Viewpoint

Tamper Detection for Safeguards and Treaty Monitoring: Fantasies, Realities, and Potentials

ROGER G. JOHNSTON[1]

Dr. Roger G. Johnston, CPP is a Science Fellow at the Center for International Security and Cooperation (CISAC), Stanford University, for 2000-2001. He also heads the Vulnerability Assessment Team in the Applied Monitoring and Transparency Laboratory at Los Alamos National Laboratory (LANL).

Tamper detection[2] has an important role to play in domestic nuclear security and safeguards,[3] as well as in international verification and treaty monitoring.[4] Unfortunately, ideas about tamper detection often seem to be based on misconceptions, fuzzy goals, and wishful thinking.[5] Current tamper detection programs are hampered by these problems, as well as by poor training, limited analysis, vague (or nonexistent) standards, "see-no-evil" mentality, "one-size-fits-all" thinking, and unmitigated vulnerabilities. Better approaches, more sophistication, improved hardware, and greater understanding are sorely needed for both current and future applications.

In this essay, I review tamper detection devices, particularly tags and seals, and then discuss the erroneous beliefs held by many nuclear security practitioners about the effectiveness of these devices. Next, I explore the general problems that plague the use of seals and other tamper devices in the United States and worldwide, and then look at specific problems in U.S. and Russian material protection, control, and accounting programs (MPC&A) and in the International Atomic Energy Agency's (IAEA's) tags and seal program. I conclude with a survey of new tamper detection applications and recommendations for improving tamper detection both for domestic security and international transparency and treaty monitoring. Throughout, I argue for a more realistic assessment of the possibilities and vulnerabilities of tamper detection devices.

TAMPER DETECTION MEASURES

Tamper detection often involves the use of tags and/or seals. Tags are applied or intrinsic features or devices used to identify an object or container. Familiar examples of tags from everyday life include car license plates and the holographic design found on many credit cards. Seals are tamper-indicating devices (TIDs) meant to detect unauthorized access to a door, container, or package.[6] Familiar examples of seals include the tamper-indicating packaging required on all U.S. over-the-counter pharmaceuticals, and the inexpensive plastic or wire seals often installed on home or commercial utility meters in the United States to detect pilferage.

Thousands of different seals are currently available, including both passive and active devices. Passive seals include irreversible mechanical assemblies, frangible foils or films, epoxies, adhesive labels, wires or cables, optical fibers, and other devices and materials that become damaged or show changes when cut or manipulated. There are currently two types of active seals: electronic and fiber optic. Electronic seals continuously monitor for some kind of change indicative of tampering. Active fiber optic seals periodically or randomly send light pulses down a fiber optic bundle (or single fiber) to check continuity.

It is important to realize that seals—unlike locks—are not intended to resist unauthorized access or entry. Instead, they are meant to indelibly record that such access took place.[7] Indeed, some seals are made of paper or plastic and can be easily torn by hand; however, this does not inherently make them ineffective for tamper detection. Another issue that sometimes causes confusion is the partial interchangeability of tags and seals. A secure seal must have tag-like attributes, and vice versa.[8] As a consequence, a device that is primarily being used as a seal may have secondary uses as a tag, while a tag may also be useful for detecting tampering.

One of the critical issues in tamper detection and verification is whether a given tag or seal can be "defeated," and if so, how easily.[9] "Defeating" a seal means to spoof it. Though there are other kinds of attacks,[10] defeating a seal typically involves opening it, then resealing *without being detected*, using either the original seal or a counterfeit. If the original seal is used, the seal might be opened without damage or evidence of opening, or else the damage and/or evidence must be erased or hidden. In a similar manner, defeating a tag means counterfeiting the tag without being detected, or else lifting the tag and reapplying it to another object or container without being detected. To "attack" a tag or seal means to undertake a sequence of actions intended to defeat it.

Any given tag or seal is potentially susceptible to hundreds of different kinds of attacks.[11] In the case of seals, the wide variety of possible attacks can be grouped into the following categories:

- tampering with the seal or seal design prior to use, in order to install a backdoor;
- opening and then closing the seal without damaging it or creating evidence of entry;
- hiding or repairing any damage to the seal as a result of opening it;
- hiding or erasing any evidence of entry as a result of opening the seal;
- replacing the seal with a duplicate or counterfeit (or replacing certain parts);
- tampering with the seal data;
- tampering with the seal installation, inspection, or interpretation process;
- bypassing the seal and attacking the container or hasp instead;
- false alarming and discrediting;
- social engineering,[12] bribery, or intimidation; and
- hybrid or alternative methods.

In addition to tags and seals, tamper detection for nuclear security or verification purposes may also involve the use of intrusion detectors, portal monitors, information barriers, and video surveillance.[13] Intrusion detectors (essentially "burglar alarms") are often used in conjunction with seals; they differ in that they report unauthorized entry in real-time, rather than later at the time of inspection. Such detectors offer the advantage that security forces can respond quickly to intruders. Typical disadvantages as compared to seals include significant occurrences of false alarms, high cost, the need for electrical power, and the additional vulnerabilities associated with sending an alarm signal to a distant location for interpretation. Portal monitors (such as radiation sensors or metal detectors) observe the comings and goings through entryways, doors, and hallways to control access and to assist with containment. Information barriers are hardware or software designed to block or filter the release of specific information. They are envisioned as a way to prevent radiation detectors from revealing classified information while still providing useful results to nuclear inspectors.[14] Video cameras are frequently proposed or used to reduce the intrusiveness or manpower requirements for security, safeguards, and verification applications. While intrusion detectors, portal monitors, information barriers, and video cameras can sometimes be used in place of tags or seals, they must still be protected from tampering themselves. This can be addressed through the use of additional tags and seals.

TAG AND SEAL FANTASIES

Many analysts have expressed realistic views about the limitations and fallibility of verification, tamper detection, and tags and seals.[15] There are also persuasive calls for better worldwide practices and standards for the safeguarding of nuclear materials.[16] Nevertheless, among many nuclear security practitioners, as well as disarmament/nonproliferation theorists, there continues to be an erroneous belief that totally "tamper-proof" tags, seals, and other monitoring technologies exist,[17] or will exist in the near future. This is a fantasy.

The term "tamper-proof" is particularly unrealistic and even nonsensical. Most tags and seals will break if they are struck hard enough with a hammer. This is a particularly vehement kind of tampering. By "tamper-proof," however, most people probably mean that the tag or seal cannot be defeated.[18] Even in this context, however, the term "tamper-proof" is problematic because it is usually not possible to prove a negative. How can one prove that a tag or seal cannot be defeated for every possible adversary, attack strategy, and attack technology, present and future? Any given vulnerability assessment may fail to find vulnerabilities—though this should be viewed as an inherently suspicious result.[19] It may mean merely that the study lacked adequate funding, time, technology, personnel, expertise, motivation, or cleverness to find some of the inevitable vulnerabilities. It is also often the case that the assessors do not really want to find vulnerabilities. The assessors are sometimes the tag/seal developer or promoter, or may be under subtle or not so subtle pressure to "certify" that the tag or seal is ready for field use after large sums of money have been spent on its development and/or procurement. The embarrassing discovery of vulnerabilities can cause unwelcome consternation.

The use of the term "tamper-proof" is sometimes excused by saying that it is not meant literally. In my experience, however, people using this term usually *do* mean it literally. Those who do not, however, should avoid such sloppy terminology. When issues of nuclear warfare, terrorism, and national security are involved, and when disarmament and nonproliferation regimes require international diplomacy and multi-lingual translations, it is essential to use precise terminology. Words are powerful. The phrase "tamper-proof seal" has become so ubiquitous, that people come to believe it literally. Indeed, I have been told more than once by security personnel, including those involved in domestic nuclear security and safeguards applications that, "our seals are tamper-proof," apparently based primarily on the fact that they are called "tamper-proof seals."

The issue of vulnerability is important because theorists planning START III or other disarmament, nonproliferation, or safeguards regimes often rely heavily on the use of undefeatable tags, seals, video cameras, and other monitoring hardware.[20] (These invulnerable devices may or may not be called "tamper-proof" by the theorists themselves.) In some cases, invulnerable tags, seals, or other monitoring hardware is envisioned as the sole or most critical means for verification of treaty compliance,[21] with absolute verification often being thought essential for the success of the regime.[22]

The imaginary, "tamper-proof" tags and seals that are invoked by theorists are often not identified. When they are, they are usually described as electronic or fiber optic seals,[23] or tags based on intrinsic microscopic surface roughness or other complex surface features.[24] Often they will report their status remotely,[25] or else will be inspected every few months or years as part of a periodic on-site inspection.[26] In either case, the inspectors will have total faith that these tags and seals will detect diversion or undeclared activities because they are "tamper-proof." The fact that the tags and seals will be out of the hands of the inspectors for extended periods of time and under the control of the nation being monitored (with all its massive resources), is thus not considered a problem.

Some of these hypothetical tags and seals appear to have an amazing power beyond being merely "tamper-proof" themselves. They apparently can impart "tamper-proofness" on the objects or containers to which they are attached. Thus, if a "tamper-proof" tag is attached to a missile, for example, we apparently do not need to worry about attempts to cut into the missile at a location well away from the tag in order to remove the contents. The tamper-proof "aura" of the tag somehow prevents this. Similarly, "tamper-proof" seals seem to somehow impart "tamper-proofness" on entire containers and on the container hasp to which the seal is attached.

To their credit, some theorists at least try to devise a mechanism for this volumetric protection. For example, it is suggested that multiple fiber optical cables could be used to form a net around the object to be protected.[27] It is not clear, however, what keeps the nodes of this net intact and safe from movement and physical tampering.

The unfortunate reality is that there is no convincing evidence that "tamper-proof" tags and seals exist and a number of reasons to believe they are not possible.[28] There is, furthermore, little theoretical understanding of tamper detection,[29] no useful tag/seal vulnerability testing standards,[30] and (as discussed above) no way even to prove a given tag or seal is tamper-proof. Indeed, ALL seals that have been subject to a *comprehensive* and *effective* vulnerability assessment[31] by personnel intent on finding problems (rather than striving to "certify" the seal) have shown significant vulnerabilities, though details of the application and the exact use protocols[32] appear to be highly relevant. Moreover, there has been remarkably little research and development (R&D) by government or the private sector in the past six-plus years devoted to developing new, high-security tags and seals, especially for transparency and treaty monitoring applications. This, despite the fact that dramatically better tags and seals seem possible,[33] are clearly needed, and that additional R&D on verification technologies has been repeatedly called for over the years.[34]

The common assumption that the best seals will always be high-tech is also dubious. Los Alamos National Laboratory found, after studying 135 seals in detail, that high-tech seals are often easier to defeat than low-tech seals.[35] There are a number of possible reasons for this, including the fact that low-tech, hands-on verification methods often work best and are easier to negotiate.[36] Even if high-tech seals were to provide superior tamper detection, they might still not be appropriate for certain applications (such as use in Russia) because of the problems associated with upkeep and sustainability,[37] their susceptibility to unpredictable failure and radiation damage, and concerns (by the nation being inspected) about safety and espionage during treaty monitoring.

A related, equally common assumption is that tampering can be better detected if the seals (even if low-tech) are read with high-tech readers. "Readers" are electronic or optical devices (often hand-held) used in the field to inspect a seal to determine if tampering has occurred. The reality is that high-tech readers, at least the way they are typically used, often decrease security. Even though high-tech readers are usually introduced in order to save time and money, seals read by high-tech readers typically require more effort—not less—than manually inspected seals to achieve reliable tamper detection.[38]

Another fantasy some disarmament theorists float about is the idea of using high-tech black boxes for treaty monitoring.[39] "Black boxes" are on-site monitoring devices owned by the inspectors that are not fully described to the inspected (host) nation in terms of function, mechanisms, encryption, and/or detailed technical specifications.[40] Given, however, the current meticulous, mandatory requirements for obtaining nuclear explosive safety (NES) and security approval for any kind of equipment brought into MPC&A control areas inside U.S. nuclear facilities,[41] as well as the inevitable concerns by any inspected nation about loss of secret information,[42] it seems highly unlikely that mystery hardware, encryption, or "traps" (covert seals) will be allowed inside sensitive nuclear facilities, or anywhere near nuclear warheads.

GENERAL PROBLEMS[43]

The way seals are currently used in the United States and worldwide for nuclear (or other) applications is far from ideal. Seals are frequently chosen for a given application without careful analysis, and sometimes based on hearsay. Seal vulnerabilities are rarely understood and effective countermeasures are usually lacking. The training of seal inspectors typically emphasizes rigid formality rather than the flexibility and observational skills required to provide effective real-world security. Seal inspectors are usually given little useful information on how to detect tampering, no information about the vulnerabilities and most likely attack scenarios for the seals they are using, and zero practice at detecting seals that are attacked either crudely or subtly. Effective, independent, periodic vulnerability assessments of tamper detection programs or devices are rare; vigorous outside input and review are even rarer. When vulnerability assessments are undertaken, the findings and recommendations are often ignored.

Even more counterproductive—at least from the viewpoint of a vulnerability assessor—are attempts to suppress vulnerability findings, or even the assessors themselves.[44] It is not unusual, in my experience, to demonstrate a seal vulnerability to security personnel, and then have them request (or demand) that, "this not be discussed with my superiors." This is not the sign of a healthy security program! Vulnerabilities are always present. The discovery of them should ideally be viewed as good news since it allows the possibility of improving security.

Many current seal users appear to believe (incorrectly) that the seals they are using are "tamper-proof," or nearly so. In my experience, they usually quickly change their minds when one or more attacks are demonstrated on the seals they are using. They then often contemplate doing away with seals entirely. This may be an example of what Kevin J. Soo Hoo calls (in the context of computer security) a "binary" view of security: "...systems are [believed to be] either secure, in which case they have no vulnerabilities, or are insecure...".[45] The more realistic and useful view is that security is a continuum. Seals (like everything else in the world) are imperfect compromises and will always have vulnerabilities. Some of these vulnerabilities may be very serious, others can be mitigated or eliminated with countermeasures, and others will never even be known by the user.

Unfortunately, nuclear tamper detection programs sometimes insist—for political, self-image, or public relations reasons—that vulnerabilities do not exist, have never existed, and never will exist. Such a position is irresponsible. One also often hears assurances from seal users that seal tampering has never occurred. This conclusion is highly problematic. Without an independent method of verifying that there has been no tampering or diversion, e.g., by establishing a material balance, seal inspections alone cannot support such a conclusion.[46] By definition, defeated seals are never detected.

It is not uncommon for security managers to have little interest in the vulnerabilities of the seals they are using. The reason typically given (other than that the seals are "tamper-proof") is that there are multiple layers of other physical security to "backup" the seals should they be defeated.[47] There are five serious problems with this rationale. Firstly, seals should not be considered part of the physical protection system (the "P" in "MPC&A") for nuclear materials as they often are;[48] seals are more properly part of the control and accounting function ("C&A").[49] Secondly, the idea that the alarms and security failures at one level of security will be automatically compensated for by other layers is surely a recipe for lax security.[50] Each layer must be taken seriously in its own right and optimized to the extent practical.[51] Thirdly, seals (and tags) will often be the security feature found physically closest to the nuclear material or warhead being monitored. As such, they are certainly deserving of serious consideration. Fourthly, dismissing seal vulnerabilities as not worth correcting might be valid if the countermeasures required substantial cost or difficulty. In many cases, however, effective countermeasures for seal vulnerabilities can be implemented relatively cheaply and easily.[52]

A fifth reason that it is dangerous to assume that seal failures will be caught by other levels of security is that potential adversaries do not necessarily have to defeat all the outer security layers. An insider such as a security guard who attempts to divert nuclear materials or to sabotage operations will already be authorized to pass through many or all of these outer layers of physical security. External inspectors will typically be escorted past at least some of the layers of security in order to accomplish their assigned tasks. In the case of transparency and treaty monitoring, furthermore, the nation being monitored *owns* the facility and most or all of its layers of security. Thus, at least some of these security layers do not provide "backup" to the tamper-indicating seals because the people who control these layers are the potential adversaries being monitored by the seals!

One of the continuing problems in applying tamper detection to transparency and treaty monitoring is confusion about how they differ from domestic security and safeguards.[53] It is often assumed that existing domestic security and safeguards measures (including seals) can simply be borrowed with little modification for use in transparency and treaty monitoring.[54] In reality, domestic "safeguards" differ dramatically from international (IAEA-like) "safeguards" in terms of goals, personnel, economics, environment, adversaries, secrecy, confidence in the preceding and subsequent processing steps, optimum hardware, who owns/operates/installs the hardware, and consequences of a safeguards failure. These differences are often ignored. We are assured, for example, that perimeter monitoring for international nuclear production monitoring will be "easier than it first appears because sensitive production facilities presumably already have a perimeter security system."[55] This overlooks the fact that the existing perimeter security system has a completely different purpose, different potential adversaries, and is owned, operated, and controlled by the nation being monitoring for treaty compliance. Similarly, discussions about how START III might be implemented at the U.S. Pantex warhead storage and dismantlement facility in Texas are often prefaced on the idea that international inspectors can simply use the existing Pantex seals and seals database for treaty monitoring functions. This makes no sense because the domestic seals are intended to deal with one type of adversary—an individual or small group working at cross purposes to the facility—while seals for transparency and treaty compliance monitoring are intended to detect tampering by the very nation that owns the facility.[56] The monitored nation that is the adversary for international "safeguards" will have six to nine orders of magnitude more resources than the rogue individual or relatively small group of concern to domestic nuclear "safeguards."

Seals for transparency and treaty monitoring applications require significantly different attributes than seals used for U.S. domestic security and safeguards.[57] Existing domestic seals, for example, are not designed to give observers (or video cameras) a good view of seal installation, inspection, and removal. Yet such "transparency" may be essential for bilateral or trilateral monitoring of nuclear warhead dismantlement. The reason is that foreign inspectors are unlikely to be permitted to handle nuclear warhead containers or to directly install seals on them due to nuclear explosive safety (NES) and security concerns. Instead, host facility personnel will probably install and remove seals under the watchful eye of inspectors. Even if foreign inspectors are eventually allowed to personally install seals on warhead containers, however, current seal designs and use protocols for domestic security and safeguards are based on the idea that the seal installer has no hidden agenda. This is not a given for treaty monitoring.

Another problem with current tamper detection practice is that, although it is well over 7,000 years old,[58] the field remains poorly understood. There is no underlying theory, and surprisingly little published (classified or unclassified) about tags and seals. Only a handful of security or physical security textbooks devote more than a paragraph to seals, and fewer still mention tags. There is no general text on the subject of tamper detection. The few standards that exist for seals are neither comprehensive nor substantive regarding seal choice, performance, or how vulnerabilities should be tested.[59] There is considerable discussion about "international norms or standards" for the general physical protection of nuclear materials, as well as great interest in the U.S. "Stored Weapons Standard" and the IAEA (INFCIRC/225, Revision 4) recommendations for protecting nuclear materials.[60] None of these, however, have much to say about tags, seals, and tamper detection.

SPECIFIC PROBLEMS[61]

As has been well documented and discussed,[62] Russian nuclear MPC&A, including technical assistance provided by the United States, has a number of serious problems. Russia tends to use antiquated seals, seals that can be trivially defeated, or no seals at all.[63] The Russians often seem relatively uninterested in dealing with insider threats.[64] There is no comprehensive MPC&A testing program and no push from the U.S. Department of Energy (DOE) to install one, though this is essential for effective operation.[65] Overall DOE management of MPC&A assistance programs to Russia has been far from ideal,[66] and the U.S. Department of Defense (DOD) threat reduction programs are also beset with difficulties.[67] In the case of the Mayak Fissile Material Storage Facility,[68] for example, DOD is unclear about what the United States is supposed to be "verifying," i.e., the effectiveness of the Russian domestic MPC&A program or Russian compliance with bilateral/trilateral agreements, or both.[69] Both DOE and DOD are deeply confused about the differences between domestic security and safeguards versus transparency and treaty monitoring, and about what security or monitoring hardware is appropriate for use in Russia and who should own and operate it.

In contrast to Russia, the U.S. domestic nuclear MPC&A program is generally recognized as being the most rigorous and effective in the world.[70] There have been, however, continuing problems and criticisms, and there is clearly significant room for improvement.[71] When it comes to tamper detection, the DOE complex generally lacks sophisticated seal knowledge or implementation. Many DOE managers believe that DOE uses "tamper-proof" seals.[72] The main DOE handbook for safeguards seals programs is remarkably devoid of useful information about seals, and shows no interest in training that would let seal inspectors understand seal vulnerabilities and likely attack scenarios.[73] DOE, furthermore, maintains that seals can help to reduce personnel radiation exposures.[74] In reality, the way some passive seals are used does the exact opposite. DOE seal installation, inspection, and removal often require such time-consuming manual procedures that personnel receive exposures that would be unnecessary if seals were not used. DOE's frequent double-checking of seals, and ordering of replacement seals when security procedures are second-guessed, also adds extra personnel radiation exposure.

There are seals in use for U.S. domestic nuclear security and safeguards that have never undergone any kind of vulnerability assessment, seals that have undergone only cursory vulnerability assessments or "certification" testing (sometimes by the developer or promoter of the seal), and seals that have undergone vulnerability assessments producing significant findings that are ignored or unknown to the seal users. Few seal users or security managers within the U.S. nuclear complex appear to have even a rudimentary understanding of the vulnerabilities associated with the seals and use protocols that they employ.

A particularly unfortunate practice in recent years has been the premature transfer to the international community of MPC&A methods and hardware used for U.S. domestic security and safeguards.[75] Technology transfer may well be warranted after hardware characteristics and vulnerabilities are well understood, or when the hardware clearly offers only modest security, or is not implemented in U.S. nuclear facilities. It does not seem prudent, however, to hand over critical domestic MPC&A systems when the United States has only a rudimentary understanding of the issues associated with their use. Not only does this potentially compromise U.S. national security, but also it severely confuses the differences between security and safeguards applications versus those of transparency and treaty monitoring. No one security system or device can be optimized for both kinds of applications.

Turning to the IAEA, it is clear that the agency must deal with a variety of difficult challenges and constraints[76] including the "zero-budget growth" policy, funding holdups, limited resources, morale problems, cultural and language differences, harsh and sometimes adversarial field conditions, the need to work closely with bureaucratic governments and diverse member states having conflicting agendas and widely differing attitudes about security, and unrealistic expectations from some critics. Despite all these challenges, the IAEA operates a safeguards program with a truly commendable degree of professionalism, quality, and efficiency. The IAEA has a sophisticated tags and seals program, and considerable understanding of practical tamper detection issues. It conducts first-class postmortem exams[77] on seals returned from the field. The IAEA also has a highly educated, well-motivated group of inspectors unequaled in the world in terms of qualifications and dedication.

The IAEA, however, appears to have a number of deficiencies and problems, at least in regards to tamper detection. The agency takes a somewhat binary view of its safeguards[78] (as discussed above), and largely maintains—without convincing arguments—that its seals are tamper-proof.[79] The IAEA has also been accused of lacking sufficient transparency in its safeguards programs,[80] and failing to undergo or accept sufficient outside, independent review and feedback that may not always be positive.[81] There are concerns about the agency's willingness to aggressively report evidence of tampering, diversion, or cheating; concerns about its lack of intelligence capabilities; and concerns about public misconceptions of what the agency does.[82]

The IAEA is generally conscientious about arranging for vulnerability assessments on many of the seals it uses. It often begins thorough vulnerability assessments, however, only after having (at least informally) committed to using a given seal design. The agency has no substantial in-house tags/seals R&D program, and no internal program for conducting vulnerability assessments or optimizing seal use. The IAEA relies instead upon uneven technical assistance provided in an ad-hoc, political, and inefficient manner by various member states, with limited and unreliable funding. It is not clear that the vulnerability assessment findings that are generated are fully incorporated into IAEA seal use protocols, inspector training, or postmortem exams, or that the seals that are chosen in the first place are optimum for the application of interest. Though highly trained and motivated, IAEA seal inspectors are typically unfamiliar with the vulnerabilities of the seals they are using or with the most likely attack scenarios.[83] This greatly decreases the odds that they can detect tampering. There are also concerns that IAEA inspectors lack a holistic, proactive, and critically observant approach, and that they are not permitted the necessary flexibility or individual initiative.[84]

The IAEA conducts blind (not double blind) tests on its seals program to check if defeated seals will be detected.[85] These tests, however, appear to be more focused on quality control than evaluating the probability of detecting real-world tampering. The test seals introduced into the postmortem analysis primarily involve substitution or blatant tampering, instead of seals that have been attacked with more subtle and realistic methods.

Another problem that should be of enormous concern for any safeguards or on-site inspection program is the reliability of security personnel and inspectors. IAEA INFCIRC/225 recommendations on background checks are vague, and IAEA inspectors themselves appear to undergo no significant background screening either before or after being hired. The reliability of tag and seal inspectors is a critical issue for effective tamper detection and can be the source of serious vulnerabilities.[86] Apart from their role in tamper detection, giving inspectors who have not undergone a thorough background screening access to nuclear facilities and nuclear materials is unwise. Many IAEA inspectors, safeguards personnel, and high-level managers are probably more thoroughly screened when applying for a personal credit card than when they are granted access to seals, safeguards data, monitoring hardware, and nuclear materials and facilities. The IAEA also appears unprepared for social engineering and other attacks upon seal inspectors and managerial IAEA personnel involved in the safeguards program.

The reliability of IAEA safeguards and tamper detection is weakened by the organization's lack of basic security measures. Little of substance has changed from 1994 when David Kay accused the IAEA of being "...an international bureaucracy that does not even perform background checks on its own staff before or after hiring, has no real communications security, does not have document storage that measures up to national secure storage standards, and lacks any counterintelligence culture or capability."[87]

NEW TAMPER DETECTION APPLICATIONS

There is considerable interest in using "e-monitoring" such as video surveillance and remote monitoring systems for treaty monitoring purposes.[88] Traditionally, video surveillance has been used to protect facilities from outside attack, or for double-checking the activities of insiders. In the case of treaty monitoring, however, the potential adversaries are typically neither outside intruders nor rogue insiders. The adversary is the nation that owns the facility and the very walls that the video cameras are mounted on. Little analysis of video security has been conducted in this context, a context that is not simply a trivial extension of conventional video monitoring approaches.

The limited vulnerability assessment that has been done for video signals and video encryption usually assumes that the sending unit and the receiving station are physically inaccessible to the adversary. This is not a safe assumption given the relatively mundane efforts undertaken to date to protect video surveillance systems from physical tampering at the sending or receiving end, and to guard against counterfeited optical or electronic signals. Sensor data from other types of remote monitoring devices are also subject to tampering.

Even if the hardware is somehow "tamper-proof," the video encryption (or authentication) itself is likely to be vulnerable to attack.[89] This particularly should be a concern given that the most advanced encryption methods are unlikely to be available for international treaty monitoring, and that the monitored nation may be able to marshal considerable resources to break an encryption algorithm.

Continuous, close-up video monitoring of tags and seals is an unconventional type of video monitoring that may prove useful for nonproliferation or dismantlement regimes.[90] It is not uncommon to use video cameras in security applications that also employ seals. Ordinarily, however, the video surveillance is directed at a room, portal, or at people; it is usually not focused close-up on the seals themselves. Little is understood about the vulnerabilities and optimum use protocols associated with close-up, continuous video surveillance of tags and seals.

Another potentially important application for seals in treaty monitoring involves preserving inspection evidence, such as environmental samples. International arguments about the veracity of environmental samples may eventually become as controversial as arguments about drug testing results for world-class athletes.[91]

WHAT IS NEEDED?

Given the variety of problems discussed above, what is needed for better tamper detection—both now and in the future—for domestic security and safeguards, as well as for international transparency and treaty monitoring? Here are some recommendations.

1. Existing seals need to be used more effectively. This should include implementing better use protocols and more relevant training that fully incorporate a sophisticated understanding of the vulnerabilities and most likely attack scenarios of the specific seals being used. Seal inspectors should practice detecting subtlety attacked seals, and should be encouraged to think about seal vulnerabilities.
2. Existing seals and tamper detection programs need more vulnerability assessments. Any resulting recommendations should be implemented if useful, practical, and cost-effective.

3. At least some minimal level of background screening should be implemented for seal inspectors and tamper detection personnel, as well as for other inspection personnel granted access to nuclear facilities.
4. Existing seals need to be chosen with more analysis and care.
5. New/better tags and seals need to be developed, especially for transparency and treaty monitoring applications. Their vulnerabilities need to be fully understood. Better containers are also needed.[92]
6. There should be R&D on protecting video surveillance equipment and other types of remote monitoring hardware from tampering.
7. Studies should be undertaken to understand the security implications and vulnerabilities of close-up, continuous video monitoring of tags and seals.
8. Tags, seals, and tamper detection in general deserve more theoretical study and practical analysis. This should include developing a better understanding of what to do when tampering evidence is found. This is usually not well worked out in current tamper detection programs.
9. Security norms and standards for tamper detection should be further developed and widely adopted.
10. We need realistic expectations and an understanding that treaty verification is, in the end, a probabilistic, "interpretive activity"[93] that involves both evaluating the evidence and attempting to understand its meaning. No matter how sophisticated and quantitative the monitoring technology, or how great our confidence (rightly or wrongly) in it, verification will always come down to subjective judgments.

When it comes to tags and seals, the point is not to despair of the possibility of effective verification, or to abandon the use of tags, seals, and video surveillance simply because they—like all security measures—have vulnerabilities. Rather, the prudent approach is to have a realistic, continuum (non-binary) view of verification and tamper detection, a clear understanding of the vulnerabilities of the devices and security programs being used or contemplated, a willingness to incorporate reasonable countermeasures into the devices or the overall tamper detection program, and a commitment to engage in R&D to improve tamper detection and to better understand its role and limitations.

In the end, the realistic goals of any tamper detection program should be to:

1. detect amateurish or overt tampering with high probability;
2. detect tampering by a sophisticated adversary with some probability significantly above zero (but that will never be 100 percent), maximized to the extent consistent with a cost-benefit analysis;
3. have a low false alarm rate; and
4. provide a significant level of psychological deterrence by making would-be tamperers spend significant amounts of money developing/implementing an attack, and also make them worry about getting caught.

Finally, it may be worth noting that treaty verification would be considerably easier, cheaper, more negotiable, and more reliable if a limited amount of classified information could be shared between each party to a treaty. A partial release of sensitive or classified information tends to occur over time as nonproliferation or dismantlement regimes are maintained, especially when intrusive on-site inspections are involved.[94] It would be useful for both Russia and the United States to undertake a realistic review of what must truly be kept secret from each other. There may well be a category of information that can be shared between the two nations, but that must not be released to the public or to third parties.[95] The likely problem with this kind of review is that it must be thorough, holistic, and well balanced. Security managers, weapons designers, and conservative political leaders will tend to see the harm done to national security by releasing some of their own country's secrets, but may ignore or underestimate the benefits to national security of learning the analogous secrets of the other side. Intelligence analysts and disarmament advocates, on the other hand, may tend to get excited about the new information that can be gained from the other side, while being less concerned about the implications of giving up the secrets of their own nation.

[1] The views expressed in this paper are those of the author and do not necessarily reflect any official position of the Center for International Security and Cooperation (CISAC), the United States Department of Energy (DOE), or Los Alamos National Laboratory (LANL).

[2] Tampering with nuclear weapons or nuclear materials is defined as gaining unauthorized or surreptitious access for purposes of theft, diversion,

sabotage, vandalism, espionage (military, political, or industrial), or in an attempt to cheat or breakout from a treaty, commitment, or declaration.

[3] The term "safeguards" as used by the U.S. government typically means domestic nuclear Material Protection, Control, and Accounting (MPC&A) functions. Sometimes nuclear "security" and "safeguards" are considered separate functions, in which case the former is the "P" in "MPC&A" and the latter is the "C&A." There can be confusion about the differences between domestic "safeguards" and IAEA international "safeguards," the latter really being treaty monitoring, not nuclear custodianship.

[4] See, for example, Roger G. Johnston, "Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste Management," forthcoming in *Science & Global Security*; Steve Fetter and Thomas Garwin, "Tags," in Richard Kokoski and Sergey Koulik, eds., *Verification of Conventional Arms Control in Europe* (Boulder, CO: Westview Press, 1990), pp. 139-154; Oleg Bukharin and Helen M. Hunt, "The U.S.-Russian HEU Agreement: Internal Safeguards to Prevent the Diversion of HEU," *Science & Global Security* 4 (issue 2, 1994), pp. 189-212; Roger G. Johnston and Anthony R.E. Garcia, *Simple, Low-Cost Ways to Dramatically Improve the Security of Tags and Seals*, paper IAEA-SM-351/63 delivered to the Symposium on International Safeguards, sponsored by the International Atomic Energy Agency (IAEA), Vienna, Austria, October 13-17, 1997, pp. 1-9, <http://lib-www.lanl.gov/la-pubs/00418766.pdf>; Roger G. Johnston, Anthony R.E. Garcia, and W. Kevin Grace, "Vulnerability Assessment of Passive Tamper-Indicating Seals," *Journal of Nuclear Materials Management* 24 (Fall 1995), pp. 24-30; A. DeVolpi, *Tags and Seals to Strengthen Arms Control Verification*, Argonne National Laboratory Report ANL/EP/PP-71829, Argonne, IL, October 3, 1990.

[5] Roger G. Johnston, "The Real Deal on Seals," *Security Management* 41 (September 1997), pp. 93-100, <http://lib-www.lanl.gov/la-pubs/00418795.pdf>.

[6] Tamper-evident (tamper-indicating) packaging and so-called "secure containers" are other forms of tamper-indicating seals.

[7] It is thus not helpful to define a lock as "a device similar to a seal except that it can be opened with a key" as is done in Patricia Lewis, "The New Verification Game and Technologies at Our Disposal," in Dietrich Schroeer and Alessandro Pascolini, eds., *The Weapons Legacy of the Cold War: Problems and Opportunities* (Brookfield, VT: Ashgate, 1997), p. 151.

[8] DeVolpi, *Tags and Seals to Strengthen Arms Control Verification*, pp. 1-10.

[9] Roger G. Johnston and Anthony R.E. Garcia, "Vulnerability Assessment of Security Seals," *Journal of Security Administration* 20 (June 1997), pp. 15-27, <http://lib-www.lanl.gov/la-pubs/00418796.pdf>; Roger G. Johnston, "Effective Vulnerability Assessment of Tamper-Indicating Seals," *Journal of Testing and Evaluation* 25 (July 1997), pp. 451-455.

[10] R.G. Johnston and Anthony R.E. Garcia, "An Annotated Taxonomy of Tag and Seal Vulnerabilities," *Journal of Nuclear Materials Management* 28 (Spring 2000), pp. 23-30.

[11] Ibid.

[12] "Social engineering" is compromising security by manipulating, exploiting, or compromising people.

[13] David Anderson, *Nuclear Safeguards*, Australian Foreign Affairs, Parliamentary Research Service, <http://www.aph.gov.au/senate/committee/uranium_ctte/report97/ch12_0.htm>.

[14] Duncan W. MacArthur and Rena Whiteson, *Comparison of Hardware and Software Approaches to Information Barrier Construction*, Los Alamos National Laboratory Report LAUR-00-2422.

[15] See, for example, Albert Gore, Jr., "Verification of Arms Control Limits on Mobile Missiles," in Michael Krepon and Mary Umberger, eds., *Verification and Compliance: a Problem-Solving Approach* (Cambridge, MA: Ballinger. 1988), pp. 3-16; Lawrence Scheinman, "Nonproliferation Regime: Safeguards, Controls, and Sanctions," in Jack N. Barkenbus, Marcelo Alonso, and Alvin M. Weinberg, eds., *The Nuclear Connection: a Reassessment of Nuclear Power and Nuclear Proliferation* (New York: Paragon House, 1985), pp. 193-199; National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium* (Washington, D.C.: National Academy Press, 1994), pp. 55-59; Thomas C. Schelling and Morton H. Halperin, *Strategy and Arms Control* (New York: Pergamon-Brassey, 1985), pp. 91-106; Bukharin and Hunt, "The U.S.-Russian HEU Agreement," pp. 199-201; Paul Leventhal, *Safeguards Shortcomings—A Critique*, <http://www.nci.org/plsgrds.htm>; Washington Nuclear Corporation, "Containment and Surveillance" and "Other Safeguards Requirements" Sections, *Safeguards and Security*, <http://www.nuke-energy.com/data/safeguards.html>; David L. Poli, *Security Seal Handbook*, Sandia National Laboratories Report SAND78-0400, December 1978, <http://www.sandia.gov/doe-oss/DOC-Reports.html>; James L. Jones, *Improving Tag/Seal Technologies: the vulnerability assessment component*, Idaho National Engineering Laboratory Report 95/00599, December 1996.

[16] See, for example, George Bunn, "Raising International Standards for Protecting Nuclear Materials from Theft and Sabotage," *Nonproliferation Review* 7 (Summer 2000), pp. 146-156; Matthew Bunn, "Security for Weapons-Usable Nuclear Materials: Expanding International Cooperation, Strengthening International Standards," in *Comparative Analysis of Approaches to Protection of Fissile Materials: Proceedings of a Workshop at Stanford University*, July 28-30, 1997, Lawrence Livermore National Laboratory Report Conf-97-0721, <http://ksgnotes1.harvard.edu/BCSIA/Library.nsf/pubs/s4wunm>.

[17] Manufacturers and vendors of tags, seals, and video surveillance equipment do not help the situation by claiming—usually without offering a shred of evidence—that their products are "tamper-proof." See, for example,
<http://www.randtec.com/versatag.htm>;
<http://www.aquilagroup.com/safeguards/safeguards_overview.html>;
<http://rsasecurity.com/news/pr/950923.html>;
<http://www.techlabsinc.com/ids.html>;
<http://www.aitechnology.com/st2.html>;
<http://www.ford.co.uk/fd/fdst.html>;
<http://www.canberra.com/literature/technical_ref/safeguards/rf_seal.htm>.

[18] The term "tamper-resistant" is sometimes used instead of "tamper-proof" when discussing tags and seals. This is at least less absolute, but it is still misleading. Many seals are made of paper or plastic and can be easily ripped open—thus not resisting tampering in the slightest. This does not automatically make them ineffective as seals. Because they were so misleading, the U.S. Food and Drug Administration abandoned its original terms "tamper-proof" and "tamper-resistant" in referring to packaging, and now requires "tamper-evident" packaging for over-the-counter pharmaceuticals. Note that we can probably dismiss as disingenuous the idea that the "tamper-resistance" provided by a seal actually refers to the (very real) psychological hesitancy on the part of an adversary to attempt tampering if he may be caught by the seal.

[19] Johnston and Garcia, "Vulnerability Assessment of Security Seals," pp. 15-27, <http://lib-www.lanl.gov/la-pubs/00418796.pdf>; Johnston, "Effective Vulnerability Assessment of Tamper-Indicating Seals," pp. 451-455.

[20] See, for example, Steve Fetter, *Verifying Nuclear Disarmament*, Occasional Paper No. 29, Henry L. Stimson Center, October 1996; Michael Krepon, "Technology Won't Solve Verification Problems," *Bulletin of the Atomic Scientists* 41 (February 1985), pp. 3-4; David B. Thomson, *A Guide to the Nuclear Arms Control Treaties*, Los Alamos National Laboratory Report LAUR 99-3173, July 1999, p. 235; Harold A. Feiveson, *The Nuclear Turning Point* (Washington, D.C.: Brookings Institution Press, 1999), pp. 226-229, 239; Kathleen Vogel, "Ensuring the Security of Russia's Chemical Weapons: A Lab-to-Lab Partnering Program," *Nonproliferation Review* 6 (Winter 1999), pp. 70-83, <http://cns.miis.edu/pubs/npr/vogel62.htm>; Paul Leventhal and Brahma Chellaney, *Nuclear Terrorism: Threat, Perception and Response in South Asia*, Paper for the Institute for Defense Studies and Analyses, New Delhi, October 10, 1988, <http://www.nci.org/pl-bc.htm>; Jason D. Ellis and Todd Perry, *Nunn Lugar's Unfinished Agenda*, October 1997, <http://www.armscontrol.org/ACT/oct97/nunnoct.htm>; Nazir Kamal, *Pakistani Perceptions and Prospects of Reducing the Nuclear Danger in South Asia*, Cooperative Monitoring Center Occasional Paper/6, Report SAND98-0505/6, January 1999, <http://www.cmc.sandia.gov/issues/papers/pakisperc/>; David Albright and Tom Zamora, "South Africa flirts with the NPT," *Bulletin of the Atomic Scientists* 47 (January/February 1991), pp. 27-31, <http://www.bullatomsci.org/issues/1991/jf91/jf91albright.html>; Greenpeace International, Amsterdam (GP), *TL: a Nuclear Weapons Materials Production Cutoff: Stopping the Arms Race at the Source*, 1990, <http:/

/www.alternatives.com/library/env/envgmil/nukes2.txt>; Theodore B. Taylor, "Global Abolition of Nuclear Weapons—Verification of Compliance of and Deterrents to Violation," Draft of Contributed Paper for Working Group 2 of 40th Pugwash Conference, September 15-20, 1990, Egham, United Kingdom, <http://www.tbtaylor.com/ZNAPUG.htm>; Robert Mozley, "Verifying the Number of Warheads on Multiple-warhead Missiles," in Frank von Hippel and Roald Z. Sagdeev, eds., *Reversing the Arms Race* (New York: Gordon and Breach, 1990), p. 120; Alexei A. Vasillev, Mikhail Gerasev, and Sergei Oznobishchev, "SLCMs: Regimes for Control and Verification," in von Hippel and Sagdeev, eds., *Reversing the Arms Race,* p. 146; Karl Pieragostini, "Cooperative Verification," in Robert Travis Scott, ed., *The Race for Security: Arms and Arms Control in the Reagan Years* (Lexington, MA: Lexington Books, 1987), p. 266; Ann M. Florini, "A New Role For Transparency," in Nancy Gallagher, ed., *Contemporary Security Policy* 18 (August 1997), p. 60.

[21] "Seals...allow conclusions that no material has disappeared," according to IAEA, *International Safeguards and the Peaceful Uses of Nuclear Energy*, <http://f40.iaea.org/worldatom/Periodicals/Factsheets/English/safeguards.html>. See also, Jonathan Dean, "Step-By-Step Control Over Ballistic and Cruise Missiles," *Disarmament Diplomacy* Issue 31 (October 1998), Global Beat, <http://www.nyu.edu/globalbeat/nuclear/Jdean1098.html>; "Political Factors in the Development and Implementation of Technology-Based Confidence Building Measures," final draft report published in *Proceedings of the Conference on Technology-Based Confidence-Building Measures*, Center for National Security Studies, University of California and Los Alamos National Laboratory, July 1989, pp. 413-426; Valerie Thomas, "Verification of Limits on Long-Range Nuclear SLCMs," *Science & Global Security* 1 (issues 1 & 2, 1989), pp. 29-39; Taylor, "Global Abolition of Nuclear Weapons—Verification of Compliance of and Deterrents to Violation"; Robert Mozley, "Verifying the Number of Warheads on Multiple-warhead Missiles," p. 120 ff.

[22] An outstanding analysis of the psychology and politics of treaty verification can be found in Nancy Gallagher, *The Politics of Verification* (Baltimore: John Hopkins University Press, 1999).

[23] Theodore B. Taylor, 'Dismantlement and Fissile-material Disposal," in von Hippel and Sagdeev, eds., *Reversing the Arms Race*, p. 101; Steven Fetter and Thomas Garwin, "Using Tags to Monitor Numerical Limits in Arms Control Agreements," in Barry M. Blechman, ed., *Technology and the Limitation of International Conflict* (Washington, D.C.: Foreign Policy Institute, 1989), pp. 38-47; Vasillev, Gerasev, and Oznobishchev, "SLCMs: Regimes for Control and Verification," p. 146; Dean, "Step-By-Step Control Over Ballistic and Cruise Missiles".

[24] Juergen Altmann, Peter Deak, Catherine McArdle Kelleher, and Vadim I. Makarevsky, "Verification and Conventional Arms Reduction," in Francesco Calogero, Marvin L. Goldberger, and Sergei P. Kapitza, eds., *Verification: Monitoring Disarmament* (Boulder, CO: Westview Press, 1991), pp. 189-191; Theodore B. Taylor, "Dismantlement and Fissile-material Disposal," p. 101; Steve Fetter, "A Comprehensive Transparency Regime for Warheads and Fissile Materials," *Arms Control Today* 29 (January/February 1999), p. 5. Counterfeiting is only one possible method for defeating a tag or seal, and usually not the easiest. Even so, counterfeiting complex surface morphologies or properties is not as difficult as many assume. In my experience, it is often trivial. The difficulty of counterfeiting, however, depends critically on the sophistication (often minimal) of the inspection procedure or postmortem analysis that must be spoofed. Note that counterfeiters are NOT, as is often assumed, limited to exactly the same methodology or technology that was originally used to create the unique surface morphology or property. In general, adversaries do better if they do not let the user or developer of the tag/seal define the problem.

[25] Rose Gottemoeller, "Verification of Arms Control Limits on Mobile Missiles," in Michael Krepon and Mary Umberger, eds., *Verification and Compliance: a Problem-Solving Approach* (Cambridge, MA: Ballinger, 1988), pp. 32-33; Fetter and Garwin, "Using Tags to Monitor Numerical Limits in Arms Control Agreements," p. 47; Vasillev, Gerasev, and Oznobishchev, "SLCMs: Regimes for Control and Verification," p. 146; Dean, "Step-By-Step Control Over Ballistic and Cruise Missiles"; Pieragostini, "Cooperative Verification," p. 266; Scheinman, "Nonproliferation Regime: Safeguards, Controls, and Sanctions," pp. 193-199; Fetter, "A Comprehensive Transparency Regime for Warheads and Fissile Materials," pp. 5, 7.

[26] See, for example, Thomas, "Verification of Limits on Long-Range Nuclear SLCMs," pp. 29-39; Greenpeace, *TL: a Nuclear Weapons Materials Production Cutoff.*

[27] Vasiliev, Gerasev, and Oznobishchev, "SLCMs: Regimes for Control and Verification," p. 146; Fetter and Garwin, "Using Tags to Monitor Numerical Limits in Arms Control Agreements," p. 46; Albright and Zamora, "South Africa flirts with the NPT," pp. 30-31.

[28] Johnston, "Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste Management"; Poli, *Security Seal Handbook*; Naval Facilities Engineering Services Center (NFESC), *Antipilferage Seal User's Guide*, October 1997, <http://locks.nfesc.navy.mil/lockweb/security%20seals/sp2086.pdf>; Naval Facilities Engineering Services Center (NFESC), *DoD Training Course on Effective Seal Use*, Spring 2000, <http://locks.nfesc.navy.mil/lockweb/security%20seals/sp2086.pdf>; James L. Jones, *Improving Tag/Seal Technologies*; Ross Anderson, <http://www.cl.cam.ac.uk/Research/Security/tamper>; Patricia M. Lewis, "Verification Experiments in the 1960s: from CLOUD GAP to Exercise FIRST LOOK," in R. Kokoski and S. Koulik, eds., *Verification of Conventional Arms Control in Europe: Technological Constraints and Opportunities* (Boulder, CO: Westview Press, 1990), p. 264; Ross Anderson and Markus Kuhn, "Tamper Resistance—a Cautionary Note," *Proceedings of the Second USENIX Workshop on Electronic Commerce*, Oakland, CA, November 18-21, 1996, pp. 1-11, <http://www.cl.cam.ac.uk/users/rja14/tamper.html>; Johnston, "The Real Deal on Seals," pp. 93-100; Johnston and Garcia, "Vulnerability Assessment of Security Seals," pp. 15-27; Johnston and Garcia, "An Annotated Taxonomy of Tag and Seal Vulnerabilities," pp. 23-30; Washington Nuclear Corporation, *Safeguards and Security*.

[29] Johnston, "Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste Management"; Johnston, "Effective Vulnerability Assessment of Tamper-Indicating Seals," pp. 451-452; Johnston and Garcia, "An Annotated Taxonomy of Tag and Seal Vulnerabilities," pp. 23-30.

[30] Even the U.S. Food and Drug Administration (FDA) "standards" for the tamper-evident packaging legally required for U.S. over-the-counter drugs are skimpy and vague. Yet this is an area where one would expect there to be enormous care and effort, and well developed standards. See, for example: Title 21 of the *Code of Federal Regulations*, Sec 211.132 covering tamper-evident packaging requirements for over-the-counter (OTC) drugs and also FDA, May 21, 1992, *Tamper-Resistant Packaging Requirements for Certain Over-the-Counter (OTC) Human Drug Products*, FDA Compliance Guides, Chapter 32A, Drug Alteration Guide 7132A.17.

[31] A vulnerability assessment involves finding and demonstrating weaknesses (vulnerabilities) in a tag, seal, or tamper detection program, perhaps accompanied by suggested countermeasures. A definition of an "effective" vulnerability assessment can be found in Johnston, "Effective Vulnerability Assessment of Tamper-Indicating Seals," pp. 451-455.

[32] Seal "use protocols" (or simply "protocols") are the official and unofficial procedures used for seal procurement, storage, accounting, installation, inspection, removal, disposal, reporting, interpreting, and training. A seal is no better than the protocols for using it.

[33] Johnston, "Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste Management."

[34] Theodore B. Taylor, "Technical Requirements for Nuclear Safeguards," talk at the Symposium on Safeguards Research and Development, Argonne National Laboratory, June 26, 1967, <http://www.tbtaylor.com/6706m.htm>; Lewis, "The New Verification Game and Technologies at Our Disposal," p. 155; Gerard C. Smith, "No Dead End for Arms Control," *Bulletin of the Atomic Scientists* 41 (January 1985), pp. 3-4; The Canberra Commission on the Elimination of Nuclear Weapons, Annex A, November 1995, <http://www.dean.usma.edu/socs/ECON/ens/canberra_A.htm>; Matthew Bunn, "A Detailed Analysis of the Urgently Needed New Steps to Control Warheads and Fissile Material," in Joseph Cirincione, ed., *Repairing the Regime* (New York: Routledge, 2000), pp. 80-103; Thomas, "Verification of Limits on Long-Range Nuclear SLCMs," p. 29; Ivan Oelrich and Victor Utgoff, "Confidence Building with Unmanned Sensors in Central Europe," in Barry M. Blechman, ed., *Technology and the Limitation of International Conflict*

(Washington, D.C.: Foreign Policy Institute, 1989), p. 24.

35 Johnston and Garcia, "Vulnerability Assessment of Security Seals," pp. 15-27; Johnston, Garcia, and Grace, "Vulnerability Assessment of Passive Tamper-Indicating Seals," pp. 24-30; Johnston, "The Real Deal on Seals," pp. 93-100.

36 See, for example, "INF Shows High-Tech On-Site Treaty Monitoring Not Essential, Expert Says," *Aerospace Daily*, December 27, 1989, p. 480; Altmann, Deak, McArdle Kelleher, and Makarevsky, "Verification and Conventional Arms Reduction," p. 184; Johnston, "Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste Management."

37 Vogel, "Ensuring the Security of Russia's Chemical Weapons," p. 81.

38 Johnston, "Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste Management"; Johnston, "Effective Vulnerability Assessment of Tamper-Indicating Seals," pp. 451-452; Johnston and Garcia, "An Annotated Taxonomy of Tag and Seal Vulnerabilities," pp. 23-30.

39 See, for example, Pieragostini, "Cooperative Verification," p. 266; Fetter and Garwin, "Using Tags to Monitor Numerical Limits in Arms Control Agreements," pp. 38, 41. The term "black box" has two slightly different meanings in the context of transparency and treaty monitoring. It usually refers to a device or system that has internal workings unknown (wholly or in part) by the nation, facility, or personnel being monitored for compliance. This type of black box is not generally going to be allowed close to nuclear warheads, for example, due to nuclear explosive safety, security, and espionage concerns. Sometimes, "black box" refers instead to a device or system that *is* fully understood by the people being monitored, but that they are supposed to leave alone. The two definitions actually merge, however, in that the only way the monitored party can be absolutely sure of what the device or system is actually doing is to reverse-engineer it, which requires tampering.

40 Black boxes make sense for seismic monitors because such monitors can be placed miles away from nuclear facilities and test sites. Concerns about mystery hardware and encryption are thus substantially less than for on-site inspection and monitoring inside critical nuclear facilities.

41 See for example, U.S. Department of Energy (DOE), "Nuclear Explosive Safety Study Process," DOE Standard DOE-STD-3015-97, January 1997, <http://tis.eh.doe.gov/search97cgi/s97_cgi.exe>.

42 There tends to be enormous concern on the Russian side about the possibility of audio listening devices being covertly embedded inside monitoring hardware.

43 The comments in this section, except where other sources are cited, are based on the author's first-hand experiences.

44 Richard Feynman gives an entertaining (but unhappily all too common) account of the pitfalls of exposing security vulnerabilities in Edward Hutchings, Ralph Leighton, Richard Phillips Feynman, and Albert Hibbs, *Surely You are Joking, Mr. Feynman: Adventures of a Curious Character* (New York: Bantam, 1985), pp. 119-137.

45 Kevin J. Soo Hoo, *How Much is Enough? A Risk-Management Approach to Computer Security*, CISAC Working Paper, Center for International Security and Cooperation, August 2000, p. 15.

46 DOE, *Followup Review of Fissile Material Assurances in the Department of Energy Complex*, Report by the Office of Oversight of the Office of Environment, Safety, and Health, DOE, July 1998, <http://tis.eh.doe.gov/iopa/reports/specrevs/specrevs_cont.html>; U.S. General Accounting Office (GAO), *Nuclear Nonproliferation: Uncertainties with Implementing IAEA's Strengthened Safeguards System*, GAO Report NSIAD/RCED-98-184, July 9, 1998, pp. 6-8, <http://www.fas.org/spp/starwars/fao/nsaid-98-184.htm>; Leventhal, *Safeguards Shortcomings*; Washington Nuclear Corporation, *Safeguards and Security*.

47 See, for example, DOE, Office of Safeguards and Security, *Safeguards Seals Reference Guide*, September 1995, pp. 3, 17, 20-21, and F-1.

48 Abrams and Pollack, for example, discuss seals only in the section on physical security, but not in the MC&A section: Herbert L. Abrams and Daniel Pollack, "Security Issues in the Handling and Disposition of Fissionable Material," *Contemporary Security Policy* 15 (December 1994), pp. 2-17.

49 Seals play a role in nuclear accounting, not just control/containment. See, for example, Anderson, *Nuclear Safeguards*; U.S. Nuclear Regulatory Commission, *Tamper-Indicating seals for the Protection and Control of Special Nuclear Material*, Regulatory Guide 5.15, Revision 1, March 1997, <http://www.nrc.gov/NRC/RG/05/05-015.html>. Seals can be used to detect tampering with accounting data, analysis results, and material accountancy instruments, including their calibrations. Seals can also be used to help assure that materials that have already been counted or assayed do not require a new analysis or re-inventory. Indeed, such inventory control is one of the major non-nuclear, commercial applications for seals.

50 For a good discussion of the vulnerabilities associated with (for example) visual surveillance and two-man rules, see Bukharin and Hunt, "The U.S.-Russian HEU Agreement," pp. 199-201.

51 An excellent discussion of how redundancy often makes things worse, not better, can be found in Scott D. Sagan, *The Problem with Redundancy Problem: Or Why Organizations Try Harder and Fail More Often*, unpublished manuscript, Center for International Security and Cooperation, Stanford University, 2000.

52 Johnston and Garcia, *Simple, Low-Cost Ways to Dramatically Improve the Security of Tags and Seals*, pp. 1-9; Johnston, "Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste Management"; Johnston and Garcia, "Vulnerability Assessment of Security Seals," pp. 15-27.

53 I have often heard it said that the differences between domestic safeguards and international safeguards are widely understood. Perhaps this is so on some theoretical level. In practice, however, DOE and DOD personnel, security managers, arms control theorists, and the public often treat international safeguards as if they were extensions of domestic safeguards. See Paul L. Chrzanowski, *Preparation for the Nuclear Non-Proliferation Treaty Extension Conference in 1995*, Lawrence Livermore National Laboratory Report UCRL-JC-113936, pp. 9-10; and Leventhal, *Safeguards Shortcomings*. Descriptions of what the IAEA does sometimes make it sound as if the IAEA acts as a custodian of nuclear materials, rather than simply as a verifier of treaty commitments. See, for example, Alan S. Krass, "Arms Control and Treaty Verification," in Mary E. Lord, ed., *Encyclopedia of Arms Control and Disarmament* (New York: Scribner's & Sons, 1993), pp. 308-309; Hans Blix, "The Peaceful and Safe Uses of Nuclear Energy," paper for the IAEA/OPANAL Seminar on IAEA Safeguards: Verifying Compliance with Non-Proliferation Commitments, Kingston, Jamaica, 25 April 1996, <http://www.iaea.org/worldatom/Press/Statements/FormerDG/dgsp1996n04.html>; Mohamed Elbaradei, *Safeguarding the Atom*, IAEA Bulletin (April 1999), <http://www.iaea.org/worldatom/Periodicals/Bulletin/Bull414/article1.pdf>. It is not surprising that there should be confusion about tamper detection for verification purposes when transparency and treaty monitoring themselves are so poorly understood. See, for example, Ronald B. Mitchell, "Sources of Transparency: Information Systems in International Regimes," *International Studies Quarterly* 42 (March 1998), pp. 109-130.

54 Thus historically, many IAEA seals and their use protocols were simply copied from those used for U.S. domestic security and safeguards. This occurs despite the fact that the IAEA "safeguards program" (actually treaty monitoring) differs substantially from U.S. nuclear "safeguards" (MC&A). In some cases, however, the IAEA has implemented significant improvements or modifications, such as the double e-cup vs. the single e-cup.

55 Ivan C. Oelrich, "Production Monitoring for Arms Control," in Michael Krepon and Mary Umberger, eds., *Verification and Compliance: a Problem-Solving Approach* (Cambridge, MA: Ballinger, 1988), p. 116.

56 There are also problems with sharing classified information from a seals' database with foreigners.

57 Johnston, "Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste Management."

58 Roger G. Johnston, Debbie D. Martinez, and Anthony R.E. Garcia, "Were Ancient Seals Secure?," forthcoming in *Antiquity*.

59 Johnston, "Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste Management"; Johnston, "Effective Vulnerability Assessment of Tamper-Indicating Seals," pp. 451-452; Johnston and Garcia, "An Annotated Taxonomy of Tag and Seal Vulnerabilities," pp. 23-30.

60 Oleg Bukharin and William Potter, "Potatoes Were Guarded Better," *Bulletin of the Atomic Scientists* 51 (May/June 1995), p. 46-50; IAEA, "Requirements for Physical Protection Against Unauthorized Removal of Nuclear Material in Use and Storage," INFCIRC/225/Revision 4, <http://

www.iaea.org.worldatom/program/protection/inf225rev4/rev4_removal.html>; Bunn, "Raising International Standards for Protecting Nuclear Materials from Theft and Sabotage," pp. 146-156; Bunn, "Security for Weapons-Usable Nuclear Materials."

[61] The comments in this section, except where other sources are cited, are based on the author's first-hand experiences.

[62] Jessica Eve Stern, "Cooperative Activities to Improve Fissile Material Protection, Control, and Accounting," in John M. Shields and William C. Potter, eds., *Dismantling the Cold War: U.S. and NIS Perspectives on the Nunn-Lugar Cooperative Threat Reduction Program* (Cambridge, MA: MIT Press, 1997), p. 309-344; Abrams and Pollack, "Security Issues in the Handling and Disposition of Fissionable Material," pp. 9-11, 16-17; Kevin O'Neill, "The Risk of Theft: Protecting Fissile Materials in the Former Soviet Union," in David Albright and Kevin O'Neill, eds., *The Challenges of Fissile Material Control* (Washington, D.C.: Institute for Science and International Security, 1999), pp. 69-83; Bukharin and Potter, "Potatoes Were Guarded Better," p. 46-50; Bunn, "A Detailed Analysis of the Urgently Needed New Steps to Control Warheads and Fissile Material," pp. 80-103, 122; National Research Council, *Protecting Nuclear Weapons Material in Russia* (Washington, D.C.: National Academy Press, 2000), <http://books.nap.edu/html/nwm_russia/index.html>.

[63] *Preventing Nuclear Proliferation: The Cold War Challenge*, Lawrence Livermore National Laboratory, <http://www.llnl.gov/str/Dunlop2.html>; Matthew Bunn, "Remarks for the Carnegie International Non-Proliferation Conference," March 16, 2000, <http://www.ceip.org/Programs/npp/bunn2000.htm>; Bunn, "Security for Weapons-Usable Nuclear Materials"; Bukharin and Potter, "Potatoes Were Guarded Better," p. 48; Stern, "Cooperative Activities to Improve Fissile Material Protection, Control, and Accounting," p. 309-344; National Research Council, *Protecting Nuclear Weapons Material in Russia*, p. 10.

[64] See, for example, National Research Council, *Protecting Nuclear Weapons Material in Russia*, p. 10; Stern, "Cooperative Activities to Improve Fissile Material Protection, Control, and Accounting," pp. 309-344.

[65] Bunn, "A Detailed Analysis of the Urgently Needed New Steps to Control Warheads and Fissile Material," pp. 80-103; National Research Council, *Protecting Nuclear Weapons Material in Russia*, pp. 19-20; Johnston, "The Real Deal on Seals," p. 100.

[66] Bradley Graham, "Weaknesses Found in Nuclear Safeguards; Energy Dept. Report Urges Improvement in U.S. Protection of Russian Stockpile," *Washington Post*, September 25, 1999, p. A11, <http://search.washingtonpost.com/wp-srv/WPlate/1999-09/25/135l-092599-idx.html>; National Research Council, *Protecting Nuclear Weapons Material in Russia*, pp. 21-22; *Combating Proliferation of Weapons of Mass Destruction*, Report of the Commission to Access the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction, pp. 62-64.

[67] U.S. Senate, Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, *The Defense Department's Cooperative Threat Reduction Program and the Energy Department's Russian Nonproliferation Program*, 106th Congress, 2nd sess., March 6, 2000.

[68] Center for Nonproliferation Studies, "The Moscow Summit: Mayak Fissile Material Storage Facility," <http://cns.miis.edu/research/summit/mayak.htm>.

[69] U.S. Senate, Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, *The Defense Department's Cooperative Threat Reduction Program and the Energy Department's Russian Nonproliferation Program*, 106th Congress, 2nd sess., March 6, 2000.

[70] See, for example, Matthew Bunn and John P. Holdren, "Managing Military Uranium and Plutonium in the United States and the Former Soviet Union," *Annual Review of Energy and the Environment* 22 (1997), p. 406; M. Willrich and Theodore B. Taylor, *Nuclear Theft: Risks and Safeguards* (Cambridge, MA: Ballinger, 1974); and U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, *Nuclear Weapon Facilities: Adequacy of Safeguards and Security at Department of Energy Nuclear Weapons Production Facilities*, 99th Congress, 2nd Session, March 6, 1986; Bunn, "Raising International Standards for Protecting Nuclear Materials from Theft and Sabotage," p. 149-150.

[71] See, for example, Abrams and Pollack, "Security Issues in the Handling and Disposition of Fissionable Material," pp. 6-9, 14-16; DOE, *Followup Review of Fissile Material Assurances in the Department of Energy Complex*; Bunn and Holdren, "Managing Military Uranium and Plutonium in the United States and the Former Soviet Union," p. 406 ff.; Willrich and Taylor, *Nuclear Theft*; U.S. House of Representatives, *Nuclear Weapon Facilities*. In the United States from 1979-1987, for example, there were 87 known incidents involving insiders tampering with nuclear power plant instruments or equipment to interfere with plant operations. (Gordon Thompson, *War, Terrorism and Nuclear Power Plants*, Working Paper No. 165, Australian National University Peace Research Center, 1996, p. 23.)

[72] See, for example, the April 28, 1999 Statement by Secretary of Energy Bill Richardson at <http://www.securitymanagement.com/library/nuclear.htm>; DOE, *Proposed Action and Alternatives*, <http://tis.eh.doe.gov/nepa/docs/deis/eis0279/2/SNF_2.html>; DOE, *II. Improving the Security of Nuclear Material at the Latvian Academy of Sciences Nuclear Research Center: Material Control and Accounting (MC&A) System*, <http://www.nn.doe.gov/mpca/pubs/latvia/lat_mca.htm>.

[73] DOE, *Safeguards Seals Reference Guide*, pp. 3, 17, 20-21, and F-1.

[74] Ibid., p. 4.

[75] An example is the Materials Monitoring System (MMS), including the T-1 active fiber optic seal, developed by Sandia National Laboratories. The MMS is in use at the Savannah River Materials Storage Area for U.S. domestic security and safeguards, has been given to the Russians, and will be turned over to the IAEA for international safeguards under the U.S.-Russia-IAEA trilateral initiative. See Sandia National Laboratories, *Arms Control Verification, Sensors, and Monitoring Systems*, Sandia Lab News, February 28, 2000, <http://www.sandia.gov>.

[76] A particularly thoughtful analysis of IAEA problems can be found in Anderson, *Nuclear Safeguards*. See also David Kay, "The IAEA: How can it be Strengthened?," in Mitchell Reiss and Robert S. Litwak, eds., *Nuclear Proliferation After the Cold War* (Washington D.C.: Woodrow Wilson Press, 1994), p. 319-332; Gordon Thompson, "Verifying a Halt to the Nuclear Arms Race," in Frank Barnaby, ed., *A Handbook of Verification Procedures* (New York: Macmillan, 1990), pp. 202-207.

[77] A "postmortem exam" = "postmortem analysis" means taking a tag or seal to a laboratory for later analysis after it has been inspected and removed in the field. Such an analysis, which may be low-tech or high-tech, can dramatically improve the odds of detecting tampering or counterfeiting.

[78] Scheinman, "Nonproliferation Regime," pp. 195-196.

[79] Ibid., pp. 195-199; Blix, *The Peaceful and Safe Uses of Nuclear Energy*; IAEA, *International Safeguards and the Peaceful Uses of Nuclear Energy*.

[80] See, for example, Tom Graham, *Disarmament: Ending Reliance on Nuclear and Conventional Arms*, Transcripts of the Disarmament Week Symposium, sponsored by the United Nations, New York, October 25-27, 1994, U.N. Publication E.95.IX.4, p. 63; Gerald M. Steinberg, "US Non-Proliferation Policy: Global Regimes and Regional Realities," *Contemporary Security Policy* 15 (December 1994), pp. 132-135; Scheinman, "Nonproliferation Regime," p. 199; Leventhal, *Safeguards Shortcomings*; Anderson, *Nuclear Safeguards*.

[81] Scheinman, "Nonproliferation Regime," pp. 193-199; Bunn, "Security for Weapons-Usable Nuclear Materials"; Kay, "The IAEA," pp. 319-332; Graham, *Disarmament*, p. 63-65; Leventhal, *Safeguards Shortcomings*; Anderson, *Nuclear Safeguards*.

[82] National Academy of Sciences, *Nuclear Arms Control: Background and Issues* (Washington, D.C.: National Academy Press, 1985), p. 265; Chrzanowski, *Preparation for the Nuclear Non-Proliferation Treaty Extension Conference in 1995*, pp. 9-10; Kay, "The IAEA," pp. 319-332; Leventhal, *Safeguards Shortcomings*; Anderson, *Nuclear Safeguards*; Steinberg, "US Non-Proliferation Policy," pp. 132-135.

[83] This may be partially due to the IAEA's unwillingness to admit that vulnerabilities exist.

[84] James F. Keeley, "Verification, On-Site Inspection and '93+2'," in Andrew Lathan, ed., *Multilateral Approaches to Non-Proliferation*, Proceedings of the 4th Canadian Non-Proliferation Workshop, 1995, pp. 75-94; Kay, "The IAEA," pp. 319-332; Anderson, *Nuclear Safeguards.*

[85] Frances Mautner-Markhof, "The IAEA Experience," in Richard Kokoski

and Sergey Koulik, eds., *Verification of Conventional Arms Control in Europe* (Boulder, CO: Westview Press, 1990), p. 256.

[86] Schelling and Halperin, *Strategy and Arms Control*, pp. 91-106; Bunn, "Raising International Standards for Protecting Nuclear Materials from Theft and Sabotage," pp. 148, 151; Johnston and Garcia, "An Annotated Taxonomy of Tag and Seal Vulnerabilities," pp. 23-30.

[87] Kay, "The IAEA," p. 326.

[88] GAO, *Nuclear Nonproliferation*, pp. 6-8; Elbaradei, *Safeguarding the Atom*; International Atomic Energy Agency (IAEA), 1997 Annual Report, Safeguards Section, <http://www.iaea.org/worldatom/inforesource/annual/anrep97/sfgds.html>.

[89] For discussions of why real-world encryption is vulnerable, see Bruce Schneier, *Secrets and Lies* (New York: Wiley, 2000), pp. xi-xiii, 346-398; Ivars Peterson, "Chinks in the digital armor: exploiting faults to break smart-card cryptosystems," *Science News* 151 (February 1,1997), pp. 78-79, <http://www.sciencenews.org/sn_arc97/2_1_97/bob1.htm>; Ross Anderson, <http://www.cl.cam.ac.uk/Research/Security/tamper>; Anderson and Kuhn, "Tamper Resistance," pp. 1-11; Bruce Schneier, "DVD Encryption Break is a Good Thing," *ZDNet News*, November 16, 1999, <http://www.zdnet.com/zdnn/stories/comment/0,5859,2395497,00.html>.

[90] Eric R. Gerdes, Roger G. Johnston, and James D. Doyle, "A Proposed Approach for Monitoring Nuclear Warhead Dismantlement," forthcoming in *Science & Global Security*.

[91] See for example, "Cuban Denies Cocaine Use; Official Says Test was Sabotaged," *Seattle Post-Intelligencer*, August 6, 1999, Sports Section; *Cuba Wire: Cuban Sports Official: Sotomayor Drug Charge a Frameup*, August 6, 1999, <http://www.mapinc.org/drugnews/v99.n809.a10.html>.

[92] Gerdes, Johnston, and Doyle, "A Proposed Approach for Monitoring Nuclear Warhead Dismantlement."

[93] For an excellent discussion of the meaning of verification, including its intrinsic nature as "an interpretive activity" (p. 39), see Seong W. Cheon and Niall M. Fraser, "Arms Control Verification: An Introduction and Literature Survey," *Arms Control* 9 (May 1988), pp. 38-58.

[94] Raymond R. McGuire, "The Impact of Intrusive Inspections on Sensitive Government Facilities," in Kathleen C. Bailey, *Director's Series on Proliferation*, Lawrence Livermore National Laboratory Report UCRL-LR-114070-4, May 23, 1994, pp. 101-108; Feiveson, *The Nuclear Turning Point*, pp. 226-229.

[95] Hopefully such a review would result in a new classification category. This is certainly needed for classified transport information. For legitimate security reasons, the United States considers information about the movement of nuclear weapons to be secret. Under future dismantlement regimes, Russian or third-party inspectors may need advance notice about the movement of treaty-limited items and might even accompany them in transit. This creates the somewhat bizarre situation (which has already occurred) where adversarial foreigners are given classified information that the U.S. government keeps from its own citizens. A new classification scheme would similarly be useful for confidential/secret deliberations and agreements undertaken via bilateral commissions such as the Standing Consultative Commission (SCC) created by the U.S. and Soviet Union in 1972 to deal with a variety of treaty issues. See Gloria Duffy, "Arms Control Treaty Compliance," in Mary E. Lord, ed., *Encyclopedia of Arms Control and Disarmament* (New York: Scribner's Sons, 1993), pp. 289-292. Ideally, any new scheme to classify such information would avoid the problems of information categories such as "UCNI" (DOD/DOE), "Official Use Only" (DOE), or "Safeguards Confidential" (IAEA). In practice, these categories are often arbitrary, inconsistent, and ambiguous.