylvester	LANL
10/25/2010	Historical Perspectives on Proliferation and Perspectives on China	Mr. Brad Roberts	DASD, OSD/Policy
10/25/2010	Sufficiency of R&D Activities Across Gov't	Dr. Pat Falcone	OSTP
10/25/2010	Data Processing for Wide Area Surveillance	Dr. Sheila Vaidya	LLNL
10/25/2010	Army Asymmetric Warfare Group	LTC Tom Newman, LTC David Wright	USA
10/25/2010	Technology Exploration	Dr. Joe Braddock	Member
10/26/2010	Hyperspectral Capability	Mr. Christopher Simi	Briefer
10/26/2010	Open Source Center Capabilities	Mr. Winston Dunleer, Mr. Darko Gerovac	Briefer
10/26/2010	Constant Hawk and Parallel Sensors	Mr. Steven Gotoff	DIA
10/26/2010	Task Force Briefing v3	Dr. Mim John	Co-Chair
1/6/2011	Technologies for Monitoring and Verification	Mr. Darryl Sargent	Draper Laboratory
1/6/2011	Wide Area Surveillance System Based Multi-INT Integration and Analysis for Situational Awareness and Knowledge Distillation	Dr. David Cremer	LANL
1/6/2011	Fast Fission Neutron Time Correlations from Fission for Non-Proliferation and Arms Control Applications	Dr. Leslie F. Nakae	LLNL
1/6/2011	Nonproliferation monitoring with distributed sensor networks	Dr. Simon Labov	LLNL
1/6/2011	The potential of small satellites for application to persistent monitoring and verification issues	Dr. Scot S. Olivier	LLNL
1/26/2011	Task Force Briefing v4	Dr. Mim John	Co-Chair
1/25/2011	Gamma Ray and Neutron Detection Methods for Nuclear Materials	Dr. Glenn Knoll	University of Michigan
1/25/2011	Domestic Nuclear Detection Office	Joel Rynes, Ph.D., PMP Brendan Plapp, Ph.D. Caroline Purdy, Ph.D.	DHS
1/25/2011	Radiation Detector Materials	Dr. Steve Payne	LLNL
1/25/2011	Radiation Detection at Sandia	Mr. Jim Lund	Sandia

1/25/2011	Laboratory Directed Research and Development: An Open Market for Ideas, Driven by Mission	Dan Holden	LANL
1/25/2011	Radiation Detection at NA-22	David Beach, Peter Vanier, Arden Dougan	NNSA
1/25/2011	DTRA Nuclear Detection	Dr. Peter Zielinski	DTRA
1/25/2011	Global Nuclear Architecture Report	DNDO	DHS
3/2/2011	Part 2. Framework end-to-end	Dr. Joan Woodard, Mr. Jason Reinhardt	Member/Lab Advisor
3/2/2011	Part 3. Sense and Assess – Rad detection	Dr. Bruce Tarter &Dr. Rhys Williams	Member/Exec Sec
3/2/2011	Part 3. Sense and Assess – Characterizing capabilities, “patterns of life”	Dr. Joe Braddock, Mr. John Lauder, Mr. Mike Toomey	Member/Exec Sec
3/2/2011	Part 3. Sense and Assess – Persistent ISR	Mr. Lou Von Thaer, Dr. Tony Pensa, Dr. Sheila Vaidya	Member/Lab Advisor
3/3/2011	Part 3. Sense and Assess – Multi-INT analyses	Mr. Mike Toomey	Exec Sec
3/3/2011	Part 4. Access – Joint Experiments	Dr. Paul Robinson, Dr. Mona Dreicer	Member/Lab Advisor
3/3/2011	Part 4. Access – Open Skies	Dr. Jim Tegnelia, Mr. John Lauder	Member
3/3/2011	Part 4. Access – Materials control	Dr. Kory Budlong-Sylvester	Lab Advisor
3/3/2011	Part 4. Access – Dismantlement and Weapons Modernization Programs	Dr. Nancy Jo Nicholas, Mr. Bob Huelskamp, Dr. Rich Wagner	Member/Lab Advisor
3/3/2011	Part 4. Access - Non-cooperative environments	Mr. Darryl Sargent	Member
3/3/2011	Part 5. Iterate and Adapt	Dr. Rich Wagner, Dr. Jim Tegnelia, Dr. Joe Braddock	Member
3/3/2011	Adapt & Iterate Paper	Dr. Joe Braddock	Member
3/3/2011	DOTMLPF-Theater Nuclear Forces Paper	Dr. Joe Braddock	Member
3/3/2011	Non-Traditional Signatures	Dr. Joe Braddock	Member
3/3/2011	Part 6. Leadership	Mr. Whit Peters, Mr. John Lauder, Dr. Mim John, Hon. Don Kerr	Member/Co-Chair

3/3/2011	Detecting Nuclear Threat	Dr. Michael A. Kuliasha	DTRA
3/3/2011	STASIS	Dr. Jasper Lupo	Applied Research Associates
3/3/2011	Task Force Briefing v5	Dr. Mim John	
3/3/2011	Open Source Center	Mr. Mike Toomey	
5/3/2011	General Story Line and Part 1. Introduction	Dr. Mim John, Hon. Don Kerr	
5/3/2011	Part 4. Sense and Assess – Rad detection	Dr. Rhys Williams, Dr. Don Cobb, Bruce Tarter	
5/3/2011	Part 2. Framework end-to-end	Dr. Joan Woodard & Mr. Jason Reinhardt	
5/3/2011	Part 3. Monitoring Architecture: Access-Sense-Assess-Iterate	Mr. Lou Von Thaer	
5/3/2011	Part 4. Sense and Assess: NTM: its role and its limitations	Mr. John Lauder and Dr. Don Kerr	
5/3/2011	Part 4. Sense and Assess: Signs of activities Associated with Having a Viable Capability	Mr. Mike Toomey, Dr. Rhys Williams & Dr. Joe Braddock	
5/3/2011	Part 4. Sense and Assess: Initial filter: "Patterns of life" analyses	Mr. John Lauder & Mr. Mike Toomey	
5/3/2011	Part 4. Sense and Assess: DOTMLPF	Dr. Joe Braddock	
5/4/2011	Part 4. Sense and Assess: Next tier of observation: Persistent ISR	Mr. Lou Von Thaer & Dr. Tony Pensa	
5/4/2011	Part 4. Sense and Assess: Developments for counter-IED problem (COIC)	Group discussion re what we should say about this	
5/4/2011	Part 4. Sense and Assess: Large data set processing	Dr. Sheila Vaidya & Dr. Tony Pensa	
5/4/2011	Part 4. Sense and Assess: "nth-country/group" analytical capability evolved for today's problem space	Dr. Mona Driecer	
5/4/2011	Part 4. Sense and Assess: Concept for the CWMD-COP	Dr. Jim Tegnelia	
5/4/2011	Part 5. Access: Whether facing cooperative or non-cooperative environments, we need more options to improve access	Dr. Paul Robinson, Dr. Mona Dreicer & Kory Budlong-Sylvester	

5/4/2011	Part 6. Experiment, Iterate and Adapt	Dr. Rich Wagner, Dr. Jim Tegnelia & Dr. Joe Braddock
5/4/2011	Clarifying terms: Monitoring and Verification	Paul Robinson
5/4/2011	the “Building Transparency” Recommendation	Paul Robinson & Mona Dreicer
5/4/2011	Open Source Reporting and Analysis	Mike Toomey
5/4/2011	Testing Capability Chart	Joe Braddock
5/4/2011	Open Source Center Text	Mike Toomey

Appendix E. Acronyms Used in This Report

AF	Air Force
ASD(NCB)	Office of the Assistant Secretary of Defense for Nuclear, Chemical and Biological Defense Programs
ASW	Anti-Submarine Warfare
AT&L	Acquisition, Technology, and Logistics
AVC	Bureau of Arms Control, Verification and Compliance
CD	Compact Disc
CIS	Commonwealth of Independent States
COCOMs	combatant commands
COIC	Counter IED Operations Integration Center
CONOPs	Concept of Operations
Counter-IED	Countering Improvised Explosive Devices
CP	Counter proliferation
CPP	Counterproliferation Program
CTBT	Comprehensive Nuclear-Test-Ban Treaty
CTR	Cooperative Threat Reduction
DARPA	Defense Advanced Research Projects Agency
DC	Dual Capable
DCA	Dual-capable aircraft
DHS	Department of Homeland Security
DNDO	Domestic Nuclear Detection Office
DNA	Defense Nuclear Agency
DNI	Director of National Intelligence
DOD	Department of Defense
DOE	Department of Energy
DOS	Department of State
DTRA	Defense Threat Reduction Agency
EUCOM	United States European Command
FFRDCs	Federally Funded Research and Development Centers
GCAS	Global Counter Weapons of Mass Destruction Awareness System
GEOINT	Geospatial Intelligence
GLCM	Ground launched cruise missile
GNDA	Global Nuclear Detection Architecture

HEU	Highly-Enriched Uranium
HUMINT	Human Intelligence
IAEA	International Atomic Energy Agency (IAEA)
IC	Intelligence Community
IED	Improvised Explosive Device
INFCIRC	International Atomic Energy Agency Information Circular
INT	Intelligence
IWG	Interagency Working Group
ISAB	International Security Advisory Board (Department of State)
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
JVE	Joint Verification Experiment
M&V	Monitoring and Verification
MASINT	Measurement and Signature Intelligence
MOU	Memorandum of Understanding
NATO	North Atlantic Treaty Organization
NCPC	National Counterproliferation Center
NGA	National Geospatial-Intelligence Agency
NGO	Non-governmental Organization
NNSA	National Nuclear Security Agency
NNSA/NA-20	NNSA Defense Nuclear Non-Proliferation
NNSS	Nevada National Security Site
NNWS	Non-Nuclear Weapons States
NPT	Non-Proliferation Treaty or Treaty on the Non-Proliferation of Nuclear Weapons
NSS	National Security Staff
OSC	Open Source Center
OSINT	Open Source Intelligence
OSTP	Office of Science & Technology Policy
P-5	Five Permanent Members of the United Nations Security Council
POET	Phase One Engineering Team
Pu	Plutonium
R&D	Research and Development
RDT&E	Research, Development, Test & Evaluation
RSTA	Reconnaissance, surveillance, and target acquisition

S&T	Science and Technology
SDIO	Strategic Defense Initiative Organization
SHAPE	Supreme Headquarters Allied Powers Europe
SIGINT	Signals Intelligence
SNM	Special Nuclear Material
SSD	Safe, Secure Dismantlement
START	Strategic Arms Reduction Treaty
TMM	Treaty Monitoring Manager
TNF	Theater Nuclear Forces
TOR	Terms of Reference
TOSI	Technical On-Site Inspection
TTPs	Tactics, techniques and procedures
U.S.	United States
UAV	Unmanned Aerial Vehicle
UGS	Unattended Ground Sensor
USAEDS	U.S. Atomic Energy Detection System
USG	United States Government
VCJCS	Vice Chairman of the Joint Chiefs of Staff
WMD	Weapons of Mass Destruction
WP	Soviet/Warsaw Pact
WSSX	Warhead Safety and Security Exchange
WUNM	Weapons Usable Nuclear Material


DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA