Science & Global Security, Volume 9 pp 113-141

0892-9882/01 $12.00 + .00

A Proposed Approach for Monitoring Nuclear Warhead Dismantlement

Eric R. Gerdes[a], Roger G. Johnston[b], and James E. Doyle[c]

Two novel approaches for monitoring nuclear warhead dismantlement have been developed by the Applied Monitoring and Transparency Laboratory at Los Alamos National Lab. These approaches were recently demonstrated at Pantex and in the Device Assembly Facility (DAF) at the Nevada Test Site. The systems used to demonstrate these concepts are called the Integrated Facility Monitoring System (IFMS) and the Magazine Transparency System (MTS). IFMS is intended as a limited chain-of-custody system for monitoring dismantlement operations, while MTS can be used for short or long-term storage (and possibly the transport) of nuclear weapons, components, and materials. Both IFMS and MTS possess a number of the attributes required for an effective START III regime including negotiability, simplicity, good confidence and transparency, minimal invasiveness, limited needed for the presence of foreign personnel or hardware inside nuclear facilities, protection for classified information, and no compromise of domestic nuclear security and safeguards. Additional testing of these approaches under realistic conditions will improve the chances that such systems could be used effectively in future arms control agreements.

INTRODUCTION

At the Helsinki summit of March 21, 1997, the United States and the Russian Federation established a framework agreement for a third Strategic Arms Reduction Treaty.[1] For the first time, the two sides agreed to negotiate arms control measures directly relating to the reduction of nuclear warheads. This commitment presents important opportunities, but also poses significant challenges.

The original version of this manuscript was received by *Science & Global Security* on 16 August, 2000.
a Technical Staff Member, Nonproliferation and International Security Division, Los Alamos National Laboratory
b Team Leader, Vulnerability Assessment Team, Los Alamos National Laboratory
c Director, Applied Monitoring and Transparency Laboratory, Los Alamos National Laboratory

A bilateral agreement on nuclear warheads as part of the next strategic nuclear arms treaty has several potential benefits for U.S. and Russian national security.[2] First, limits on warheads and their associated fissile materials would make nuclear arms reductions far more difficult to reverse. Without verified elimination or bilateral monitoring of excess nuclear warheads, these weapons could be re-deployed in active stockpiles. Second, mutual suspicions regarding clandestine stockpiles will prevent much deeper reductions in nuclear arsenals unless verified limits on total quantities of available warheads and fissile materials are established. A warhead and fissile material treaty regime could also build mutual confidence that these items are safe and secure.

To provide these potential benefits, any agreement directly limiting warhead inventories or monitoring the dismantlement of nuclear warheads must overcome a range of political and technological difficulties.[3] Nuclear warheads are relatively small and can be hidden or diverted from a storage facility. Further complicating the problem is the fact that the United States and Russia keep secret the number of nuclear warheads they have produced, recycled, and eliminated. Indeed, great care will need to be taken to prevent the loss of classified information while also allowing the inspection or monitoring activities necessary to confirm treaty compliance.[4] The nuclear warhead and component storage facilities and assembly/disassembly plants where inspections for a warhead arms control treaty would take place are some of the most sensitive government installations in the United States and Russia. There can be no release of classified details of warhead designs, the readiness of nuclear forces, or information that would aid an adversary attempting to disable or steal nuclear warheads. Finally, there are serious concerns that the actions necessary to demonstrate compliance with a warhead limitation or reduction agreement would be too intrusive. The nuclear facilities that will be monitored in each country will probably need to conduct non-treaty stockpile maintenance operations simultaneously with treaty-monitored operations. The two activities cannot seriously interfere with each other.

It is clear that negotiating the details of implementing nuclear warhead reductions will be difficult. New, innovative and non-intrusive techniques for monitoring compliance with a warhead treaty regime are needed to provide confidence that required treaty activities are taking place, while simultaneously protecting classified information. Traditional on-site inspections or verification by national technical means will not be adequate. Rather, a skillful combination of jointly approved technologies and procedures (“protocols”) will be needed for successful treaty implementation.

In an attempt to address some of the challenges of the next stages of U.S.-

Russian nuclear arms reductions--likely to be called START III--Los Alamos National Laboratory (LANL) has developed two prototype systems for monitoring the storage and dismantlement of nuclear weapons and components. These systems take an innovative approach to reciprocal monitoring of the dismantlement process. They are designed to meet the goal of providing high levels of negotiability and mutual confidence. They are also designed to minimize interference with non-treaty-limited nuclear stockpile operations within the nuclear facilities of the potential treaty partners.

PROTOTYPE MONITORING SYSTEMS

The first system, known as the Integrated Facility Monitoring System (IFMS), was initially demonstrated at the Device Assembly Facility (DAF) at the Nevada Test Site in the spring of 1999, and again at the Pantex nuclear weapons assembly/disassembly plant in Amarillo, Texas in November of 1999.[5] The second system is called the Magazine Transparency System (MTS). It was also demonstrated at Pantex in November of 1999. The components for both the IFMS and MTS passed a Nuclear Explosive Safety (NES) review. The development of these systems was initiated with Laboratory-Directed Research and Development funds at Los Alamos and partly supported by the Energy Department's Office of Nonproliferation and National Security.

The IFMS uses commercial off-the-shelf hardware and custom LANL software to track nuclear weapon and nuclear component containers during the dismantlement process, providing strong evidence that nuclear warheads have been dismantled in accordance with a potential treaty. The IFMS is a limited chain-of-custody system that can monitor nuclear warhead containers from the point at which the nuclear warheads are authenticated as treaty-limited items, through stops at various dismantlement bays, all the way to some final on-site storage of the nuclear weapons components. The IFMS is intended to provide confidence that treaty activities are taking place as declared, while protecting sensitive and classified information.

The IFMS uses a combination of live sensors, video cameras, tags, tamper-indicating seals, and a computer-based expert system to track treaty-limited nuclear warheads and components. The use of modular sensor suites allows flexibility for monitoring different facility locations as determined by treaty commitments.

The second major system, MTS, is designed to monitor treaty-limited items in a magazine during either short-term storage prior to dismantlement, or for long-term storage after dismantlement. It may also have applications

for monitoring the long-distance transport of nuclear components and materials. The MTS consists of tags, seals, video cameras, and a notebook computer internal to the storage magazine to monitor treaty-limited items stored within.

FUNDAMENTAL PRECEPTS

Several postulates regarding the fundamental principals needed for a negotiable and effective nuclear warhead monitoring regime were established to help development of the IFMS and MTS. The postulates, discussed below, deal with basic treaty objectives, technical approaches, and inspection protocols.

At Least Some Monitoring of the Warhead Dismantlement Process is Essential

Without monitoring the warhead dismantlement process, it will be difficult for a new treaty to meet the objectives of the Helsinki Summit Statement.[1,2] Hypothetical treaty regimes that do not include monitoring within the dismantlement facility, or at least robust portal-perimeter monitoring, offer little confidence that treaty-declared warheads have actually been dismantled. This is because the weapons components that would be checked at the back end of the dismantlement process could be surplus that were never in fully assembled nuclear warheads in the first place, or that may have resulted from the disassembly of warheads other than those declared for dismantlement under the treaty. Only by maintaining a chain of custody on the set of warheads declared for monitored dismantlement from the point of receipt prior to disassembly through the disassembly process (and also accounting for the resulting warhead components), can high confidence be gained that the declared warheads were dismantled.

Dedicated Treaty Monitoring Systems are Needed

Another assumption that influenced our technical and procedural approaches was that treaty monitoring systems will neither replace, nor be direct extensions of, existing domestic nuclear stockpile security and safeguards measures. This assumption (often overlooked in treaty monitoring discussions) was made for several reasons.

First, domestic systems contain much more detailed information on the disposition of the nuclear stockpile than could be provided to a foreign government for treaty purposes.[4] National statutes and DOE orders forbid the disclosure of detailed information on domestic nuclear weapon inventory control due to security concerns. Second, there are fundamental differences in the

requirements for domestic nuclear weapons security systems and those for bilateral or multilateral treaty monitoring. The primary goal of domestic monitoring systems is to prevent loss or diversion of nuclear materials and to assist with nuclear materials control, accountability, and safety. Domestic security and safeguards are designed to deny unauthorized access to nuclear weapons and materials and to conceal information on weapons design and operational procedures. By contrast, arms control transparency measures seek to provide information of sufficient detail and authenticity to convince inspecting parties that the other side is complying with treaty requirements.

Another key difference is that for domestic security and safeguard systems, information regarding the status of nuclear weapons or materials provided by a manufacturer or previous custodian is generally regarded as authentic. This would not automatically be the case for information provided by one country to another for the purposes of monitoring treaty compliance. Moreover, nuclear facilities and agencies with custody of nuclear warheads already must follow a variety of regulations, procedures, security measures, classification rules, and safety requirements. It would be difficult, expensive, and extremely time-consuming to modify these complex arrangements in order to integrate specialized treaty monitoring functions.[6]

There is also a great disparity between the operational and performance environments for domestic security and safeguards systems as compared to treaty monitoring systems. Even the temporary loss or diversion of a single nuclear weapon is a major catastrophe for an internal security and safeguards program. Treaty inspections, on the other hand, need not be seriously threatened by temporary uncertainty about the status of a few of the nuclear weapons being dismantled.[7] In fact, any successful treaty will likely need robust mechanisms and protocols for resolving item tracking and accounting questions during inspections.

As a final reason for needing dedicated monitoring systems, we note that the risk of weakening domestic security and accounting systems by making them perform treaty monitoring functions may simply be unacceptable in the context of overall national security.

Monitoring Technologies Should be Procured and Maintained by the Inspected Party

Another fundamental precept used in designing our prototype monitoring systems is the idea that the inspected (host) party should procure the monitoring systems that will be used in their facilities. Following this rule to the maximum possible extent can help eliminate a number of serious (and difficult to negotiate) issues concerning nuclear safety and espionage. For example, any

equipment used in a nuclear weapons facility must pass rigorous safety evaluations. To be done efficiently and effectively, these evaluations should begin during system development and be conducted with the participation of the user facility. Monitoring systems brought to a facility by a foreign inspecting party would be extremely difficult to evaluate in a reasonable time period. Another major obstacle to using inspector-provided equipment is the likely suspicion on the part of the inspected party that foreign equipment would include clandestine intelligence-gathering capabilities. For these reasons it is likely that both Russia and the U.S. will insist that only host (or jointly) provided equipment be used for on-site monitoring of future nuclear arms reduction agreements.

The Performance and Data from Host-Provided Equipment Must be Reliably Verified by the Inspecting Party

A treaty regime that intrinsically relies on hardware provided by the host (or inspected) party creates a corresponding set of problems. The primary concern of the inspectors will be that the monitoring equipment has been clandestinely modified to falsely indicate that the host is complying with treaty requirements. Therefore the treaty will need to include procedures that assure inspectors the performance and data from monitoring systems are accurate and authentic.[8]

A layered approach to providing such assurances is likely to be most effective. A first level of confidence-building could be achieved by reciprocal familiarization visits by joint delegations to nuclear warhead dismantlement facilities in the U.S. and Russia. During these visits the host facility would describe the process used to dismantle treaty-accountable warheads. The host would also demonstrate the monitoring equipment that they propose to use for demonstrating compliance with treaty requirements. The visiting side would be presented with the technical specifications and procedure documents for the monitoring systems and may even be permitted to retain and analyze some monitoring sub-systems or components. Joint development of monitoring systems is another alternative that could have clear advantages in this regard.

A second level of confidence could be established during an initialization period at facilities where treaty monitoring will take place. This step would occur just prior to the beginning of treaty-monitored dismantlement activities and include exercising the monitoring equipment with inspector participation to verify performance. During the initialization period (and also at random time during treaty monitoring) specialized protocols could be used to further increase confidence in the authentic performance of the monitoring equip-

ment.

Two such techniques, which we call the "choose or keep" and "keep the used parts" protocols, were incorporated into the IFMS and MTS demonstrations. Under the "choose or keep" approach, the inspectors are allowed to choose in real-time or near real-time (either in person or by request from a remote monitoring location) which of several identical host-provided monitoring sub-systems (such as tamper-indicating seals) will be installed on actual treaty-limited items. They are allowed to keep (and take home for analysis) one or more of the sub-systems or components not chosen for use, in order to check for flaws, signs of tampering, or spoofing. Under the "keep the used parts" protocol, inspectors are permitted to keep some or all of the used monitoring system parts or sub-systems for analysis after the equipment has performed its assigned treaty functions. Both these protocols provide the inspectors with a random check on host-provided hardware and an opportunity to detect tampering or cheating.[9]

A third layer of confidence could be provided by several simple techniques for authenticating sensor data of dismantlement operations as part of a treaty monitoring system. This approach was also used in the IFMS prototype and demonstrated at the Pantex Plant. For example, inspectors can call for a "live verify" of the video data from a dismantlement facility. One simple technique would be for the inspector viewing video images from the dismantlement facility to ask host personnel who are conducting the dismantlement operations to perform a specific hand or body motion or gesture in front of one of the monitoring camera. Seeing the requested action performed in real-time demonstrates to an inspector that the video signal is likely to be authentic and live. Inspectors may also call for a "local verify" protocol to demonstrates with some level of confidence that the monitored video transmissions are emanating from the declared dismantlement facility. Both "local verify" and "live verify" protocols are discussed in more detail below.

Inspector Presence and Impact on Facility Operations Should be Minimized

Because of the sensitive nature of warhead dismantlement operations and the fact that neither Russia nor the United States have designated active dismantlement facilities that can be dedicated exclusively to treaty-monitored operations, it is essential that monitoring approaches be designed for facilities that would continue to conduct non-treaty nuclear weapon operations. Consequently, the need exists to select monitoring technologies and protocols that strictly limit the scope of monitoring to only those activities required for treaty compliance.

Demonstrations of the IFMS and MTS systems at the Pantex Plant pro-

vided proof of concept that treaty monitoring could take place within an operating facility. IFMS system components are designed to have a minimal impact on existing dismantlement workspaces and are easy to install, modify, turn on/off, or remove. The great majority of monitoring operations can be performed and authenticated by inspectors from a remote location outside of the facility. For example, one of the few requirements for inspector presence is for the initial and final sweeps of dismantlement bays to ensure that they contain no non-treaty-limited items. Foreign inspectors may also need to perform occasional in-person challenge inspections to verify, for example, that containers declared to contain non-nuclear weapon components have the appropriate radiation signature.[10]

Although the treaty could limit the frequency of such inspections, the very presence of foreign personnel in a nuclear facility during warhead dismantlement operations causes significant problems. It is likely that certain disassembly bays and cells would have to be temporarily dedicated to monitored dismantlement operations as required by a future treaty. A major focus of further research, development, and testing of monitoring systems and protocols should be to simplify procedures in order to reduce their impact on non-treaty operations.

The Treaty Should Challenge the Host Facility to Demonstrate Compliance

A final precept worth considering has to do with the psychological or "human factors" approach to joint monitoring of the dismantlement process. If completed, START III will represent a step towards increased trust and cooperation between the two signatories. Conventional approaches for monitoring arms control treaties, however, tend to place an emphasis on inspectors uncovering non-compliant activities committed by the host. The inspectors thus tend to be viewed by personnel in the host nuclear facility as adversarial auditors. Under this approach, "winning" for the host personnel can come to be viewed (either consciously or subconsciously) as fooling the inspectors. It would be better from a "human factors" perspective for the treaty to require the dismantlement facility to demonstrate that it is in compliance with the treaty. "Winning" from the standpoint of the facility personnel then involves successfully convincing the inspectors that the treaty is being properly implemented. The IFMS and MTS approaches, with their live sensor feeds, are consistent with this goal.

THE IFMS SYSTEM

The Integrated Facility Monitoring System (IFMS) consists of four sub-systems: the Central Monitoring Station (CMS) where the foreign inspectors primarily reside, the Integrated Tamper-Indicating Device (ITID) which rides attached to the weapon and component containers, the Cart-Cam (CC) that provides the inspectors with a close-up video view of ITID installation and removal, and the Integrated Monitoring Station (IMS) that monitors the comings and goings at the entrance of dismantlement bays and cells. See Figure 1. Appendix B contains an abbreviated list of general steps involved in operating the IFMS system.

Central Monitoring Station (CMS)

The Central Monitoring Station (CMS) is the display and assessment center for all monitoring data collected by the IFMS. It would ordinarily be staffed by foreign inspectors, and would be located somewhere outside the nuclear facility being monitored, ideally nearby. Treaty-monitored dismantlement activities can be viewed via real-time video at the CMS. Past events can also be retrieved from archives. All video and sensor data sent to the Central Monitoring Station by the IFMS are live and unclassified.

The video signals sent by the IFMS are processed at the CMS by LANL-developed NTVision software. This program stores only video segments where motion occurs, thereby reducing the amount of data stored on the computers and the amount of video that the inspectors must review.[11] In addition, an expert system was developed to integrate sensor information with known disassembly protocols to ensure treaty compliance and maintain an inventory of treaty-limited items. Examples of protocol violations that the expert system can detect are excess time of movement between process stages, inventory discrepancies, and improper installation of the ITID.

The CMS can also be used to monitor data sent from the Magazine Transparency System (MTS), which is used to monitor temporary or long-term storage of weapon containers.

Integrated Tamper-Indicating Device (ITID)

The Integrated Tamper-Indicating Device (ITID) is an IFMS sub-system that is attached to every container holding a declared treaty-limited weapon or component. The ITID consists of a tamper-indicating seal to detect tampering with the container, an infrared (IR) tag to identify the container, a miniature

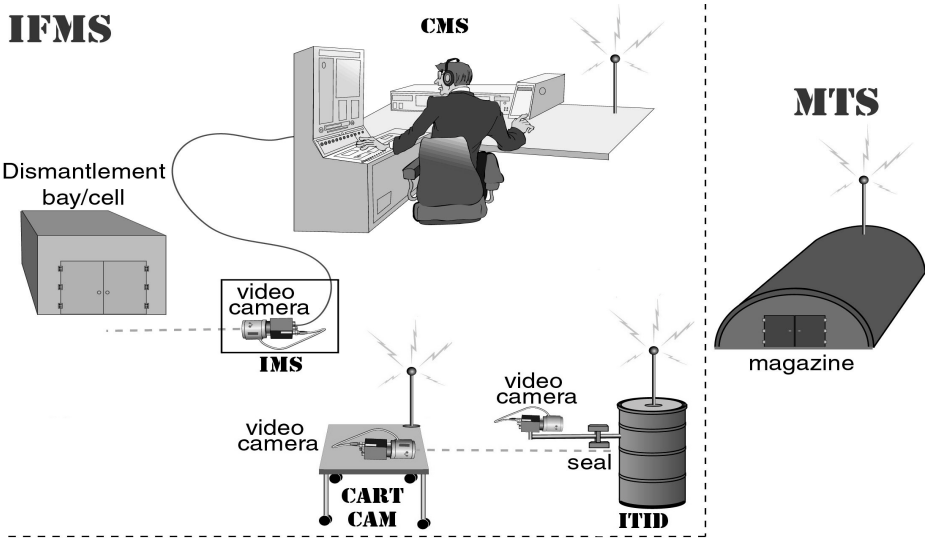

Figure 1: A schematic of the Integrated Facility Monitoring System (IFMS) and the Magazine Transparency System (MTS). The IFMS subsystems are shown (IMS, ITID, Cart-Cam, and CMS). Wireless video transmissions are sent to the Central Monitoring Station (CMS) from the ITID and Cart-Cam. The Integrated Monitoring Station (IMS) outside each dismantlement bay, however, is hard-wired to the CMS. The MTS also sends a low-bandwidth wireless signal (a few baud) to the CMS containing the "All OK" signal, indicating no unauthorized activity. To simplify the diagram, the active IR tag used as part of the ITID, and the IR receiver in the IMS module are not shown.

video camera to monitor the tag and seal, a wireless video transmitter (and battery) to transmit the video image, and mounting hardware to attach the components to the container. [12] See Figure 2. The video camera unit includes an IR illuminator and an IR filter in front of the camera to block ambient room light. This prevents moving shadows and changes in ambient room lighting from being interpreted as a significant video scene change by the NTVision video change detection software located back in the CMS.

The ITID video camera permits the uninterrupted surveillance of the sealed container, as opposed to periodic checks of seal integrity. This may

Figure 2: A photo of a portion of the Integrated Tamper-Indicating Device (ITID) on one type of container. The video camera (with IR illuminator) monitors the seal, its barcode, and a portion of the container. Not shown is the IR tag, or the battery-powered video transmitter that broadcasts the ITID video images. The latter is typically housed in a box that sits on top of the container. The ITID's video camera is focused on a narrow region of the container and shows nothing of facility operations as the container moves through the facility.

greatly improve confidence that no tampering has occurred. The ITID is always removed, under video observation by the IMS and the Cart-Cam, before entering a disassembly bay or cell. This is to avoid transmitting any classified information during the dismantlement process. Any containers emerging from a disassembly bay or cell that are declared to contain treaty-limited items must have an ITID attached before they are permitted to move to a new location.

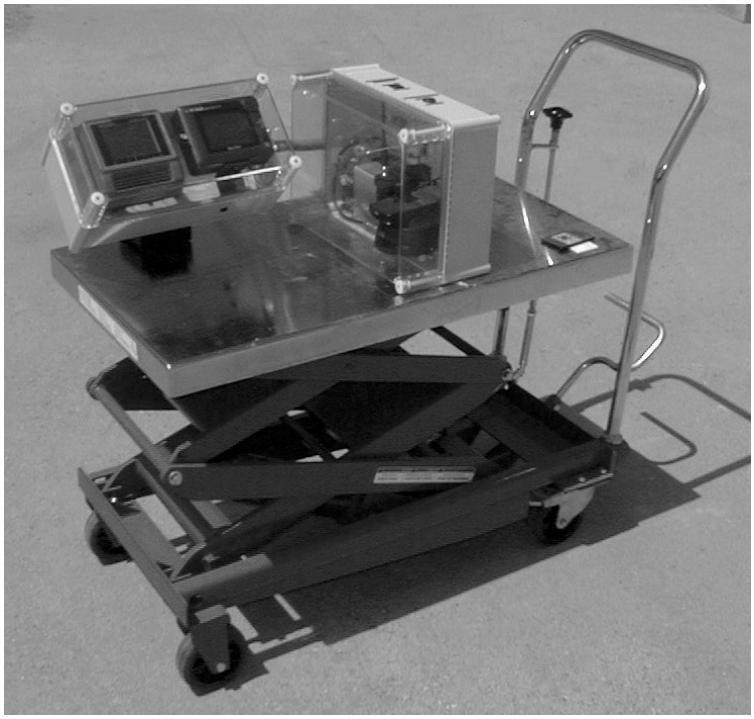

Figure 3: The Cart-Cam used by the IFMS for close-up video images of ITID installation and removal from individual containers.

Cart-Cam

The Cart-Cam (CC) is shown in Figure 3. It consists of a small video pinhole camera, a wireless video transmitter to transmit the video signal back to the CMS, a battery, and a LCD monitor to allow facility personnel to see the camera video image. The CC is rolled up close to a weapon container prior to installing or removing the ITID. The CC allows the inspectors back in the CMS to have a close-up view of the ITID installation or removal process.

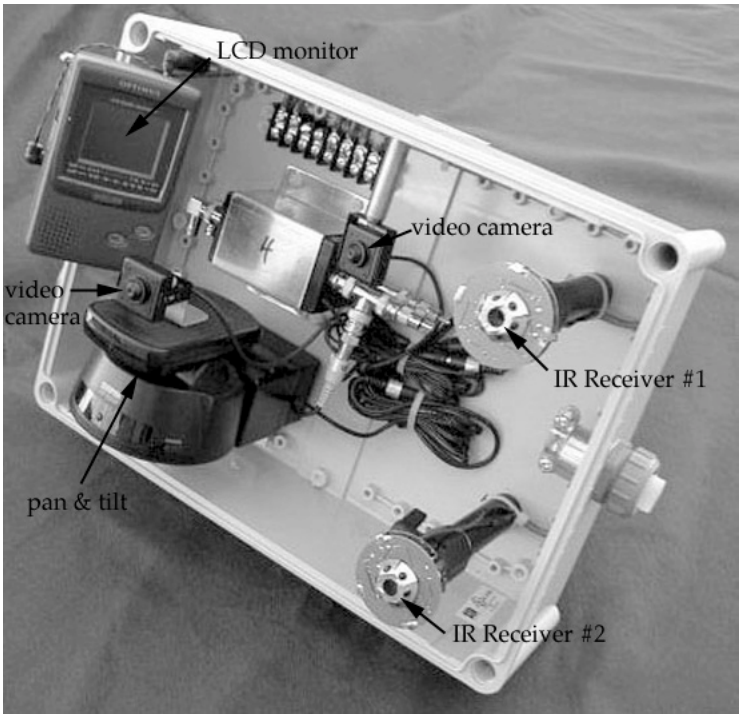

Figure 4: A photo of the Integrated Monitoring Station (IMS) module. One is placed outside each dismantlement bay or cell to monitor activities taking place. The clear polycarbonate cover has been removed in this photo to allow a better view. The components (left to right) are a LCD monitor (for live verify purposes), a pinhole camera mounted on a remote-control pan & tilt unit, a second (fixed) pinhole video camera, and 2 IR tag receivers that read the serial number flashed by the active IR tag attached to each container. A small mirror, which allows the fixed camera to view the LCD monitor in a corner of its field of view, is attached to the clear polycarbonate cover (not shown). The dimensions of the IMS module (including polycarbonate cover) are 38 cm X 28 cm X 18 cm, though it could be greatly miniaturized.

Integrated Monitoring Station (IMS)

The Integrated Monitoring Station (IMS) is shown in Figure 4. The IMS is a sensor module placed outside the entryway to disassembly bays and cells that have been declared for treaty use. It consists of two pinhole video cameras, two infrared tag receivers (for redundancy), and a small LCD monitor. One of the cameras is mounted on a pan and tilt unit that can be remotely operated from several meters away by facility personnel using a hand-held infrared remote control unit. This gives the IMS a stereoscopic view which is useful for

the "live verify" procedures discussed below.

The purpose of the IMS is to track treaty-limited items as they enter and exit disassembly bays, and to monitor the removal and re-attachment of the ITID on weapon and component containers. The IMS continually relays its sensor data (video signals & any infrared tag serial numbers it receives) to the Central Monitoring Station (CMS) for analysis by the inspectors and the computer expert system. Video from the IMS is also sent to nearby LCD monitors located just outside each dismantlement bay or cell. These monitors give the facility personnel a view of the video images being sent to the inspectors in the CMS.

THE MTS SYSTEM

The Magazine Transparency System (MTS) detects unauthorized movement of weapon containers from storage, and maintains magazine inventory. It is installed in magazines or storage areas containing nuclear warheads or components declared for START III use. The MTS can maintain and transfer data on the inventory of stored treaty-limited items to the Central Monitoring Station.

Only passive tags and seals are placed on the weapon containers in the magazine to reduce host country safety and security concerns, and to eliminate the problems associated with finite battery life.

The MTS is intended to be a flexible system, capable of readily accepting new or alternative security sensors. The system demonstrated at Pantex (see Figure 5) had the following elements[13]:

- barcode reader
- low-light video camera
- infrared (IR) illuminators for the video camera
- passive radio frequency (RF) identification tag (transponder) and RF Receiver
- magnetometer with 1 nT resolution
- MAGTAG blanket—a blanket or tarp, containing randomly oriented rare earth magnets plus the RF tag, used to cover each weapon container
- notebook computer to analyze the video, RF tag, magnetometer, and barcode sensor data

- one-time keypad cipher, used by the computer to send the "All OK" signal

All but the MAGTAG blanket, the one-time keypad, and the LANL computer software are off-the-shelf commercial items.

The barcode reader is used to record the barcode on the arms-control seal on each container when it enters or leaves the magazine. This hand-held bar code transmits data to the MTS notebook computer via a wireless pickup unit. Data from the barcode reader, including time stamp, reader number, and bar-code number can be stored in the MTS notebook computer for later analysis, or it can be transmitted from the MTS computer to the Central Monitoring Station (CMS).

For demonstrating MTS at Pantex, we used pinhole monochrome video cameras because of their low cost, light sensitivity, and large depth of field (which eliminates focusing adjustments). The (LED) IR illuminators provide efficient illumination of the storage magazine without the need for additional lighting.

The RF tag we used for the MTS demonstration at Pantex was a passive RF transponder measuring 10.4 x 3.2 x 0.2 cm thick. It requires no batteries for operation but reports its unique serial number when excited by the active RF receiver/antenna. A different RF tag (with a unique serial number) can be used for each container.

The magnetometer and associated software measure the magnetic field within the magazine and detect changes in the field caused by the movement of the permanent magnets randomly sewn into the MAGTAG blankets that cover the weapons or component containers.[14, 15] Typically between 2 and 8 rare earth magnets (Neodymium 30 or Neodymium 35) are used per MAGTAG blanket, each ranging from 2 to 8 cubic centimeters in volume.

The MTS video camera(s) detect any scene changes and the RF tag system interrogates the (passive) RF tag located in the MAGTAG blanket for additional monitoring. Other types of intrusion detectors can be easily incorporated into the MTS system, including acoustic, thermal, microwave, photoelectric, fiber optic, and proximity sensors.

All MTS sensor data is collected and analyzed by a single notebook computer. If the computer senses no anomalous container movement or other unauthorized activity, it sends an "All OK" signal once per second, encrypted via a one-time keypad.[16] The one-time keypad is provided and loaded by the inspectors into the notebook computer just prior to the start of storage monitoring; the one-time keypad is unknown to the host facility. This approach was chosen because it allows for a simple, but unbreakable cipher that is not constrained by national security, proprietary, or export control issues. Even if

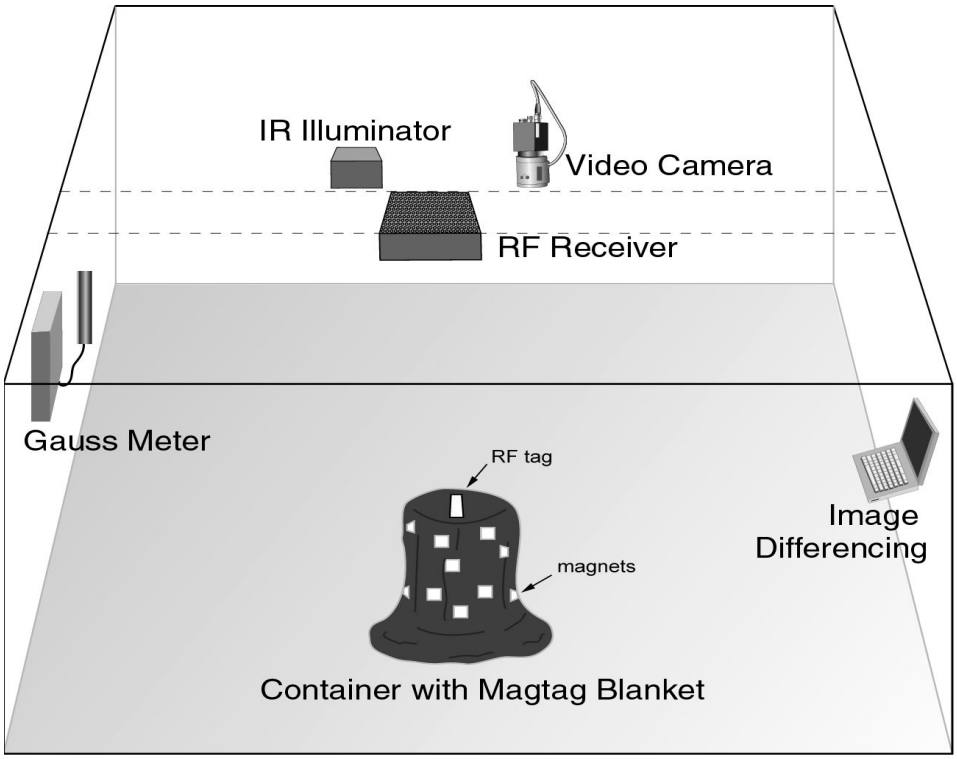

Figure 5: A schematic of the Magazine Transparency System (MTS) showing the primary components.

a one-time keypad is intercepted, its possession is of no value for other magazines or for the same magazine once a new one-time keypad is installed.[17]

If an adversary wanted to gain access to the one-time keypad in order to counterfeit the "All OK" signal, he could do so. Assuming he did not spoof the sensors, however, he would have only 1 second to reach the notebook computer, determine the one-time keypad, block the MTS signal, and begin sending his own counterfeit "All OK" signal.

Note that if the "All OK" signal consists of a single byte per second (8 bps), the one-time keypad needs only 31.5 MB of data per year.[18] In contrast to

other storage monitoring schemes, where streams of high-bandwidth encrypted/authenticated sensor data must be sent by each and every magazine back to a central headquarters for interpretation, the MTS thus has a very low bandwidth requirement.[19]

Should the notebook computer detect container movement or unannounced entry to the magazine, the one-time keypad is incremented so that the inspectors are alerted that there has been an event. The notebook computer stores video, magnetometer, RF tag, and other sensor data for any such events. These recorded files are available to the inspectors to examine when the magazine is reopened so that they can understand what took place. After any such anomalous events, or on a regular basis, the magazine can be opened and the inspectors are then given immediate possession of the notebook computer. They may analyze it for events or signs of tampering.

Appendix C contains an abbreviated list of the general steps involved in using the MTS.

LIVE VERIFY & LOCAL VERIFY

Both IFMS and MTS eliminate much of the need for information barriers and encryption by requiring the host facility to provide continuous, live sensor data (including video signals) to inspectors outside the facility. The veracity of these signals is confirmed by techniques known as “live verify” and “local verify.”

The live verify techniques are intended to increase confidence that the sensor data is live, not pre-recorded. This helps to overcome the inspectors' concerns that they are being fed recorded video and sensor data showing what is supposed to be occurring, rather than what is actually taking place inside the dismantlement facility.

The local verify techniques help to establish that the signals originate from the facility of interest (or at least nearby) and not, in the case of video signals for example, from a dummy location made to look like the facility. The live verify techniques include graffiti methods to “mark” the facility while the inspectors watch via remote cameras. Inspectors are allowed later to inspect and test the markings in person. Time-of-flight data can also be used to establish the approximate distance from the live sensors or video cameras. The finite travel time of electronic signals helps to establish that the live sensor data is emanating from within a few kilometers of the dismantlement facility. This requires the inspectors to provide some kind of random, fast rise-time signal (such as a video transmission) to modulate the live sensors or video

cameras.

IFMS Live Verify

There are a number high-tech ways that live verify tests for the IFMS can be implemented, though we suspect that the simple, low-tech versions will be the most effective. In the case of a video live verify, the inspectors could call for a halt to operations at unannounced times.[20] They would then request that a facility employee (perhaps a specific one) walk in front of one of the video cameras in the IMS module and perform a specified action, such as waving with the left hand. (The specific action would not be announced in advance). Alternately, the employee could be asked to place his hand or fingers in front of the Cart-Cam or ITID cameras and perform a particular motion.[21] He/she could also be asked to hold up a specific card in front of the camera, using a specified orientation or direction of motion, or to shine a flashlight on the scene.

While it certainly is possible for the host facility to switch between prerecorded video and live feed for these live verify checks (or splice in different video signals into a portion of the video frame) in order to try to fool the inspectors, it is very difficult in real-time to get an exact match between the live scene vs. the pre-recorded one. The illumination, shadows, boundaries, and pixel gains seen in the two images are very difficult to match realistically in real-time, at least with current technology. An analysis by the inspectors of the video waveforms, sync signal, or of the image frame-by-frame and pixel-by-pixel is likely to turn up anomalies.[22, 23]

To further complicate any attempt to spoof the inspectors using high-tech, real-time image processing techniques, the inspectors can request at random times that the pan and tilt for one of the cameras in the IMS module be activated. This provides a stereoscopic view of the scene outside the dismantlement bay or cell. Counterfeiting this essentially 3-dimensional image in real-time is much more difficult than counterfeiting a 2-dimensional image.

Other types of IFMS sensors in addition to the video cameras can be tested in a similar manner. For example, the inspectors can call for a specific unused infrared tag with a serial number known only to them to be placed directly in front of a IMS module so that the infrared tag receiver can detect its serial number and pass that information on to the CMS.[24] Strategies and logistics are similar to using calibrated radiation sources to verify the performance of radiation detectors.[25]

IFMS Local Verify

The idea with the time-of-flight local verify test is to use the finite speed of electronic signals to determine that the IFMS video signals must be more or less local. The local verify test can be undertaken without the involvement of host facility personnel.

The IMS module used at Pantex contained a small curved mirror located in the corner of the field of view of one of the video cameras in the module. This mirror allowed the camera to view a small LCD monitor. The monitor displayed a live video feed that would be provided by the inspectors and not known in advance by the host facility. The bandwidth of video signals is sufficient to time the arrival of certain pixel intensity information in the IFMS video signal, based on knowing when they were generated in the inspectors' video signal being sent to the host facility.[26, 27]

Another type of "local verify" check is especially low-tech. It appears to be surprisingly difficult to spoof. At random times, the inspectors request that facility personnel stop operations and spray paint a small spot of graffiti on the facility walls or floors or container, under the watchful eye of the IMS, Cart-Cam, or ITID camera.[28] If the inspectors are allowed into the facility a short time later, they can inspect the graffiti, verify that it is fresh paint, and compare it with their previous video image. Spray-painting is preferred to brush strokes or permanent markers because it has nebulous boundaries that are difficult to quickly replicate accurately. Other, more high-tech ways of marking the facility are also possible.

MTS Live and Local Verify

Performing live and local verify tests on the MTS inside a magazine is somewhat more difficult than for IFMS because the magazine is sealed. Live and local verify tests, however, can always be performed prior to closing the magazine, and shortly after it is opened. Inspectors can also perform live and local verify tests on the MTS magnetometer even after the magazine is sealed. A rare earth magnet or an electromagnet brought to within 10 meters of the magazine can be easily detected by the magnetometer inside the magazine. This will be recorded as an event, as indicated by a shift in the "All OK" signal. The field strength and magnetic vector orientation of the magnet or electromagnet that is used would not be known by the host facility personnel.

ADDITIONAL COMMENTS ON THE IFMS AND MTS APPROACHES

Both the IFMS and the MTS approaches outlined in this paper involve principles and concepts for dismantlement that work quite independently of specific hardware. This flexibility is crucial for planning START III or subsequent treaties because of the unknowns in what can be negotiated between the two countries, our lack of understanding of much of the Russian weapons complex, the rapidly advancing state of technology, and the unexpected surprises and problems that inevitably will accompany any significant effort at something as complex as transparency for nuclear dismantlement.

The hardware that was used for the IFMS and MTS demonstrations was commercially available off-the-shelf. This lowers costs and provides additional comfort levels to facility operators and security personnel. Both IFMS and MTS, and much of the commercial hardware components they use, including the tags and seals, are not currently in use at U.S. government nuclear facilities. This may give the Russians a sense of confidence that the U.S. does not have an unfair decades-long lead in understanding these security devices and their vulnerabilities. It also means that the U.S. side can share these systems without fear of compromising the domestic security at U.S. nuclear facilities.

The hardware used in the IFMS and MTS can be designed, constructed, procured, and packaged in any way that the host facility prefers. Treaty-mandated requirements for the hardware need only involve performance specifications, rather than details about the design, construction, or procurement of the components.

FUTURE WORK

We are in the process of installing working versions of the IFMS and MTS in the new Applied Monitoring and Transparency Facility (AMTL) at Los Alamos National Laboratory. This facility will allow the demonstration and testing of the IFMS and MTS in an unclassified setting available to foreigners. Additional technologies for treaty monitoring, security, and transparency will also be on display.

It is clear that more work needs to be done in the future on tags and seals. Existing tags and seals, whether government or commercial, are not optimally designed for transparency and treaty monitoring. They are designed primarily for conventional security applications.[29] Furthermore, existing tags and seals are far too easily spoofed.[30]

Under the IFMS system, video imaging is used in an unconventional man-

ner to monitor tags and seals on moving containers in real-time. It is certainly not unusual to use video monitoring for domestic nuclear security and safeguards. Traditionally, however, fixed video cameras usually watch the facility, controls, or personnel, rather than directly monitoring moving tags and seals (or traveling along with them). Direct, close-up video monitoring of tags and seals may allow a significant improvement in security, and increased confidence that tampering can be detected. This belief, however, has yet to be thoroughly tested. Existing tags and seals have not been designed with the idea that they would be monitored continuously with close-up video. Seals used in the IFMS approach will require modified designs, mounts, and/or hasps in order to fully exploit this live video monitoring during item movements.[6] Vulnerability assessments need to be conducted that take the presence of live video monitoring into account. Effective use protocols need to be more fully developed and tested in order to exploit the video feature.

Another area requiring further research and development is the one-time keypad cipher for use on the MTS notebook computer inside the magazine. There are many procedural, logistical, software, and vulnerability questions associated with implementing this concept. These issues need to be explored in more detail.

Other issues that require further work include the development of appropriate handoff interfaces between IFMS and storage monitoring systems (including the MTS), as well as transparency methods for monitoring the transport of dismantled weapons to off-site storage areas for permanent storage or eventual conversion. We plan to test the feasibility of using MTS for such applications.

Finally, the IFMS demonstrated at the Nevada Test Site and at Pantex was configured for U.S. nuclear facilities. In Russian, the distances, facilities, and environment may be considerably different. Testing of both the IFMS and the MTS under conditions more realistic for Russian facilities needs to be done before the practicality of these approaches can be fully evaluated.

ACKNOWLEDGMENTS AND DISCLAIMER

This paper was prepared under the auspices of the United States Department of Energy (DOE). The views expressed herein are those of the authors and do not necessarily reflect any official position of Los Alamos National Laboratory or DOE. Kristy Adair, Anthony Garcia, Ron Martinez, Robert Landry, Doug Brubaker, Ken Brodeur, Gregg Titus, Roger Osantowski, Steve Fellows, Sharon Seitz, Caroline Boyle, Cheryl Ammann, Connie Buenafe, Janie Enter,

Eric Baca, and Gerry Ansell contributed significantly to this work. Gracious assistance from personnel at the Pantex Plant and at the DAF at the Nevada Test Site was extensive and essential, and gratefully acknowledged.

APPENDIX A - Acroynms

AMTL: Applied Monitoring and Transparency Laboratory at LANL.

CC: The Cart-Cam used to provide the inspectors with a close-up video view of ITID installation and removal.

CMS: Central Monitoring Station where the foreign inspectors primarily reside.

DAF: The Device Assembly Facility at the Nevada Test Site.

DOE: United States Department of Energy.

IFMS: Integrated Facility Monitoring System, used to monitor the dismantlement process. It consists of 4 sub-systems: the CMS, ITID, CC, and IMS.

IMS: Integrated Monitoring Station located at the entryway to START III dismantlement bays and cells. Includes video cameras and infrared tag readers.

IR: Infrared.

ITID: Integrated Tamper-Indicating Device (ITID) which rides attached to the weapon and component containers to monitor the container seal.

LANL: Los Alamos National Laboratory.

LCD: Liquid Crystal Display.

MAGTAG: The blanket or tarp placed over a container being monitored by MTS. Contains a passive RF tag and randomly oriented rare earth magnets.

MTS: Magazine Transparency System, intended to monitor the storage of nuclear weapons.

RF: Radio frequency.

APPENDIX B - Abridged Sequence of Steps for Using the Integrated Facility Monitoring System (IFMS)

1. Each IMS module located outside a disassembly bay or cell is powered up by the host facility and begins to send live video signals of the entryway to the bay or cell. The IMS modules operate continuously until step 17, which would typically occur a few days to a few weeks later.

2. Inspectors are escorted into the disassembly facility to inspect ("sweep") the dismantlement bays and cells that will be used for the treaty-monitored dismantlement. They look for evidence of undeclared entryways ("trap doors"), and may use radiation detection equipment to check for undeclared nuclear materials inside the bay or cell.

3. A nuclear weapon is authenticated from outside its container using radiation sensors. (This is not part of the IFMS protocol.) The weapon is now officially entered into the dismantlement process. The handoff to the IFMS can occur before or after authentication.

4. The Cart-Cam is rolled close to the weapon container for a close-up view of the ITID installation process. Under observation of the video camera on the Cart-Cam, plus the video cameras in the appropriate IMS module, the ITID is installed using the specific IR tag and seal chosen by the inspectors via the "choose or keep" protocol. (The inspectors may have previously inspected--under close observation by host personnel--the tags and seals provided by the host facility.) The inspectors may veto a particular ITID installation (in which case, it is repeated) if they don't like what they see.

5. Once installed, the ITID video camera and video transmitter are powered up. These provide a live video signal (whether the container is at rest or in motion) showing the container tag and seal, as well as a small portion of the container.

6. The weapon container is now transported to the first dismantlement bay or cell, typically via a forklift. (The ITID video transmission continues while in transit.) The container must arrive at the previously declared dismantlement

bay or cell within the allotted time, or the IFMS expert system at the CMS alerts the inspectors. The video image transmitted by the ITID must not change substantially during transit (such as would occur with tampering), or the NTVision software at the CMS will detect a video scene change.

7. The IMS module at the first dismantlement bay or cell is used to detect the arrival of the container by: (1) NTVision recording a video scene change in the video signal from the IMS module and (2) the IR receiver detecting the IR tag and reporting its ID (serial) number.

8. The Cart-Cam and IMS video camera are used to monitor the removal of the ITID. The seal is cut off, but the IR tag can be re-used. The inspectors may request the used ITID components.

9. Live or Local Verify procedures may be called for by the inspectors at any time during steps 4-8 (up to the maximum number of times permitted by treaty).

10. The container enters the dismantlement bay or cell with the doors closing behind it. No video transmissions occur during the dismantlement process.

11. Within the allocated time, the entryway of the dismantlement bay or cell is opened. One or more containers emerge. The host facility specifies which contain declared, treaty-limited items, and which contain other components. Inspectors may request a challenge inspection (from their quota of allowed challenge inspections) to check the radiation signatures of the latter.

12. The IMS module and the Cart-Cam observe the installation of an ITID on the container(s) declared to container treaty-limited items. (IFMS can simultaneously monitor the movement of multiple containers.)

13. The containers, with their ITIDs, are moved to the next dismantlement bay or cell for the next operation. Again, they must arrive within the allotted time, or the IFMS expert system sounds an alarm at the CMS.

14. Steps 8-13 are repeated as necessary to complete the dismantlement process for one warhead. This may involve multiple stops at various dismantlement bays/cells.

15. Eventually, IFMS hands off responsibility for the nuclear weapon contain-

ers to the temporary or long-term storage monitoring system, such as MTS.
16. When sufficient warheads have been dismantled for the current phase of the dismantlement process, the inspectors are escorted back into the facility for a final sweep of the dismantlement bays and cells, similar to the initial sweep in step 2.

17. The IFMS system can now be turned off until the next time that START III dismantlement operations are scheduled. In the meantime, the dismantlement bays and cells can be used for non-treaty, domestic stockpile stewardship activities.

APPENDIX C - Abridged Sequence of Steps for Using the Magazine Transparency System (MTS)

1. Under escort, the inspectors perform an initial sweep of the storage magazine, checking for undeclared entryways ("trap doors") and undeclared nuclear materials.

2. As part of the "choose or keep" protocol, inspectors randomly pick which of the host-provided MTS modules, components, and notebook computers will be used, and which they can keep for analysis.

3. Host facility personnel install the chosen MTS modules, components, and notebook computer in the magazine while the inspectors observe.

4. While host facility personnel observe, the inspectors insert the removable media containing their one-time keypad into the MTS notebook computer.

5. Weapons containers are moved into the magazine, ideally (from the standpoint of transparency) while the inspectors are present.

6. Both before and after the magazine is closed, inspectors can perform live verify tests, such as by moving permanent magnets around outside the magazine.

7. When the magazine is reopened, either because that is scheduled, or because MTS has indicated a significant number of unauthorized events has taken place, the inspectors are granted immediate ownership of the notebook computer. They can then review the events stored in the computer, perhaps

jointly with host facility personnel. The inspectors are allowed to keep the computer for later analysis. If they choose not to, the original MTS system can be put back into immediate operation, or else a replacement MTS can be installed.

REFERENCES AND NOTES

1. The White House Office of the Press Secretary, *Joint Statement on Parameters on Future Reductions in Nuclear Forces*, March 21, 1997.

2. S. Fetter, "A Comprehensive Transparency Regime for Warheads and Fissile Materials," *Arms Control Today* 29 (January/February 1999): 1, ; G. Kiernan, M. Percival, L. Bratcher, "Transparency in Nuclear Warhead Dismantlement - Limited Chain of Custody and Warhead Signatures," (paper presented at the 37th Annual Institute of Nuclear Materials Conference, Naples, Fla., July 28 – August 1, 1996); Department of Energy, Office of Arms Control and Nonproliferation, "Transparency and Verification Options: An Initial Analysis of Approaches for Monitoring Warhead Dismantlement," May 19, 1997.

3. O. Bukharin and K. Luongo, "U.S.-Russian Warhead Dismantlement Transparency: The Status, Problems, and Proposals," *Princeton University's Center for Energy and Environmental Studies (CEES), PU/CEES Report No. 3*, (April 1999); A. Dyakov, "Nuclear Arms Reduction and Transparency Problems," *Yaderny Kontrol Digest* 12 (1999): 7; C. Olinger et al., "Technical Challenges for Dismantlement Verification" (paper presented at the 38th Annual Institute of Nuclear Materials Conference, Phoenix, Az., July 20-24, 1997); J. Morgan, "Transparency and Verification Options" (paper presented at the 37th Annual Institute of Nuclear Materials Conference, Naples, Fla., July 28- August 1, 1996).

4. In 1995, the U.S. government proposed to Russia a draft agreement that would allow the exchange of classified information relating to nuclear weapon stockpiles. Russia rejected that proposal, and no new attempt has been made by the United States to reach such an agreement. In any event, Congressional approval would almost certainly be required, making any exchange of classified information highly unlikely within the next few years. See H. Feiveson, ed., *The Nuclear Turning Point* (Washington, D.C.: The Brookings Institution, 1999, 186.)

5. For additional information, see "Tracking Warheads From Dismantlement to Storage," *Dateline: Los Alamos*, Los Alamos National Laboratory (March 2000), 9-11; and J. E. Doyle and R.G. Johnston, "Report To The Joint DoD/DOE Integrated Technology Implementation Plan Steering Committee On The Integrated Facility Monitoring System (IFMS) And Magazine Transparency System (MTS)," *Los Alamos National Laboratory report LAUR-00-1671* (March, 2000).

6. For example, placing both domestic security & safeguards seals and START III seals on a weapons container can be a problem. Existing weapons containers are often not designed to incorporate extra seals.

7. A realistic START III regime needs flexibility to deal with unanticipated problems in a time-effective manner. Inspectors should be allowed by treaty to occasionally veto the dismantlement of a specific nuclear weapon (without suspending overall treaty operations) if they do not like how things are proceeding, or if there is a loss of signal from monitoring equipment. Similarly, host facility personnel must be allowed to occasionally pull a weapon out of the dismantlement process if they are having trouble with

it. In either case, the weapon could presumably go back into the dismantlement queue at step 1 if both parties agree. If they don't agree, the host nation would simply lose the right to get credit for ultimately dismantling that specific weapon. Such flexibility might, of course, not be appropriate for dismantlement treaties in the distant future (START VII, for example), when the size of existing nuclear arsenals may already be greatly reduced, and uncertainties about even a few nuclear weapons could be critical.

8. D.W. MacArthur and R. Whiteson, Mayak/PPIA Demonstration Attribute Measurement System with Information Barrier: Functional Requirements, Los Alamos National Laboratory report LA-UR-99-5634.

9. To reduce treaty costs, there may be negotiated limits on the frequency with which the random "choose or keep" or "keep the used parts" protocols may be invoked, especially for the most expensive components and sub-systems. Inspectors may also not wish to automatically exercise all their rights to invoking such protocols.

10. Challenge inspections would typically take place on containers that have been declared by the host country as containing non-treaty limited items. These challenge inspections provide an incentive for the facility not to cheat. If the inspectors are allowed to use sophisticated radiation sensors to probe these containers, they have the possibility of gathering important classified information should the containers actually be full of treaty-limited, nuclear materials.

11. Presumably under the treaty, identical hardware and software for the Central Monitoring Station (CMS) could be offered to each side. The foreign inspectors, however, would be free to use their own hardware and software, and to analyze and record data sent to the CMS in any manner of their own choosing.

12. The seal we used most frequently on the weapons containers during the demonstration at Pantex was the Guardian seal manufactured by RELCOR (North Palm Beach, FL). This commercial seal has a number of advantages for treaty monitoring applications including simplicity, ease of use, durability, robustness, safety, relatively low cost, optical transparency, good visibility for video monitoring, a large (embedded) barcode and serial number (easily seen on video), and the fact that the seal it is not currently used for nuclear applications. The infrared (IR) tag employed for most of the demonstrations was a VER-1700 IR "locator badge" manufactured by Versus Technology (Traverse City, MI). The 447.5 kHz digital IR signal it emits is at 875 nm and includes a programmable 16-bit unique ID (serial number) for each tag. In order to increase battery life, the badge includes a motion sensor that decreases the IR (digital) signal rate when the tag is at rest. The two (Model VER-4420) IR receivers inside the IMS module that read the tag's IR signal were also manufactured by Versus Technology. Maximum detection distances were typically 4 to 7 meters.

13. The commercial components used to demonstrate MTS at Pantex included a Model 1552 hand-held barcode reader and Model 9745 wireless barcode pickup unit manufactured by Intermec (Everett, WA), an Intermec Model 2100/915NV2 RF tag reader system, and a Model FGM-5DTAA triaxial fluxgate magnetometer manufactured by Walker Scientific (Worcester, MA). The magnetometer occupies a volume less than 0.6 liter. The MTS notebook computer inside the magazine can analyze signals from multiple video cameras and magnetometers, though only one of each was used for the Pantex demonstrations.

14. Permanent magnets can also be placed on the magazine access door(s) so that any movement of the door is detected in a non-contact manner by the magnetometers. There are additional intriguing extensions of the MAGTAG blanket concept, some

potentially quite difficult to defeat, as discussed in a 1999 U.S. patent application by R.G. Johnston and A.R.E. Garcia entitled, "Magnetic Vector Field Tag and Seal."

15. With a 1 nT resolution, one magnetometer can detect changes in the DC field out to a distance of about 20 meters, depending on the number and strength of the magnets used in each MAGTAG blanket. Rotations of 0.1°, or translations of a few mm, for a single magnet can be readily detected.

16. J. Luger, Code Making and Code Breaking, Breakout Productions, 1990.

17. The one-time keypad, used in conjunction with live verify and local verify protocols, reduces or eliminates the need for information barriers, standard encryption or data authentication schemes, equipment state-of-health checks, seals or tamper-indicating enclosures for the system sensors, and high-bandwidth streams of sensor data being sent considerable distances to a central analysis station. All of these tend to be complex and expensive to implement/maintain, difficult to negotiate, and highly vulnerable to spoofing.

18. It may not be necessary to send an "All OK" signal as often as every second if it takes longer than 1 second to attack the MTS. Nevertheless, at 1 byte per second, an Iomega Zip or Jazz drive can, for example, hold over 3 years and 30 years worth of data for the one-time keypad, respectively, even without data compression. With compression, a floppy disk can hold nearly 3 weeks worth.

19. The data transmission rate for the MTS is so low, in fact, that the "All OK" signal can be transmitted over considerable distances using just flashing lights, low-power laser beams, or mechanical signs. This could be useful in some of Russia's more rural, isolated, and heavily forested nuclear facilities. The low-bandwidth also may make the MTS system attractive for monitoring nuclear components and materials while in transit, such as on board a truck or railcar. It eliminates the need for a high-bandwidth signal that can draw undue attention to the moving vehicle--something not desirable for security reasons when transporting nuclear items.

20. The treaty would need to limit the number of times that unannounced live verify and local verify tests (as well as challenge inspections) could be invoked by the foreign inspectors.

21. We speculate that the health of the international cooperation taking place under the treaty could be gauged by the frequency with which obscene gestures are requested by the inspectors for live verify tests.

22. Even if a frame-by-frame or pixel-by-pixel analysis of the recorded video signals was not performed routinely, each side would be fully aware that it remained an option for the other side.

23. The two cameras in the IMS module located outside each START III disassembly bay or cell are turned on when the inspectors first sweep the bay or cell during an in-person inspection. The IFMS video feed thus includes images of the inspectors entering the bay or cell. Continuous video transmission from the IMS module continues from that point on until the inspectors reenter the bay or cell for the final sweep, which is also captured on video. The IMS cameras are then turned off until the next time that the bay or cell is needed for START III dismantlement operations, when the inspectors will need to perform a new initiation sweep. (The bay or cell is available for stockpile stewardship functions when it is not in service for START III dismantlement.) When examining recorded IFMS video for signs of tampering, inspectors can reference against the video images showing themselves entering the bay for the initial

and the final sweeps.

24. In the case of, for example, verifying the response of the infrared tag receivers in the IMS module, it may be useful to have a sealed lock-box containing IR tags provided by the inspectors. To prevent espionage, these would be carried into the nuclear facility inside a sealed, acoustically-isolated Faraday box that has significant radiation shielding. (The host facility provides the seal for the box.) The box would be stored in the field of view of one of the IMS modules. While being watched on video, facility personnel, under the direction of the inspectors, would unseal the box and choose one of the tags specified by the inspectors. This tag would be held up to the IR receiver so that the inspectors can see if it records the correct serial number--a number not previously known to the host facility. The host facility then gets to keep all the tags for latter analysis (to check for espionage), while the used lock-box seal is returned to the inspectors.

25. The IFMS as demonstrated at Pantex did not include radiation sensors, though the version demonstrated at the DAF at the Nevada Test Site included Geiger-Mueller counters, which were incorporated into the IMS module.

26. The same thing can be accomplished (actually with better time resolution) by using a hard-wired, fast risetime LED controlled by the inspectors and placed in front of the IMS camera(s). When the inspectors fire the LED at random times, they can look for the delay in when the LED light shows up in certain pixels in the IMS video image. The symmetry, however, of the IMS camera watching the inspectors' video program, while the inspectors watch the IMS video feed containing the slightly delayed replay of their own video program is irresistible. Note that the inspectors' video feed can be sent into the nuclear facility via wireless transmission, thus avoiding the need for hardwiring. Even local broadcast TV programs can be used.

27. For the video live verify test, the Central Monitoring Station must be local. If it located many miles (or half way around the world) from the host nuclear facility, the electronic signal lag will be too large to guarantee locality of the IFMS video feed.

28. An even better method is to take a chisel and knock a small piece out of the concrete wall while the video cameras watch. If the cameras have sufficient resolution, replicating this 3-dimensional impression quickly, at an unpredictable spot, is non-trivial. This approach has the additional ironic advantage that, as we dismantle nuclear weapons, we also slowly dismantle the nuclear facility.

29. R.G. Johnston, "Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste Management," *Science & Global Security* (forthcoming).

30. R.G. Johnston and A.R.E. Garcia, "Vulnerability Assessment of Security Seals," *Journal of Security Administration* 20 (1997): 15-23, available at http://lib-www.lanl.gov/la-pubs/00418796.pdf; R.G. Johnston, "The Real Deal on Seals," *Security Management* 43 (1997): 93-100, available at http://lib-www.lanl.gov/la-pubs/00418795.pdf; C.A. Sastre, "The Use of Seals as a Safeguards Tool," *Report BNL 13480*, (Upton, New York; Brookhaven National Laboratory, 1969); J.L. Jones, "Improving Tag/Seal Technologies: The Vulnerability Assessment Component," *Report 95/00599*, (Idaho Falls, Idaho; Idaho National Engineering Laboratory, 1996.)