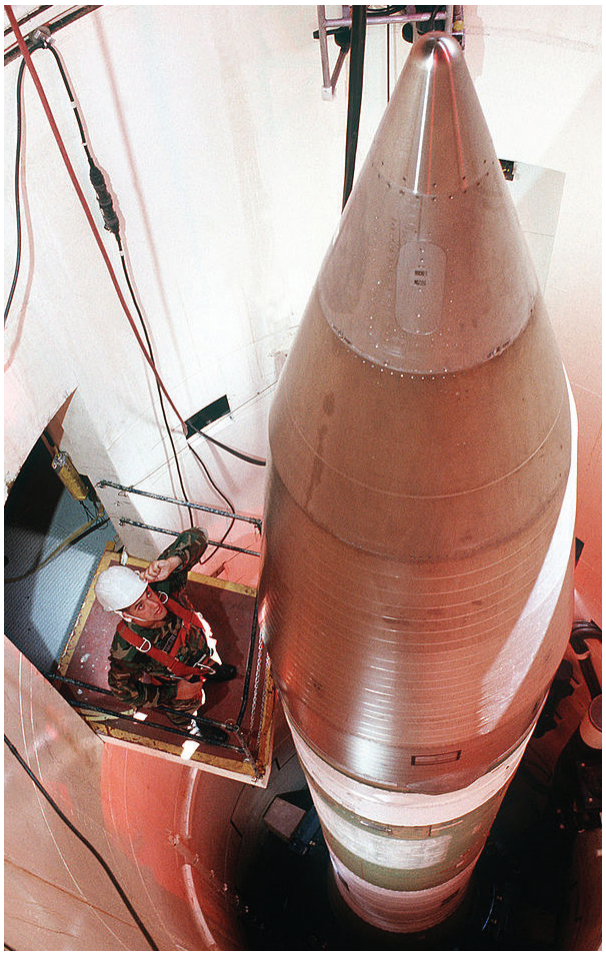
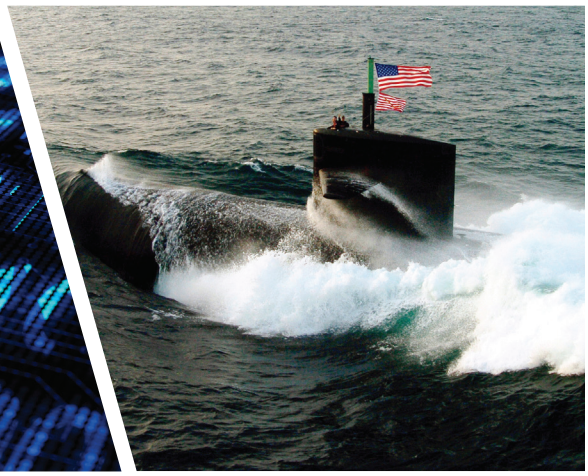
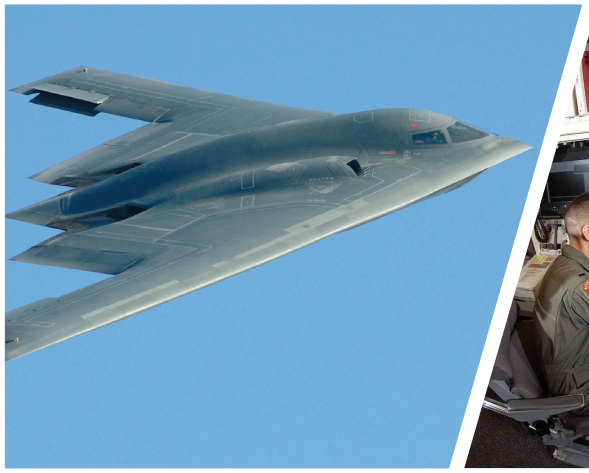
Workshop on U.S. Nuclear Weapons Safety and Security

Summary Report • December 12, 2012







Union of Concerned Scientists
Science for a Healthy Planet and Safer World

AAAS
ADVANCING SCIENCE, SERVING SOCIETY

Summary Report

Workshop on U.S. Nuclear Weapons Safety and Security
December 12, 2012

Sponsored by the American Association for the Advancement of Science and the Union of Concerned Scientists

---

Acknowledgements

The Center for Science, Technology, and Security Policy (CSTSP) at the American Association for the Advancement of Science (AAAS) gratefully acknowledges support from the Carnegie Corporation of New York and the John D. and Catherine T. MacArthur Foundation. The Union of Concerned Scientists (UCS) wishes to thank The William and Flora Hewlett Foundation, The Prospect Hill Foundation, and UCS members for their generous support of this workshop.

Published September 2013

COVER PHOTOS:

CLOCKWISE: WIKIMEDIA/DEPARTMENT OF DEFENSE; ISTOCKPHOTO/ALENGO; ISTOCKPHOTO/MICHAELBWATKINS; WIKIMEDIA/U.S. AIR FORCE PHOTO/MASTER SGT. LANCE CHEUNG; ISTOCKPHOTO/TELEGRAHAM

I. Introduction

On December 12, 2012, the American Association for the Advancement of Science's Center for Science, Technology, and Security Policy and the Union of Concerned Scientists hosted a day-long workshop to discuss issues related to the safety and security of U.S. nuclear weapons.[1] Safety measures are designed to prevent an accidental nuclear detonation or dispersal of plutonium, and security measures to prevent the unauthorized access to or use of nuclear weapons. "Surety" refers to both safety and security, including use control.

The National Nuclear Security Administration (NNSA) is seeking to strengthen nuclear weapon safety and security, in particular by adding features to warheads and bombs as part of their life extension programs. The workshop considered a range of potential warhead modifications, as well as safety and security enhancements that could be achieved through changes in operations or modifications to delivery systems. The workshop also discussed cyber-security threats to nuclear weapons, in particular as they relate to use control.

The workshop was conducted on an unclassified basis. To encourage free and open discussion, it was held under the Chatham House Rule, where statements can be cited but not attributed to individual participants.

In addition to those from the sponsoring organizations, workshop participants included active and retired scientists and engineers from Los Alamos National Laboratory, Lawrence Livermore National Laboratory, and Sandia National Laboratory; government representatives, including those from the NNSA, the Department of Defense (DOD), and the State Department; independent scientists who are members of the JASON group that advises the government on nuclear weapons and other security issues; and experts from academia and nongovernmental organizations.

II. Key Points:

1. In general, participants were not greatly concerned about the safety of existing warheads. A few participants noted that improved safety was beneficial, particularly for workers at the Pantex warhead assembly and disassembly plant. Creating a stockpile using only insensitive high explosives—primarily a safety issue—is a frequently cited NNSA goal. But overall, as one participant noted, safety "is not something I lose sleep over."

2. Participants were in greater agreement that the security, including use control, of U.S. weapons is a substantial issue, but disagreed as to the role that intrinsic features (those in the nuclear explosive package itself) should play in addressing

[1] This summary was prepared by Pierce Corden (AAAS), Lisbeth Gronlund (UCS), Derek Updegraff (AAAS) and Stephen Young (UCS).

this issue. Some held that expecting weapons to be self-protecting was impractical, and suggested that it should be assumed that any stolen weapon can be used to cause a nuclear explosion. Others felt that detonating a stolen weapon would be difficult, given such features as permissive action links (PALs) and arming sequences. Still others held that intrinsic features could add a valuable additional layer of security, reducing the probability and consequences of nuclear use if a weapon was stolen by a terrorist.

3. More specifically, participants' views regarding the advisability of modifying existing weapon types to improve safety and security as part of life extension programs fell along a spectrum. Some argued that advances in the understanding of how weapons work combined with past nuclear test experience in introducing surety features into weapons would allow modifications to be made with confidence. Others believed that current plans for aggressive changes to the nuclear explosive package as part of life extension programs, whether to increase surety or to meet other goals, are unwise and pose a risk of reducing confidence in reliability.

4. There was broad agreement that decisions about adding surety features to warheads should be informed by cost-benefit and risk-benefit analyses. Such analyses should take into account financial costs and reliability, and consider the relative benefits of making intrinsic changes to the nuclear explosive package versus making changes outside the package. Participants had differing views as to the extent that NNSA and DOD decisions are currently informed by detailed cost-benefit and risk-benefit analyses.

5. A number of participants argued strongly that more attention needs to be paid to safety and security measures outside the nuclear explosive package. It was noted that addressing concerns across the stockpile via modifications inside the nuclear explosive package would take decades. Improvements outside the nuclear explosive package can be achieved much more quickly and without creating concerns about the reliability of the stockpile. Others noted that intrinsic measures should nonetheless be considered in lifetime extension programs.

6. There was broad agreement that the cybersecurity of nuclear command and control networks in the United States, Russia, and other states is of critical importance and warrants attention. However, the high level of classification inherent in nuclear command and control procedures makes it difficult to have an in-depth understanding of the potential scope or severity of threats and of appropriate measures to counteract them.

III. Safety and Security Measures

It is best to consider safety and security measures in the context of the entire "surety system," which may include any or all of the following: (1) engineered features; (2) "guns, guards, & gates"; and (3) administrative procedures. Engineered features can be in the nuclear explosive package, in the warhead (or bomb) but outside the nuclear explosive package, or outside the warhead itself (for example, in missiles, containers, or transport systems). Administrative procedures include the two-man rule used by Air Force launch control personnel, as well as the Personnel Reliability Program at DOD and the analogous Human Reliability Program at the Department of Energy (DOE)

A. Safety

Current U.S. nuclear weapons incorporate several engineered safety features (see Table 1). First, the electrical system for all weapons has an Enhanced Nuclear Detonation Safety (ENDS) architecture, in which two independent strong links and a weak link guard against accidental detonations. (This safety system is outside the nuclear explosive package.)

Second, some U.S. nuclear weapons use insensitive high explosive (IHE). This includes all air-carried weapons because of the risk of an airplane crash. Nuclear weapons are initiated by the symmetrical detonation of a high explosive that surrounds the plutonium pit of the weapon. Insensitive high explosives are much less sensitive to being detonated by external events (e.g., fires, shock, bullet impact) than are conventional high explosives (CHE). These insensitive explosives are somewhat less energetic than conventional high explosives, so more must be used in a given weapon, thus requiring the accommodation of greater mass and volume. Since this would be a change in the design of a weapon, some have questioned whether primaries that were designed with CHE could be retrofitted with IHE. In any case, all weapons in the current U.S. nuclear arsenal are designed to be "one-point" safe – so that an accidental detonation at any point would have a probability of no more than one in a million (10^{-6}) of causing a nuclear explosion with a yield exceeding the equivalent of four pounds of TNT.[2]

Third, some weapons possess a fire-resistant pit, which is designed to reduce the probability of dispersal of plutonium in the event of a fire. While this would be useful in the event of fires involving aviation fuel, fires caused by the detonation of rocket fuel are hotter than those caused by vehicle or aircraft fuel, so a fire-resistant pit would be less effective in preventing the dispersal of plutonium in the event of a rocket fuel fire.

Fourth, some – but not all – missiles use an insensitive propellant (Table 1). There are two classes of rocket propellant, with insensitive class 1.3 propellant being somewhat less energetic than the conventional class 1.1 propellant but offering increased safety. For example, replacing the class 1.1 propellant in all three stages of the Trident II missile with class 1.3 propellant would reduce the range of the missile by 8 percent. Replacing

[2] See DOD 3150.2-M, available at http://www.dtic.mil/whs/directives/corres/pdf/315002m.pdf.

the class 1.1 propellant in the third stage of the Minuteman III missile would reduce its range by 4 percent.

Table 1: Safety features of weapons in the U.S. arsenal

ENDS = Enhanced Nuclear Detonation Safety; IHE = Insensitive high explosive; FRP = Fire resistant pit; ALCM = Air-launched cruise missile

Warhead	Warhead Safety	Delivery System	Propellant Type
ICBMs			
W78	ENDS	Minuteman III	Stages 1&2: class 1.3 Stage 3: class 1.1
W87	ENDS, IHE, FRP	Minuteman III	Stages 1&2: class 1.3 Stage 3: class 1.1
SLBMs			
W76	ENDS	Trident II	All stages: class 1.1
W88	ENDS	Trident II	All stages: class 1.1
Air-delivered			
W80	ENDS, IHE	ALCM	N/A
B61	ENDS, IHE	B-2, B-52, F-15E, F-16, Panavia Tornado, F-35	N/A
B83	ENDS, IHE, FRP	B-2, B-52	N/A

Quantitative Requirements

U.S. weapons have quantitative requirements for safety against an accidental nuclear explosion. A weapon must be designed so that the probability of an accidental nuclear explosion having a yield greater than that produced by four pounds of TNT is no more than one in a billion (10^{-9}) during its lifetime under normal conditions, and no more than one in a million (10^{-6}) during abnormal conditions such as those caused by an accident or attack. As discussed above, U.S. nuclear weapons are required to be “one-point safe.”

No quantitative requirements are established for safety against accidental plutonium dispersal. One participant suggested that the Pantex plant required that there be no more than a one-in-a-million likelihood of plutonium dispersal in any accident that

occurred during its weapons production and dismantlement activities, but others questioned whether this was an established requirement. Later investigation determined that Pantex has no such requirement, but has a guideline stating that the odds of plutonium dispersal should be no greater than one in a million. The cells at Pantex are designed to contain plutonium in the event of the detonation of high explosive in the presence of plutonium.

B. Adding New Engineered Surety Features

The NNSA has considered adding several surety technologies to weapons as part of its life extension programs. Those within the nuclear explosive package include:

- Insensitive high explosive (IHE);
- Enhanced detonator safing;
- Systems to prevent an unauthorized implosion even if the high explosive detonates (this would be a security as well as a safety feature because it could prevent a thief from quickly detonating a stolen weapon);
- Disablement (self-destruct) features; and
- Low-HEU designs (which would provide less highly enriched uranium (HEU) for any attempt to build a bomb using material from a stolen weapon or weapons).

Those within the weapon, but outside the nuclear explosive package, include:

- Additional weak links; and
- Disablement features.

Multi-point safety

The NNSA has developed technologies to provide "multi-point safety," so that even if the high explosives were detonated at more than one point essentially simultaneously (within 30 microseconds of each other), the probability of causing a nuclear explosion with a yield of more than four pounds of TNT would be no more than one in a million. The NNSA developed at least one approach to achieving multi-point safety that it proposed installing as part of the B61 life extension program. However, the Nuclear Weapons Council decided against including this option in the final project.

The necessity of the NNSA's program for multi-point safety was questioned by some workshop participants because the likelihood of essentially simultaneous explosions is very small. Others believed that, however remote the possibility of a multi-point detonation, it is sensible to explore the incorporation of multi-point safety technologies.

In general, it is important to recognize that any modifications to benefit safety or security will entail costs and performance risks. These include financial costs for research, technology development and systems engineering as well as for deployment. Adding

features that entail increases in mass or volume lead to performance tradeoffs. Additional engineering complexity can introduce new failure modes and increase failure risk. Changes involving the nuclear explosive package may make performance certification more difficult. If a feature designed to prevent an accidental explosion is added, its efficacy must be certified, and the continued reliability of the weapon (it must perform as designed despite the addition of features designed to prevent an explosion) must be certified.

C. Surety Responsibilities

Guidance for nuclear weapon safety and security is currently based on the 2003 National Security Presidential Directive (NSPD) 28: *United States Nuclear Command and Control, Safety and Security.* The objective is to prevent a safety or security failure while sustaining stockpile effectiveness. The approach is to implement a layered and functionally integrated system of "positive" measures that consist of both technical and administrative controls.

The DOD and the NNSA share responsibility for safety, security and reliability of U.S. nuclear weapons. The two work jointly to assess safety and security in a comprehensive way. One component of the work is to develop external safety and security improvements that do not require modifications to the warhead. However, the DOD and the NNSA also see life extension programs that modify warheads as a means to improve the safety and security of U.S. nuclear weapons. Key requirements for such safety and security improvements are that they have minimal impact on the reliability of the nuclear deterrent, and that they do not require nuclear explosion testing.

D. Safety and Security Improvements and Life Extension Programs

In the NNSA's view, life extension programs (LEPs) present opportunities to build safety and security improvements into weapons. Five LEPs are currently under way. The W76-1, which replaces the W76, is in production and should be completed in 2019. The remaining four LEPs are in the development stage. The NNSA plans to replace the B61-3/4/7/10 bombs with the B61-12; the W88 with the W88 Alt 370; the W80 with a new cruise missile warhead; and the W78/W88-1 with a new interoperable warhead (IW-1) that can be deployed on land- and sea-based long-range missiles. In addition, the NNSA plans to begin development of two more interoperable warheads, in FY2021 and FY2027, respectively.

The W76-1, currently in production, employs conventional HE as did the W76-0. Its surety improvements over the W76-0 are modest.

The NNSA has established surety objectives for all life extension programs beyond the W76-1. The minimum objectives are to:

- Replace all conventional high explosives with insensitive high explosives; and
- Address safety "soft spots."

Additional objectives include:

- Improved detonator safety;
- Enhanced nuclear safety;
- Use of advanced security systems; and
- Improved fire resistance.

One way to improve safety is by replacing the detonators that ignite the explosives around the pit. The B61 LEP will incorporate new detonators that will offer a modest safety improvement, in part by changing their arrangement.

The NNSA proposes to install IHE across the entire active stockpile. An all-IHE force could have long-term benefits. For example, special care must be taken when handling weapons with conventional high explosives at the Pantex Plant in Texas, where nuclear weapons are assembled and disassembled. Such weapons can be handled only in special facilities at Pantex known as Gravel Gerties, which are designed to contain the special nuclear material in the event of accidental detonation of the high explosive. The small number of Gravel Gerties has led to delays in stockpile work – a problem that an all-IHE stockpile would avoid.

Looking toward the future, at some point the NNSA may need to recapitalize the Pantex Plant. If conventional high explosives are removed from all weapons, it would simplify the safety requirements and allow the new facility to be smaller and less expensive than replacing the existing capability.

An all-IHE force, however, will not happen soon. While more stable, IHE has a lower energy density than conventional high explosive, so more of it must be used. Moreover different weapon systems have different security environments, leading to different assessments of the threats they face and the desirability of changes. For example, the Navy maintains that its warheads face fewer risks during their life cycle (assembly, transport, loading onto a submarine, and at sea) than does the Air Force B61 bomb. As a result, in the life extension program for the W76 now underway, the Navy refused to allow a switch to IHE. This refurbishment of the W76, which makes up the largest part of the U.S. nuclear force, will be completed in 2019 without IHE and will extend the lives of the warhead for 30 years, significantly setting back the NNSA's objective of an all-IHE stockpile.

The same situation holds with regard to the NNSA's goal of improving fire resistance across the stockpile. The goal is to increase the temperature and the time that pits can withstand fire before any nuclear material is released. At present, only the B83 bomb and the W87 land-based missile-launched warhead have fire resistant pits installed. The current W76 life extension program does not include a fire resistant pit.

There was a spectrum of views with regard to how much change is acceptable in a life extension program. All participants essentially agreed that some change inside the nuclear-explosive package has already been introduced because the United States has adopted different production processes than it used previously. Because the Rocky Flats production facility was closed, the United States is no longer making plutonium pits in the same way; the facility at Los Alamos uses a different manufacturing technique. Despite this change, the weapons labs are confident that newly produced pits will perform more than adequately, in part because weapons were tested with cast pits (the method used at Los Alamos National Laboratory) as well as with wrought pits (the method used by the Rocky Flats Plant).

Over time, some participants had become more comfortable with making changes to the nuclear explosive package. Other participants, however, favored a more conservative approach, with the objective of changing as little as possible while maintaining confidence in the reliability of the existing stockpile.

One participant asked how to evaluate potential warhead changes designed to increase safety and security in light of the requirement that improvements be adopted with minimal impact on nuclear weapon reliability. Non-nuclear components of nuclear weapons can be tested and modified and the reliability of changes assessed statistically, but that is not the case for the nuclear explosive package. The question was raised as to whether changes can be made to the nuclear explosive package with minimal impact.

Several participants said that investments in the Stockpile Stewardship Program and the resulting increase in knowledge about the stockpile and how weapons work allow such changes to be considered with confidence. In making changes, the labs were also informed by past nuclear explosion tests in making similar surety modifications to other weapons. In this view, technologies should not be frozen; as materials and issues are better understood it should be possible to incorporate changes in the nuclear explosive package, even without a nuclear explosion test.

The discussion therefore turned to the challenges of making qualitative judgments, since in the end the assessment of reliability must be based at least in part on expert judgment. This is particularly true considering that the reliability of the nuclear explosive package is taken to be 100 percent. Weapon designers and NNSA officials use the term “O-N-E” (the number one, spelled out) to refer to that reliability. Any changes that are introduced must result in a nuclear explosive package for which the reliability continues to be taken as O-N-E.

Some argued that if changes undermined confidence in reliability then no changes should be made. In response, a participant noted that designers use quantitative analysis (Quantification of Margins and Uncertainties, or QMU analysis) to assess confidence in key performance characteristics, such as whether the nuclear weapon primary will cause the secondary to perform as intended. It was stated that the NNSA requires certification that the introduction of a new technology has “minimal” impact on performance. When

considering new components, designers seek to maintain reliability by keeping performance margins high relative to uncertainties. Most importantly, the assessment that the warhead will work is required to be based on previous nuclear explosion testing data.

This led to a debate among participants about how to think about margins and uncertainties. In the view of some, either there was enough margin for a given uncertainty or there was not. A warhead without enough margin should not be deployed; a warhead with enough will be reliable. There are tolerances built in to ensure reliability. Others asserted that the situation was not as binary as that, not as black and white. In this view, for some existing warheads, improving the margin or developing replacement warheads with larger margins is worthwhile.

One participant noted that five or six years ago, the NNSA made a case for a Reliable Replacement Warhead (RRW) on the grounds that there were concerns about the reliability of the current arsenal, and asked how this was consistent with the requirement that changes made as part of an LEP only *minimize* changes to the reliability rather than have no impact. Some commented that despite its name, the real motivation for the RRW was not increased reliability but increased safety and security. Other rationales included ease of manufacturing and assembly, ease of replacing components in future LEPs, and reduced waste stream.

A Specific Case: the Life Extension Program for the B61 Bomb

Turning from the more theoretical discussion, many participants noted that the NNSA will face challenges if it seeks to pursue a strategy of aggressive life extension programs in an era of budget uncertainties and changing strategic environments. It is possible, for example, that the B61 could be withdrawn from Europe and retired before the life extension program is completed. Some participants argued that the NNSA should, for those reasons, consider a much simpler life extension program that would do the minimum work required to maintain the warheads until their long-term need is established.

For its part, the NNSA refers to the B61 LEP as the first “full-scale” life extension program, where the goal is to update the entire warhead (however, the NNSA did develop the B61-11 and conduct a LEP of the W87 in the 1990s). Some participants raised concerns that some improvements for security, including use control, could interfere with reliability, as well as increase the cost of the LEP. The current cost estimate for the B61 life extension program has risen dramatically. In 2012, the estimate was $4.8 billion; now the NNSA estimates the cost at almost $8 billion while the DOD places the cost at over $10 billion (when using a higher inflation rate for wages and avoiding concurrency in research and development).

Some said that adding safety, security and use-control features has not been a major reason for the cost increase, but this question was not further pursued. The proposed B61-12 will have new detonators in a new configuration that are designed to improve

safety. There are a number of safety, security and use-control features being considered, but they consist of small, marginal improvements. More significant changes, including ones that would have required alterations to the nuclear explosive package, were rejected. Specifically, these included multi-point safety and optical initiators.

The NNSA does plan to improve security by reducing the amount of highly enriched uranium in the B61-12 by choosing the B61-4 as the baseline. In the B61 LEP, four existing models (B61-3, -4, -7, and -10) will be eliminated and replaced by one, the B61-12. That model will be based on the existing B61-4, which is the variant that has the lowest yield and uses the smallest amount of highly enriched uranium. One of the motivations for this approach is the concern that the highly enriched uranium in the weapon could be used if the weapon were lost or stolen or failed to detonate after delivery. Reducing the amount of highly enriched uranium means there would be less material for any potential adversary to use.

E. Non-Deterrable Threats and Access to Nuclear Weapons

As President Obama made clear in his address in Prague on 9 April 2009, the security of nuclear weapons is essential: "…we must ensure that terrorists never acquire a nuclear weapon. This is the most immediate and extreme threat to global security."

According to some participants, President Obama's focus on the terrorist danger reflects the need to adapt the nuclear deterrent to the changing threat environment. During the Cold War, the priority objective was deterring the Soviet Union. The United States deployed nuclear weapons that would produce high yield explosions on their targets, and maintained them on a high alert status. The end of the Cold War decreased the focus on and resources for nuclear weapons, as the stockpile size dropped. Since 9/11, more attention has been paid to strengthening the security of the U.S. arsenal, and addressing the prospect that extremists or sub-national entities might acquire nuclear weapons, a threat that is by and large undeterrable. Many participants noted that the loss of custody of a nuclear weapon would be a major concern.

Participants were divided as to whether security features, including improved use-control features, can prevent a stolen warhead from being detonated. Some participants argued that guns, guards and gates must be able to assure that only authorized users have access. Introducing modifications to the nuclear explosive package should not be necessary. In this view, if loss of control cannot be prevented, the weapon should not be deployed. Another participant observed that this does not mean there is no reason to consider improvements in intrinsic surety features that could potentially prevent unauthorized persons from detonating a weapon (see the discussion of "designer proof" weapons on page 15).

Further discussion concerning undeterrable threats focused on the threat of "homegrown terrorism" in the United States. The United States has faced American terrorists (like the Oklahoma City bomber). Other countries face similar challenges. The Internet has increased the opportunity for such people to connect with like-minded individuals

elsewhere. The combination of ideology with the ability to acquire resources or information means that homegrown terrorism must be considered a serious threat.

For its part, the DOD does not draw a distinction between a deterrable and an undeterrable threat. The objective is for no unauthorized person to have access to a weapon. What has changed is the "threat space"—the risk of theft or detonation of a U.S. nuclear weapon by a subnational group is perceived to have increased. When nuclear weapons were first designed and deployed, theft by subnational groups was not considered as much of a threat as it is today. On the other hand, technology has also changed greatly over three decades, so it is now possible to add new security features to warheads that may help compensate for the increased sophistication of the potential threat.

It was also noted that another threat comes from insiders, people presumed to be reliable who cooperate with outsiders or act on their own.

More broadly, it was argued by some participants that those responsible for nuclear weapons need to find a way to discuss with the public in a serious but non-frightening way that the threat of unauthorized access to nuclear weapons is real. It was suggested that it might also be beneficial to discuss these matters and perhaps share use-control technologies with other states possessing nuclear weapons – even with potential adversaries. However, sharing use-control technologies with other states was characterized as possibly being in a legal grey area with regard to Article I of the Non-Proliferation Treaty.

The use of tags was discussed as one way to deal with the potential theft of a nuclear weapon. One option would be radioactive tags; some noted, however, that these may be problematic due to the low threshold for radiation under worker safety requirements. Another option would be radio-frequency identity tags, although an adversary could potentially detect these tags to identify the location of a weapon. In this regard, one participant proposed a beacon that would transmit if and only if two conditions were met: 1) the absence of a coded signal telling the weapon that it is where it should be, and 2) the presence of a coded signal telling the beacon to transmit. The first signal would be broadcast only by authorized storage or transportation systems, and the second only by authorized search-and-recover operations. These technologies might be shared with other nuclear nations. Another participant asked whether the NNSA and the DOD were receptive to applying these technologies to U.S. weapons.

A concluding observation was offered that it is very difficult for the U.S. government, once it becomes aware of a potential threat, to say that no action is being taken to deal with it. This leads to a situation where the government pursues solutions to every potential threat, thereby complicating attempts to apportion funds and efforts according to a cost-benefit assessment.

F. DOD Approaches to Surety

Given the different environments in which their nuclear weapons are deployed, the Navy and the Air Force may have different requirements for surety improvements made in life extension programs.

From the DOD perspective, surety also includes command and control. Surety must be balanced against the requirement that the weapon is able to perform as intended if called upon. However, in the last analysis, what matters is not so much the beliefs of DOD experts or weapon designers, but what the world believes; adding surety features must not result in a loss of credibility of the U.S. deterrent.

The DOD has a performance requirement for each nuclear weapon system. This is translated into a reliability budget that is apportioned across the entire weapon system, including the delivery system. The DOD gives the NNSA an objective for overall warhead or bomb reliability (the probability that the warhead will explode with the required yield). If this objective is not feasible, the objective is revisited to determine whether the DOD can accept a lower reliability or altered military characteristics.

The DOD has four basic nuclear surety principles (cf. DoDD 3150.2), as follows.

There shall be positive measures to:

- Prevent nuclear weapons involved in accidents or incidents, or jettisoned weapons, from producing a nuclear yield (these quantitative requirements are the same as those imposed by the NNSA and are discussed above);
- Prevent deliberate pre-arming, arming, launching, or releasing of nuclear weapons, except upon execution of emergency war orders or when directed by competent authority;
- Prevent inadvertent pre-arming, arming, launching, or releasing of nuclear weapons in all normal and credible abnormal environments;
- Ensure adequate security of nuclear weapons.

These measures are to be implemented by the combination of personnel, design features in the weapon and platform, barriers, tactics, training, techniques and procedures.

Specifically with regard to security, there are two fundamental tenets:

- Deny unauthorized access to nuclear weapons. There shall be no plausible scenario that may result in the unauthorized access to a nuclear weapon. Security configurations shall be designed to counter the most likely scenario as promulgated in the Nuclear Weapons Threat Matrix; and

- Failing denial of access, commanders shall take any and all actions necessary, including the use of deadly force, to regain control of nuclear weapons immediately.

The DOD allows the use of deadly force to ensure that no unauthorized person can approach a weapon, or seize one. If that happens, according to the DOD, the person will be shot.

The DOD has a Personnel Reliability Program that applies to some eight thousand personnel involved in the handling and protection of nuclear weapons or in nuclear related command and control systems. Such personnel must be U.S. citizens or U.S. nationals, and certification is based on comprehensive screening and continual evaluation. Control is maintained by using a two-person approach, in which two people must both take actions.

A DOD Example of the Human Factor

In 2007, Air Force personnel inadvertently transported air-launched cruise missiles armed with nuclear warheads from Minot Air Force Base in North Dakota to Barksdale Air Force Base in Louisiana. This is an example of the dynamic where inattention and haste led to a deviation from procedure in order to complete a mission. Where multiple layers of defense against a mistake are applied, people often assume that nothing can go wrong. Everyone assumes that everyone else behaves correctly and therefore that a system with multiple checks cannot fail (even if one person fails). But the objective in the nuclear enterprise is zero error. The system as a whole needs to be resilient.

One participant noted that officials commonly provided assurances, before this failure, that the system was foolproof. Now, afterwards, with some new systems in place, use of the word “foolproof” is returning again. In any complicated system with humans involved, “foolproof” is an aspiration that cannot be assured with absolute confidence.

Use Control for ICBMs

ICBM launch procedures were discussed as an example of implementing “use control.” The launch process begins with an emergency action message or messages directed by the president. On receipt at an ICBM wing, which has three squadrons, each with five launch control centers, each launch control center processes the message(s). The validity and authenticity are determined, and the Squadron Command Post assigns preparatory actions. An enable code is needed to allow a launch. Simultaneous entry of codes at each of two terminals in a launch control center enables messages to reach the missile. Targets are assigned to warheads. Two launch “votes” from each of two launch control centers are then required to launch the missile: keys and launch switches must be turned simultaneously.

The effectiveness of the “two-person” policy was discussed. In practice, there is a substantially more comprehensive system that involves elements of the missile squadron other than the two-person launch team in a launch control center. For a “rogue” missile

crew to be able to launch an ICBM, it would need to know what the code is to enable the missile. But others in the squadron can inhibit further steps in the launch sequence by removing this code from the sequence of steps leading to launch. In fact, a rogue crew so motivated could block even a valid launch sequence for some time. Within the squadron, each launch control center has the capability to monitor all the other centers, and at least two must always be in a monitoring mode. The probability of having five rogue missile crews, together with a successful guess of the code to enable launch, is considered minimal if the prescribed procedures are implemented in practice without exception.

IV. Cost-Benefit Analysis of Adding Safety and Security Features to Warheads

An overarching point, widely agreed upon, was that proposed changes for safety, security or use control should be subject to a cost-benefit evaluation in the context of the entire safety/security/use-control system for each weapon type. Each weapon system is unique, and a separate evaluation is required for each proposed technology for each weapon system. It is important to consider what features are already in place, or could be put in place. Different environments for different types of weapons mean that there is no "one-size-fits-all" approach.

What was less clear in the workshop was how to develop and apply a useful cost-benefit approach. Concern for the difficulty this challenge presents is widespread, including in the legislative branch. Unsure about how to prioritize proposals for improvements in safety and security in the nuclear stockpile, Congress in the FY11 defense authorization bill required the DOE and the DOD to develop[3]:

- Criteria for determining the appropriate baseline for safety and security of nuclear weapons through the life cycle of such weapons; and
- A methodology for determining the level of safety and security that may be achieved through a life extension program for each type of nuclear weapon.

A report was delivered to Congress in March 2012 on the criteria and methodology for determining the safety and security of nuclear weapons.

A related effort may be more effective. The Joint Integrated Lifecycle Surety (JILS) model is being created now, and represents one of the first times that the NNSA and the DOD will collect information about lifecycle surety to be considered as a whole. At present, the model provides an assessment of the consequences and likelihood of incidents involving each warhead in the stockpile in every venue where it could be, from cradle to grave and stockpile to target. The three weapons labs are each participating directly in the work,

[3] National Defense Authorization Act for Fiscal Year, 2011, Public Law 111–383, Section 1063.

with the help of outside consultants. DOD participation in this work began recently, while the NNSA has been working on it for about two years.

The JILS model is being developed too late to affect the W76 or B61 life extension programs. However, the JILS model now has information that can be used in efforts like the W78/ W88-1 life extension program. Its scope is not limited, so it could, for example, include a consideration of changing the propellant in ICBMs.

The cost-benefit analysis for a given technology for safety and security, including use control, may produce different results when applied to different weapon systems or even to a given system in different stages of its life cycle. This cost-benefit analysis should take into account explicitly the widely different damage that will result under different surety-failure scenarios, such as: a) only the high explosive of the nuclear weapon is detonated, scattering plutonium but producing no nuclear yield, b) the weapon gives the unboosted yield, c) the weapon gives the full primary yield, or d) the weapon gives the full yield of the two-stage weapon. None of these is a desirable outcome, but it is certainly preferable to have a high explosive detonation rather than a nuclear yield, and these different possible outcomes should be given different weights when deciding on procedures or allocation of resources.

Much of the discussion in the workshop focused on the desirability of intrinsic changes in the nuclear explosive package that seek to provide "self-protection" of the weapon in the event that other security measures fail. In this approach, the NNSA has cited the ultimate objective of a "designer proof" weapon, where even if a warhead fell into very technically capable hands, it could not be used. (For example, this could include disablement or "self-destruct" technologies to damage the pit.)

In discussing use control, one participant said that intrinsic features would not preclude a group from extracting the fissile material from a stolen weapon or weapons. This could be used to construct another weapon. Another participant responded that there may be ways to preclude material reuse by actors who do not have the major facilities usually associated with nation-states. This prospect was questioned, and the observation made that the objective must be to retain custody of a weapon; failing that, the assumption should be that the weapon or its material could be used to cause a nuclear explosion. Other participants suggested that such intrinsic features could nevertheless add a meaningful additional layer of security that might prevent a detonation if a weapon was stolen.

More broadly, a number of participants argued strongly that more attention needed to be paid to safety and security measures outside the nuclear explosive package. They argued that this approach has several distinct benefits:

- First, it can be completed more quickly than changes inside the nuclear explosive package. Addressing concerns across the stockpile via

modifications to the nuclear explosive package would take decades, while external improvements could happen within years or even months;

- Second, improvements outside the nuclear explosive package do not create concerns about the reliability of the stockpile. The NNSA has expressed confidence that changes inside the nuclear explosive package can be made while maintaining if not improving reliability. However, external changes offer a nearly risk-free approach to improving safety and security; and
- Third, the monetary costs of external improvements can be significantly less. For example, improving the fleet of vehicles that transport nuclear warheads would seem to offer opportunities for a positive impact at an effective cost.

A. The Reliable Replacement Warhead

In 2004, after cancelling the Robust Nuclear Earth Penetrator program that would have created a new "bunker-busting" weapon, the House Appropriations Committee proposed a different strategy. It funded the Reliable Replacement Warhead (RRW) as a more appropriate approach in the post-Cold War era. The committee wanted to send a message that it did not support efforts to produce new types of warheads, but wanted to focus on maintaining the existing stockpile.

However, despite the name of the RRW program, the issue was not that existing warheads had reliability problems. As work on the RRW proceeded, the NNSA developed a weapon that it believed had many advantages over existing warheads. According to one participant, in designing the RRW, the major objective was to provide large margins based on experience with prior designs. Such margins would mitigate potential design problems and support maintaining reliability. Additional objectives were to include additional safety and security features. One participant expressed the view that, in the end, the primary goal of the RRW was to increase safety and security. The increased margins were the way to ensure that changes made to increase surety did not affect the reliability of the warhead.

The NNSA also cited other objectives for the RRW, including improved worker safety, a reduction in the use of hazardous materials, and a reduction in waste. One workshop participant noted "The last time I counted there were 56 reasons to do the RRW."

The final design that was selected for the first RRW (called WR1) was based on a warhead that had previously been tested, although not deployed in the stockpile, but incorporated a number of newer technologies and design features. The NNSA was also planning a second RRW, based on another design, and envisioned a "family" of warheads designed using RRW principles.

In the view of some in Congress, the program's expansion became a reason to stop it. In this view, the RRW had shifted from a modest program to ensure reliability to a broad, multi-warhead program designed to ensure funding streams and the reconstitution of the

weapons complex. After initiating the program, and providing 3-4 years of support, the House Appropriations Committee ended it.

Some participants thought that the ostensible goal of the RRW program was misunderstood. They reasoned that if the program had been pursued to increase surety rather than reliability, it might have succeeded and the stockpile would be on a better path.

B. The 2009 JASON Study

A 2009 study[4] by the JASON group advised the NNSA on "LEP strategies for maintaining the U.S. nuclear deterrent in the absence of underground nuclear testing." Because significant sections of that study are relevant to safety and security issues, several findings and recommendations were highlighted at the workshop, including:

- "Further scientific research and engineering development is required for some proposed surety systems";
- "Implementation of intrinsic surety features in today's re-entry systems, using the technologies proposed to date, would require reuse or replacement LEP options";
- "All proposed surety features for today's air-carried systems could be implemented through reuse LEP options"; and
- "Implementation of intrinsic surety features across the entire stockpile [of nuclear weapons] would require more than a decade to complete."

It was noted in the workshop that the phrase "more than a decade" in the final bullet was a significant understatement of the time required to install surety features across the stockpile: it would take considerably more time to introduce new intrinsic surety features in all weapons.

The JASON report also provided a context for discussing certification challenges associated with implementing proposed surety features. In particular, the following points from the JASON report were flagged:

- "The basis for assessment and certification is linkage to underground test data, scientific understanding, and results from experiment";
- "Increased scientific understanding enables reduced reliance on calibration, enhanced predictive capability, and improved quantification of margins and uncertainties"; and
- "Certification of certain reuse or replacement options would require improved understanding of boost."

[4]Executive summary available at http://www.fas.org/irp/agency/dod/jason/lep.pdf.

Additional recommendations in the JASON report include:

- "Strengthen and focus science programs to anticipate and meet potential challenges of future LEP options, including challenges associated with boost and surety science"; and
- "Assess the benefits of surety technologies in the context of the nuclear weapons enterprise as a system, including technologies that can be employed in the near term."

One participant added that another recommendation would be to manage the development and maturation of surety technologies, something the NNSA is now working on.

The Question of Boost

Boost has been used in nuclear weapons for many years. In the primary of a two-stage nuclear weapon, the fission reaction can be "boosted" so that a greater fraction of the plutonium fissions. To achieve this, hydrogen gas (consisting of the isotopes deuterium and tritium[5]) is injected into the hollow center of the plutonium pit just before the implosion begins. As the plutonium fissions, enough heat and pressure are produced to cause the hydrogen to undergo fusion, releasing a burst of high-energy neutrons that, in turn, induce additional fissions in the plutonium.

The group discussed the JASON recommendation pointing out that certification of options for reuse or replacement would require an improved understanding of boost. The discussion focused in particular on safety and security modifications to the nuclear explosive package. More generally, the discussion related to understanding possible effects of aging, anomalies and failures that were detected during nuclear tests, gaining a better understanding of the potential capabilities of other states, and ensuring that the performance margin of a primary was maintained by the boost gas system. It was also stated that for some weapons the boost gas system has been changed because the margin was less than desired under certain adverse circumstances. It was possible to increase the margin to a satisfactory level by adopting a different system for storage and injection of the boost gas. The National Boost Initiative is pursuing a better understanding of boost.

V. Cybersecurity and Nuclear Weapon Surety

The discussion of nuclear weapon surety in the context of cybersecurity was based in large part on a presentation on cybersecurity, in turn based on previous discussions at the National Academy of Sciences and American Academy of Arts and Sciences, and the work of the National Research Council Committee on Deterring Cyber Attacks.

[5] Deuterium has one neutron, and tritium has two. All hydrogen isotopes have one proton.

Regarding cybersecurity in general, the basic element is the Internet, originally envisaged as a global network of 100,000 main frame computers but that has evolved into a global network of a billion personal computers. It has become a global public utility, without central direction, and essential to the daily operation of the global economy.

The security problem arises because the original protocols were designed to assure anonymity and freedom of use, which has empowered entrepreneurs and dissidents, but also predators. Although technical vulnerabilities can in principle be reduced, they cannot be entirely eliminated, and established expertise is insufficient to deal with them. While espionage has been widespread, and disruption has occurred frequently, thus far the system has not suffered serious destruction.

The advantage of offensive cyber weapons over defenses was characterized as giving incentive to offensive strategies, particularly since inherent difficulties in attribution render deterrence by punishment impractical in the cyber realm. This situation, it was argued by some, suggested that multilateral cooperation on cybersecurity was critical, though participants reached no strong conclusions as to the nature, utility, or practicality of such cooperation.

In relation to nuclear weapon surety, issues that were raised included the degree that nuclear weapon command and control systems are separate from the Internet. Allegedly, U.S. command and control systems are not connected to the Internet; however, keeping networks disconnected can be difficult in practice. Even offline networks are vulnerable to attack from malicious code via portable media, such as CDs or USB drives. Another question is whether isolated systems are more prone to sustained error than open, transparent systems.

Even if nuclear command and control networks were successfully guarded against cyberattack, concerns were raised as to whether difficult-to-attribute cyberattacks on key civilian and military networks might lead to mistaken escalation in a crisis.

Nuclear weapon surety, cybersecurity and prompt alert operations

The second of the Shultz-Kissinger-Nunn-Perry op-eds on eliminating nuclear weapons in *The Wall Street Journal* pointed to disastrous consequences if command and control systems were compromised by hackers.[6] In a 2012 article in *Foreign Policy,*[7] Maj. General William Chambers addressed the 2010 lapse in communications with the 50 ICBMs at F.E. Warren Air Force Base in Wyoming and reported that there was a need to review the entire nuclear weapon command and control structure to ensure adequate security when undertaking modernization.

[6] George P. Shultz, William J. Perry, Henry A. Kissinger and Sam Nunn "Toward a Nuclear-Free World," *Wall Street Journal*, 15 January 2008. Available online at http://online.wsj.com/article/SB120036422673589947.html.

[7] John Reed, "Keeping nukes safe from cyber attack," *Foreign Policy,* 25 September 2012. Available online at http://killerapps.foreignpolicy.com/posts/2012/09/25/keeping_nukes_safe_from_cyber_attack.

One participant said that inherent doubt about continued system integrity is a reason to terminate “prompt alert” operations. This would apply in particular to the Russian system. Although on a day-to-day basis there is a negligible risk of an unauthorized action, the global situation gives serious reason to think about comprehensive de-alerting. It was argued that the United States could engage in productive dialogue with other nuclear weapon states – including at least Russia and China – on the issue of command and control network security.