—| 3 |—

USING TAGS TO MONITOR NUMERICAL LIMITS IN ARMS CONTROL AGREEMENTS

BY STEVEN FETTER AND THOMAS GARWIN

The treaty on intermediate-range nuclear forces (INF) has sanctified the "zero option." It has long been understood that it is easier to verify a complete ban on a weapon system than it is to verify a numerical limit. A complete prohibition is easier to verify because a single sighting of a banned weapon would constitute clear evidence of a violation. Moreover, a complete ban would eliminate training, testing, and repair activities that could serve as a cover for clandestine weapon deployments or could support a sudden breakout from a treaty. Although a total ban may be the best option from the standpoint of verification, this is not realistic for many weapon system.

In the past, numerical limits could be verified adequately because the weapon systems in question—missile silos, bombers, and ballistic-missile submarines—were hard to conceal from national technical means (NTM) of verification (primarily reconnaissance and electronic intelligence satellites). Unfortunately, changes in technology and in the strategic environment are giving rise to new weapons whose deployment will be difficult to verify using current techniques. Mobile land-based ballistic missiles, for example, are gaining increased prominence in the strategic forces of both sides, primarily because they are less vulnerable to preemptive destruction than immobile silo-based missiles. But mobile missiles are much more difficult to count since they are designed to move around the countryside and are often hidden from view. Limits on nuclear cruise missiles would also be difficult to verify using NTM because they are small and because the conventional- and nuclear-armed versions are nearly indistinguishable. In addition, the INF Treaty is giving new impetus to the search for cooperative restrictions on the military confrontation in Central Europe, where numerical limits have been hard to agree on in part because of verification difficulties.

The United States does not have to limit itself to NTM, however. The INF treaty, as well as recent Soviet acceptance of the use of on-site inspection in a variety of arms control settings, indicates a new willingness to accept at least some cooperative and intrusive inspection measures to verify compli-

ance with arms limitations. This chapter examines a promising cooperative way of facilitating the verification of numerical limits on weapons that has received relatively little attention: the tagging of treaty-limited items.[1] Essentially, the use of tags transforms a numerical limit into a ban on untagged items. The result is that many of the verification advantages of the "zero-option" can be retained for a numerical limit. Moreover, tagging systems can verify a numerical limit without yielding simultaneous information on the location of all limited items, thereby reducing the intrusiveness of the monitoring required to achieve a given level of confidence that a limit is being obeyed.

Tagging works by certifying that every weapon observed is one of those permitted under a numerical limit. A tagging system would involve the manufacture of a number of tags equal to the number of weapons limited by treaty. One tag could be affixed to a crucial part of each allowed weapon. If even one untagged weapon were ever seen (by NTM, through on-site inspections, or even by nationals of the inspected party loyal to the treaty regime), then there would be *prima facie* evidence of a treaty violation. Other methods of counting a deployed force can only suggest that the allowed total is being exceeded, an indication that is unlikely to be conclusive and which might tend instead to cast doubt on all the information going into the count. Tagging produces a much stronger impetus for political action in the event of a violation, because observation of an untagged system would provide unambiguous evidence of an overall violation.

Tagging does not function as an independent verification system. Tagging would only be useful as an adjunct to NTM or as part of a fabric of cooperative verification procedures carefully tailored to a specific treaty proposal. Tagging systems have three crucial ingredients: a number of tags equal to the number of allowed weapons, a mechanism for associating a tag with a unique weapon, and a protocol for verifying the authenticity of the tags. In most applications, checking tags would be an aspect of on-site or challenge inspections, but systems are conceivable in which the authenticity of tags would be checked remotely. In some contexts, tagging systems that do not require the affixing of any physical tags may be feasible.

The chapter goes on to explore the potential value of tagging by describing the possible application of tags to five types of deployment limits. It then presents a discussion of various general problems that arise in tagging,

[1]Tagging systems have been discussed previously by Garwin and Fetter in, respectively, "Tagging Systems for Arms Control Verification," Report No. AAC-TR-1040/80 (Marina del Rey, CA: Analytical Assessments Corporation, February 1980) [Sponsored by the Office of Technology Assessment], and "The Use of Tags in Monitoring Limits on Mobile Missiles," UCID-21034 (Livermore, CA: Lawrence Livermore National Laboratory, March 1987).

together with possible solutions, followed by a discussion of how the complex additional burden of designing and negotiating a useful tagging regime might be borne in arms control negotiations. Finally, the question of when the benefits of verification by tags may be likely to outweigh the disadvantages is addressed.

Examples of Tagging Systems

The following examples are intended to show the weaknesses as well as the strengths of the tagging concept.

Soldiers. One possible arms control limitation is on the number of soldiers allowed in certain areas. Limits on the number of troops in Central Europe have been under discussion since the mid-1950s, as have schemes for monitoring such an agreement. Usually a continual presence of inspectors or remote monitoring equipment at checkpoints supplemented by occasional forays by human inspectors has been thought to be required. It is unclear, though, how the observation of an unusually large number of troops in a particular region would be anything more than an occasion for suspicions that could not be easily resolved. Conversely, the intrusiveness required to monitor agreed force dispositions in this manner might yield evidence of local or overall force weaknesses that in a crisis could make the military balance less, rather than more, stable. With a tagging system, however, the discovery of a single soldier without proper identification (i.e., without a tag) would be conclusive evidence of a violation, yet no information need be collected about either the overall number of troops in the region or their disposition.

A tagging system for troops might work in the following manner. Suppose that limitations were imposed on the total number of active military personnel in each of several zones. At random or fixed intervals (say, every six months) the monitoring party would supply enough ID cards (tags) so that the monitored party could issue one to each soldier in the zone. The ID cards would have a section where a thumb print could be registered within two or three days of the issuance of the card. (Chemicals in the card could ensure that after this active period the thumb print would either no longer register or that the card itself would indicate that a longer delay had occurred.) Every soldier in a controlled zone would be required to carry the appropriate ID card with his or her own thumb print. Transfers of soldiers could be accommodated by the exchange of used ID cards for new ones.

With such a system in place, if an inspector ever found a soldier without a valid ID card, there would be a clear violation that could be investigated directly. In most other verification schemes, the total number of soldiers in the zone would be inferred from the number and types of units observed to be

deployed there, or from some other set of imprecise measures that would not identify any specific individual as constituting a breach of the limit, even if they gave some general indication of a violation.

In practice, this tagging scheme would have to be elaborated in great detail. Most obviously, there is the technical design of an ID card that could be personalized by thumb print within the required time period and not provided only to those troops likely to come into contact with inspectors. Because the cards would be provided by the tagging party, and because inspectors could randomly recover a small fraction of the ID cards and return them to the laboratory for detailed analysis, occasional changes in the details of card technology could be used to ensure over time that there were no continuing copying or misuse of the tags.

The example suggests several other aspects of any tagging system. As implied by the mention of inspectors, tagging only works if there is some chance of "observing" the controlled items and the presence or absence of associated tags. In the case of ground troops, we have assumed that inspectors would be given fairly free access to transit routes, if not to all military bases. The personalized quality of the ID card would ensure that no single tag could be used to provide safe transit for a succession of soldiers, who would then disappear into uninspectable bases or other safe havens.

Finally, the example suggests that while tags can help ensure that a precisely defined limit was not exceeded, there are many potential problems of verification and arms control more general for which tags would provide no help at all. If an inspector, for example, came upon an individual in uniform with an automatic weapon but no tag, it might be explained that the person was a police officer or some other quasi-military officer (e.g., a customs agent) and not a soldier at all. In general, soldiers traveling out of uniform and separately from their weapons on civilian transport may not be identifiable as soldiers. Tagging cannot remedy imprecise definitions of what is controlled by an agreement. Only if the parties can agree on a clear definition of who is a "soldier" can numbers of soldiers be controlled.

If a precise definition could be agreed upon, however, in periods of international tension (or up to twice a year at the option of either side), soldiers as defined by the treaty might be required not only to carry tags but also to have their foreheads marked with temporarily indelible ink. This procedure would help ensure that inspectors could identify soldiers and that others not so identified could not contribute substantially to the prosecution of an attack. Over any substantial time period, soldiers could not operate effectively if they could not train, were not formed into units, and if they lacked weapons and communication. Limits on manpower, verified by tagging, accompanied by other sorts of constraints to prevent circumvention of the numerical limitation

could effectively constrain military potential. If these limits were applied in many local sectors, one could build confidence that concentration for a local attack was not under way.

Tanks and Other Conventional Weapons. Since they are an essential element in offensive military potential, tanks are an obvious target for negotiated arms limitation. Compared to limits on people, limits on hardware are in some ways easier and in some ways harder to verify by tagging. Unlike people, certain major classes of military hardware have no civilian use and so cannot merely blend into the civilian landscape. Such specialized hardware includes tanks, artillery, fighter-bombers, most bridging equipment, and most munitions, but not jeeps, trucks, buses, and transport aircraft. Observation of a tank leaves little question that it is a controlled item. For the same reason of singularity, though, close-up scrutiny of a soldier would reveal fewer military secrets than close-up scrutiny of an advanced weapon.

Several other differences make hardware harder to control through tags. First, there is less reason for any particular piece of hardware to emerge from hiding or to be involved in exercises and training. An opponent determined to violate an agreement could maintain a stock of tagged equipment to be used in peacetime operations and an untagged stockpile that would be kept out of view until shortly before the outbreak of hostilities. This problem is conceptually similar to the possibility of unknown stockpiles in an absolute ban on a class of weapons. A possibly decisive difference, though, is that, in the case of a numerical limitation, troops would have the opportunity to train with the legal weapons of the same type.

Second, each hardware item has less of an essential identity than a person. With a thumbprint tag, one can be sure that the monitored party is not using a single tag and "transplantable thumbs" to cover the transit of multiple people across inspected areas. With hardware, some care would have to be taken to design ways to take the equivalent of a fingerprint for each controlled weapon, or to attach absolutely nonremovable tags to crucial pieces of the item. The complexity of the problem is indicated by the fact that a nonremovable tag on the fender of a tank would be of little help because the same fender could be unbolted and used *seriatim* to transfer large numbers of tanks to unknown storage warehouses. If the turret of a tank represented a large part of the value of the tank and the turret could not be easily removed or concealed, however, then a nontransferable tag on the turret would suffice, because a limit on tank turrets would be equivalent to a limit on tanks.

As a technical matter, a nontransferable, noncopyable tag for a tank turret is not hard to devise. One would not require absolute confidence that each tag had not been tampered with, and so one could accept the occasional reliability

problems that attend any electronic components and batteries. The tagging system could use a capacitance, contact, or ultrasound sensor, or two electrically communicating devices on opposite sides of the turret, to ensure that once emplaced it could not removed without providing a tell-tale record. More simply, a limited amount of special epoxy glue made with unstable components and identifying trace elements or isotopes might be provided. Or tags might be emplaced with ordinary glue and an ultrasound fingerprint of the resulting assembly recorded. In the case of an electronic tag, copying could be prevented by cryptographic keys stored in a shielded microchip. Tags that would be recovered occasionally could be made further secure against copying through serial numbers and the recording of random aspects of their physical microstructure, through the use of minute amounts of complex artificial chemicals, or through the use of altered isotopic composition in particular small parts of the tag. A nation attempting to counterfeit such tags could never be sure that the copy duplicated all the identifying characteristics of the tag.

If several classes of tags were provided, or if the tags had serial numbers, then tagging could be used to control the number of tanks in each of several zones of interest, as well as the total in the overall region. The tags for each zone might be different colors and shapes, so that close inspection would not be required to ascertain that a tank was in an allowed area; only a small number of random close-in inspections would be required to verify that the tags were authentic. Such a scheme would be complicated, though, if tanks were rotated among zones and new tags were thus required to be installed.

If details about tank dispositions were not considered sensitive, the monitored party might simply be responsible for turning over to the monitoring party a roster of which tag serial numbers were in each zone prior to the beginning of each inspection period. Even if the dispositions were sensitive, the roster idea could be adapted using cryptographic techniques so that the monitored party could keep the overall roster secret while still providing assurance that any particular observed system was within a sublimit for a particular zone. Cryptographic or electronic means could be used to produce the equivalent of a system where the roster is deposited with a neutral and confidential judge who responds "yes" or "no" to queries of the form, "Is tank number 1197 allowed in zone 11?"

Rail- or Land-Mobile ICBMs. ICBMs are larger and more valuable than tanks, and they probably require more frequent servicing. These may not be the decisive differences where verification is concerned. Nations may be more anxious to keep secret the technical details of their construction, and aerodynamic requirements are such that tags probably could not be permanently attached to missiles. Tagging the canisters in which the missiles are trans-

ported and stored is an obvious alternative, but this would require that the tag provide information sufficient to ensure that a tagged canister could not be used to transfer illegal missiles to covert deployment area. The tagging scheme would have to ensure that canisters were not returned to the factory or repair depots empty or containing a decoy. This could be accomplished by an agreement that missiles would not be removed from canisters except at designated repair depots equipped with appropriate portal monitoring and inspection systems. A seal or an acoustic sensor that monitored standing waves inside the canisters could be used to ensure that the canisters were not opened except at the designated facilities.

Tags on missiles (or missile canisters) could be checked in a variety of ways. In the case of a rail-mobile missile system, it may be the case that such trains would have a distinctive and undisguiseable signature; the length or weight distribution of the trains, for example, could be measured using an unmanned sensor. After identifying such a signature, a tag reader, using a short-range radio or infrared beam, could try to interrogate a tag. Such automatic systems might be installed at choke points in the rail network.

For land-mobile missile systems, the verification protocol might allow occasional free access by inspectors within a random fraction of the specified deployment area. Tags would be checked on any missiles that were found in the area. Such inspections would be relatively effective. Consider, for example, a case in which 100 untagged missiles were illegally placed in a deployment area. If each inspection examined only one percent of the deployment area, and if there were only a 20 percent chance of locating each missile present in the inspection zone, then only four inspections per year would assure an eighty percent chance of discovering the violation within two years, no matter how many missiles were allowed under the agreement.

Alternatively (and perhaps especially outside of agreed deployment zones) the parties could rely on NTM to keep track of controlled systems and their tags. A tag incorporating a navigation system (either radio or inertial) might record its own movements, eliminating the need for real-time access for direct inspection. If the movements of the mobile system were randomized, then knowing some of the past movements of a weapon would not compromise its future survivability. If there were questions about a controlled item observed by NTM on a highway at a certain time, it would be possible, by examining the stored movement record, to prove whether or not a tagged system had been at that location at the time in question. The parties might even be willing to give each other constant information on the location of tagged missiles outside of deployment areas, reducing the risk that the monitoring party would reveal information about its intelligence capabilities in the process of requesting challenge inspections. The characteristics of the controlled weapon

and the detection system would have to be such that a tagged weapon could not serve as a decoy to provide safe passage to one or more untagged weapons kept in close proximity to a tagged systems. Tagging cannot eliminate the possibility of unknown deployments of limited weapons. If inspectors and tag readers were placed at the portals of all known production, test, and repair facilities, however, one could at least guarantee that no untagged weapons would be serviced there, thus forcing a cheater to establish a completely parallel covert maintenance and testing system. The risk of clandestine deployments could be further minimized by limiting the number of people trained to operate the controlled system.

Cruise Missiles. Weapons that are relatively small and easily moved are of course less likely to be observed by national technical means, either in normal operation or when deliberately concealed. Limitations on cruise missiles could be verified with tagging schemes similar to those used for mobile ICBMs, but cooperative measures and more stringent inspections would be essential to increase the likelihood of detecting untagged systems. The key locations to monitor a limit on cruise missiles would probably be repair and maintenance facilities.

The dual nuclear and conventional capability of cruise missiles also poses problems. If there is concern about ostensibly conventionally-armed cruise missiles actually being deployed with nuclear warheads, tags might be modified to include plastic scintillation material and appropriate instrumentation, which would provide evidence of any close-by nuclear material. Of course, even if a tagging scheme were capable of detecting the peacetime deployment of nuclear warheads on missiles declared to be conventionally-armed, it could not prevent replacing conventional warheads with nuclear warheads in a crisis or at the outset of war. One might solve the quick-conversion problem by agreeing to specific technical restrictions on cruise missile design.

Submarine Deployments. Coastal keep-out zones in which missile-launching submarines would not be allowed have been suggested as a way to guarantee increased warning time for command authorities and for alert strategic forces, thereby reducing a possible incentive to strike first during a crisis. Alternatively, safe zones from which attack submarines and other anti-submarine warfare forces would be barred have been suggested to improve the survivability of the missile-launching submarine forces. Although compliance with such agreements in peacetime obviously could not guarantee their continued observance in wartime, it is worth noting that a tagging scheme could allow nations to verify compliance with such agreements even during crises.

Each side would be given a limited number of challenge opportunities each year during which it could ask a specific submarine to demonstrate that

it was outside the prohibited areas. Since submarines cannot travel fast and remain undetected, it would be sufficient for the submarine to surface and make its location known within two days, so long as it surfaced more than perhaps a thousand miles from the keep-out zone. A transmitting tag, which would be carried permanently on-board each submarine but which would be turned on only during such challenges and only after the submarine surfaced, would serve to identify the submarine as the one whose position had been requested. The time delay would reduce the information about patrol patterns that might otherwise be gleaned from these inspections.

General Characteristics of Tags

The idea underlying any tagging scheme is that if all allowed items are tagged, then the detection of a single untagged item would constitute direct evidence of a treaty violation. In principle, tagging makes monitoring numerical limitations as easy as monitoring total prohibitions, because the monitoring party need only verify the ban on untagged items. On the negative side, however, any tagging system itself would introduce a degree of complexity to arms control verification, and the continued existence of allowed production, testing, and operational capabilities may prompt worries about potential evasion of the monitoring system or a sudden break-out from limitations. Still, tags offer considerable potential for improved verification regimes.

Any tagging system should have the following general characteristics:

1. It must be impossible to copy the tag without detection, for otherwise the monitored party could simply produce counterfeit tags to cover weapons deployed in excess of the limit. To make it more difficult for the monitored party to learn how to copy tags, the tags could be replaced at intervals with ones using different anticounterfeiting techniques. As a test before a tagging system was agreed upon, the monitoring party could offer a prize to any citizen who succeeded in defeating the anticounterfeiting scheme.

Tags might be made non-copyable in three generic ways: use of coded electronic signals, use of some natural property of a material for identification, and use of artificial properties that need not be fully disclosed to the tagged party.

Electronic tags have many advantages: the technology is well understood, the cost is likely to be low, the identity of a particular item need not be divulged, and the authenticity of a tag could be determined without direct access to the weapon on which it is emplaced.

If parties to an agreement do not object to tags that would identify individual weapons, then the simplest electronic tag would work as the equivalent of a "one-time pad." Electronic access to the tag's memory would only be allowed following the input of special code unique to the particular tag and to the number of times it had been read previously. Each tag would report its serial number, the number of times it had been inspected, and a

unique secret number for that serial number and index. The secret numbers would be compared with a master list to authenticate the reading. Each secret number would be erased after it was read, and the series of secret numbers would be different for each tag. The monitored party could be informed of, or learn by its own devices, all the information that was transmitted to and from the tag during this process and yet could not use this information to counterfeit tags.

If parties were unwilling to allow the identification of individual tags, then more complicated cryptographic schemes would be required. If the tags cannot indicate their identity, then their input and output must be identical. If tags themselves are identical, then the problem of preventing illegal duplication would be a very difficult one. In either case the tag would have to be protected by various physical means against nonelectronic means of discovering the series of secret numbers; for example, the chip could be shielded and provided with a membrane that would trigger a self-destruct mechanism if violated. In the case of unique tags, each tag need only protect its codes against tampering that does leave any indication of misuse. But in the case of identical tags, one must prevent even destructive means of discovering the secret codes, since a few tags could be sacrificed in a counterfeiting effort. This may be possible; the tag need only destroy its information in response to intrusive examination. Another possible method of allowing the parties to retain the anonymity of particular weapons would be to allow the use of unique tags but to interpose a piece of sealed equipment or a neutral party between the signal from the unique tag and the tagging party. This intermediary would certify that the tag reading was valid but not reveal the detailed basis of this certification.

Tag reading could be done by a direct connection to a local or remote console, or the tag could be queried by a transmitter. In the case of unique tags, especially those in which the tag or tag reader records the geographic position of the tag, the most sensible approach is to allow the monitored party to provide the communications circuit from the monitoring party to the tag.

Tags could also be based on patterns in a certain material or substance; for example, one could take a three-dimensional image of a certain portion of a Fiberglas missile canister using a stereoscopic camera, an acoustic or electron microscope, or acoustic holography. Alternatively, identifying material could be affixed to the weapon being controlled, as with glitter blown into a layer of epoxy on the weapon, or the use of a fiber-optic seal. If the tag were an intrinsic characteristic of the weapon, which would make duplication, spoofing, or swapping very difficult, the tagging would have to be done on-site by the monitoring party. The tag reading would be done with the same type of instrument used for the initial imaging, which would almost certainly require an on-site inspection. The pattern itself could be public knowledge, because the principle of the tag in this case is the nonreproducibility of com-

plex three-dimensional patterns. One would only need to be sure that the pattern came from a particular tag. Although all tags based on patterns would be inherently distinguishable, a tag reader could be devised to convert the identification information into a "yes" or "no" answer.

As noted already, there is great scope for using very subtle features of tags to prevent their duplication if some fraction of the provided tags could be recovered and tested in a laboratory. Such subtle features could include altered isotopic composition of particular parts, the deposit of a monoclonal antigen within a fiber, or seemingly random imperfections in a printing or manufacturing process.

2. It must be impossible to spoof the tagging system, or to fool it into thinking that a valid tag exists where there actually is none. For example, it must be impossible to re-route signals between the tag reader and a counterfeit tag so that the tag reader would actually receive a return signal from a valid tag at another location. Although preventing or detecting such signal displacements would be straightforward if an inspector had direct access to the tag, special precautions would have to be taken if tag reading was accomplished remotely. The general solution is to include coded location and time information in the response elicited from the tag.

3. It must not be possible to move the tag from one weapon to another without the knowledge of the monitoring party. If tag swapping were possible, then valid tags could simply be moved to the weapons being inspected at a particular time and place, or at least to those systems more susceptible to inspection by the other side. If tags were glued onto the tagged weapons, it could be arranged for part of the tag to change color or melt if exposed to the solvent required for the glue employed. An analog is in use in the U.S. domestic economy: to discourage the illegal parts business, automobiles now are made with serial number tags glued to their major sheet metal parts, and owners are warned not to attempt to remove these labels.

4. The tagging system must not aid the monitoring party in locating weapons in real-time, since this could render tagged weapons more vulnerable to preemptive attack. Such position information might even allow terminally-guided munitions to home on the tags during an attack. For example, a radio beacon attached to tanks or mobile missiles would certainly allow them to be counted by satellite receivers, but it could also allow attacking warheads to home on those targets.

5. More generally, the tag should reveal only information that is required for the purposes of verification. In other words, tags should not be agents of espionage that collect sensitive data about the limited weapon or its deployment patterns. Parties might be unwilling, for example, to emplace tags that could reveal low rates of readiness previously unknown to the other side. Concerns about espionage could be alleviated if the physical details of the tags and the tagging system's operation were exhaustively disclosed to the

monitored party, but this would restrict the use of sensitive technologies and may make the tags easier to copy or spoof. On the other hand, the use of open tag technology would make it easier to publicize evidence of treaty violations, since no sensitive sources or methods could be compromised. The monitored party could be assured that the tags are what the monitoring party says they are by providing twice the number of tags, half of which could be selected at random, disassembled, and returned. It would be impossible to verify that there were no secret aspects of the tag (as noted above, some subtle secret aspects would be useful to prevent counterfeiting), but it should be easy to verify the absence of homing devices, chemical explosives, cameras, or other intrusive devices.

In some contexts it may be desirable that tags not uniquely identify particular weapons. The monitored party may be concerned, for example, that valuable information could be gained if the monitoring nation were able to trace the deployment history of individual weapons. Although the easiest way to make tags irreproducible is to give each tag a unique serial number, other approaches could also to prevent counterfeiting.

6. The tagging systems must be extremely reliable and have a very low false-alarm rate. False alarms not only undermine the mutual trust of parties which a treaty otherwise might engender, but, in sufficient number, they could create a background against which cheating would become easier. Designers of tagging systems should give some attention to reducing the possibility that the monitored party could deliberately act to increase the false alarm rate as a prelude to an episode in which illegal weapons would appear in transit or in repair and then concealed.

7. The physical size and power requirements of the tag should be such that the normal functioning of the tagged weapons would not be impaired in any way. Once again, the use of open tag technologies combined with the random inspection of tags should reassure the monitored party that the tag could not somehow harm the weapon.

8. The tag must be reliable in the full range of environments that the weapon might experience during storage, testing, training, repair, and deployment. This may include extremes in temperature, vibration, humidity, radiation, etc., and some degree of deliberate abuse or tampering.

9. The tagging system must not be excessively costly. An acceptable hardware cost might be as much as a few percent of the cost of the limited weapons, especially if operating costs can be kept relatively low. Because a small percentage of the cost of a major weapon system could amount to tens or hundreds of millions of dollars, it seems likely that effective systems can be designed within this constraint.

Verification Systems Using Tags

All verification procedures seek to raise the political risk, increase the technical difficulty, and elevate the economic cost of cheating. No system can eliminate all possibility of cheating, but cheating can at least be made risky, difficult, and expensive. For example, tags could not discover hidden stockpiles of undeclared weapons, but they could make it impossible to mix those weapons with weapons being counted against negotiated limits. Depending on the facilities that would be open to inspection, this would force the monitored party to develop a completely parallel but covert system of production, assembly, storage, testing, training, repair, and deployment its secret stockpile. Not only would the economic cost of such covert stockpiles be much higher than that of allowed weapons, but the risk of being caught—simply by an accident that exposed an undeclared weapon to the light of day—could well outweigh any military advantage that might otherwise have been gained from the undeclared inventory. If, for example, the testing of covertly-produced missiles could be prevented (such testing is easily monitored by NTM), then covert missiles they would become much less valuable to a potential cheater. Large clandestine facilities would probably be required to maintain, test, and store hidden stocks, since it is generally agreed that the size of any undeclared inventory must be a sizable fraction of the allowed inventory before it would be significant militarily.

The following section examines more closely how tagging systems might operate. The discussion is organized according to how the tags would be checked: by on-site inspectors, through remote telemetry, or at natural choke points or artificial portals in the monitored country.

Tags as an Aid to On-Site Inspection

Perhaps the most straightforward way to use tags would be in conjunction with on-site inspection. The use of tags would provide a clear way in which information gained at individual on-site inspections could contribute to an overall judgment concerning compliance with a treaty. Without tags, on-site inspections cannot produce much direct information about the total number of weapons deployed unless all sites are inspected simultaneously. Simultaneous inspections not only would be extremely intrusive, but, for many types of weapons, simultaneous revelation of the location of all weapons would raise the specter of a preemptive strike. In addition, simultaneous inspection would require great numbers of inspectors and host-country guides.

Under more plausible inspection schemes, but without tagging, one might learn that thirty missiles were at site A in January, forty at site B in June, and fifty at site C in December. There would be no inherent way to conclude whether or not the total number of missiles at all sites at any one time exceeded the permissible limit. A periodically declared roster of how many missiles were at each site would reduce this problem, but such a roster would

not give confidence by itself about the completeness of the count at a given site. By contrast, if all allowed missiles were tagged, one could tell if every missile found at whatever facility was part of the allowed inventory. A single missile found anywhere without a valid tag would be *prima facie* evidence of a treaty violation. The first step in instituting a tagging system is to affix tags to the controlled weapons. This could be done during an initial round of on-site inspections, or, if the anti-swapping measures were sufficiently foolproof, one could simplify the process greatly by passing out the allowed number of tags to the monitored party, whose own personnel would affix them. Ideally, tags should be designed so that they could only be affixed within a short time after the monitoring period began, or at least so that when inspected they would give some evidence of how long they had been attached. There should be strong incentives for the monitored party to affix the tags promptly and properly to avoid a reservoir of tags that could be affixed to weapons that happen to be selected for inspection. In significant degree the necessary incentive is inherent in the tagging scheme, because maintaining a reserve of tags would increase the number of untagged weapons and thus the chance that an untagged weapon would be discovered. Note that tags need not be irremovable—they must only indicate in some obvious way that they had been removed.

Careful thought should be given to the particular component (or components) to which the tags would be attached. The component should be an essential part of the weapon system, and it should be difficult to swap this component between systems on short notice. As noted above, the main turret would be a good place to tag a tank, and the barrel might serve for a artillery piece. Many missiles are normally stored in canisters, and most mobile missiles are launched directly from the canister. Although one would naturally prefer to tag the missile itself, this would entail reading the tag through the canister or opening the canister for inspection, either of which might present difficulties. If the canister were tagged but not sealed, allowed missiles could be swapped with undeclared and thus prohibited missiles, thereby providing undeclared missiles access to declared facilities. Sealing the canister would almost certainly require an on-site human presence, however, and would probably complicate missile maintenance. One could develop a fiber-optic mesh that would surround a canister, while still allowing access to small missile components inside for adjustments and repairs, but not allowing separation of the canister and missile. The mesh would be made of a continuous single fiber that could not be cut without interrupting a light beam flowing through it, giving a signal that would be recorded by the tag electronics.[2]

[2] The fiber-optic mesh was suggested to the authors by Richard L. Garwin.

During an on-site inspection, inspectors would locate limited weapons and attempt to verify the authenticity of their tags and to verify that the tags had never been removed. (If tag reading was difficult, as would be likely for pattern-based tags, a random sample of the tags could be checked.) Electronic tags could be equipped with low-power infrared transponders (much like a television's remote control), thereby allowing the tags to be queried from a few tens of meters away. Such tags are already in use in commercial assembly lines for inventory control. This would reduce the intrusiveness of on-site inspections and yet not provide a homing capability that would make the tagged weapon vulnerable to attack. An extension of this idea would be to let robots inspect the tags, or to fly a pilotless airplane over the site to query tags.

Procedures would have to be worked out for the return of a tag when a controlled weapon was destroyed or otherwise removed from the inventory. To prevent testing of undeclared missiles produced at covert facilities, one would need to verify that the missile being tested had been tagged and thus had been taken from the allowed stockpile. Tags would alleviate the need for detailed monitoring of other methods of destruction.

If the verification regime permitted inspections on short-notice at the option of the monitoring party, they could be timed to take maximum advantage of national intelligence capabilities. The movement of controlled weapons into or out of the facility to be inspected could be monitored closely by NTM or by special cooperative measures just prior to the event. Ideally, the facility would be closed or put into a stand-down condition until the completion of the inspection. If inspections could be conducted on short notice, the movement of illegal weapons out of declared facilities might be detected. Even if an untagged missile were never actually found during an on-site inspection, tagging could force a cheater into more obviously suspicious behavior. Moreover, because untagged weapons would have to receive special handling at all times, tags might greatly increase the number of people who knew of a treaty violation on the part of their country, increasing the likelihood that the violation would become widely known.

The use of on-site checking of tags in providing evidence of cheating—indeed, the use of any type of on-site inspection for this purpose—should not be oversold, because access to the evidence would always be in the control of the monitored party. Although it is true that the detection of a single untagged missile would be evidence of a violation, the monitored party would be unlikely to allow an on-site inspection when such a possibility existed. It would always be advantageous from the cheater's perspective to make up excuses for delaying or denying an on-site inspection rather than risk discovery of a "smoking gun." This may lead to a paradox of sorts, because if a tagging system were implemented, the lack of a tag could become, in the eyes of the world community, the *only* acceptable evidence of a violation.

Thus, even though tags could provide unambiguous evidence of a violation with just a single observation, it is unlikely that this would ever happen during an on-site inspection. The monitoring party probably would have to act on more ambiguous evidence, such as a refusal or delay of on-site inspections, surreptitious movement of missiles out of declared facilities, tag tampering, or other suspicious behavior. Tagging would have played a role, however, in eliciting this suspicious behavior. Moreover, because of tagging's relative efficiency in detecting violations, tags should reduce the likelihood that a country would decide to cheat in the first place (which is presumably the main purpose of verification).

Tags read on-site could be an excellent way to help build confidence between parties who are in compliance with an agreement. Because tags make inspections more effective, they would have the virtue of minimizing the number of inspections required for a given level of confidence. Tags also could reduce the chance that false claims of treaty violation would be used for political reasons.

Monitoring Tags Remotely

In general, verification regimes are likely to be easier to negotiate if requirements for on-site inspections, especially those involving trained foreign personnel at sensitive military locations, are minimized. If tags could be read remotely, routine on-site inspections would not be needed to verify limits on even small, concealable weapons. Three basic schemes using remote reading come to mind: the tag could transmit a continuous or intermittent signal, the tag could be provided with a two-way communication link, or the tag could record position information for later interrogation.

The most obvious remote sensing method is for every tag to transmit a coded set of high-frequency radio pulses. The location of the tag could then be determined by satellite receivers using time-of-arrival measurements. If other arrangements are made for tracking tags outside of deployment areas, the power requirements for the tag beacons could be kept low by installing a set of time-of-arrival receivers and a satellite earth station in each deployment area. The obvious drawback of this scheme is that one might be able to home on the beacons during an attack. The monitored party might be given the ability to switch off the transmitters in time of crisis to ease this problem, but this would not eliminate the possibility of a surprise attack. In addition, such a system might aggravate a crisis, since switching off the beacons could be taken to indicate that the monitored party were preparing for war. Even worse, there could be pressures to launch an attack while the beacons were still on, or shortly after they were switched off, when the approximate location of the tagged weapons would still be known. The very necessity of making such decisions would distract leaders from dealing with more substantial issues.

A better plan would be to have the beacons emit signals randomly and infrequently in time, so one would never know the location of a large fraction of the tagged weapons at any one time. An inventory of weapons, for example, could be equipped with beacons that emitted a signal once every ten days. If the weapons were moved once per day, then the monitoring party would only know the location of ten percent of the inventory at any one time.

In another remote-monitoring scheme, each tag would contain a receiver that recorded position information given by a navigation system. This system has the advantage that the quality of the location information could be controlled. If, for example, the resolution of the navigation system is too great, then the system's output could be filtered to report only the number of a map square in which the tag could be found. After a period of time, the degraded information stored in the tags could be transmitted to the monitoring party. This transmission could be encrypted and security codes added to ensure the authenticity of the data. If the time delay were short (a few days), this idea would be similar operationally to the beacon scheme. Alternatively, the tags could be collected and sent back to the monitoring party and new tags issued. The tags themselves would then constitute a time-lagged data base of the position of every allowed missile. Tags of this type could be used to enforce regional limitations on weapons, such as the number of tanks near the central front in Europe.

Of course, neither of these tagging systems could detect undeclared weapons. The presence or absence of undeclared weapons would be verified by comparing the location information supplied by the tags to NTM data. For example, a satellite photograph that showed a controlled weapon at a location that was not recorded by any of the tags at that time would be evidence of a treaty violation. The advantage of this method is that it would provide reliable data on the variable of interest: the number of allowed weapons. The cost would probably be low, and data-handling requirements for this system would not excessive.

These systems do not resolve all problems, however, and they create some of their own. First, they rely on NTM to detect violations. Because a cheater would be very careful not to expose undeclared weapons to reconnaissance satellites, the probability of observing a violation would be small. One would probably have to depend on accidents (e.g., the crash of a train carrying covert missiles) to expose or deter cheating. Second, the system would place high demands on technology. It may not be possible to build the type of tag described here—the receiver or beacon may simply be too large or require too much power. One may have to develop a new receiver, and perhaps a new navigation system, which would increase costs greatly. It also may not be possible to develop tags that are sufficiently reliable. If a photograph shows the location of a controlled missile but the tag records the position information inaccurately, then a false indication of a treaty violation would

occur. Error-checking and validation protocols may be able to reduce the false-alarm rate to negligible levels, but this would have to be demonstrated. Third, the monitored party could not program the movements of tagged weapons on fixed schedules because the monitoring party would quickly learn these patterns and be able to predict the location of, and therefore target, the weapons in the future. This is a minimal concern Prudent planning already requires that deployment patterns be random, with or without tags, because mobile missiles depend for their survivability on the opponent not being able to predict where they will be at any given moment.

Monitoring Tags at Choke Points

Tags also could be used effectively at natural or artificial "choke points," or places through which all or most of the declared weapons must pass at least occasionally. As an example of a natural choke point, consider a limit on rail-mobile missiles such as the Soviet SS-24 system. It is likely that a number of missiles would be deployed on the same track, or at least that several missiles would have to pass a certain point on the track to exchange positions (the position of choke points would depend on the topology of the rail network). If choke points could be identified, tag readers could be installed at these points, along with sensors to detect untagged weapons. Imagine, for example, that a missile were approaching a choke point equipped with sensors. If the missile had a valid tag, the sensors could read the tag (perhaps using the infrared transponder mentioned earlier). If an undeclared missile tried to pass through the choke point, however, other sensors, such as scales or x-ray machines, would determine that the object could be a missile. The monitored party would then be required under the verification regime to allow more intrusive inspection to prove that the object was not a limited weapon (e.g., video cameras could be used to look inside the railroad car). A refusal to allow such an inspection would cast serious doubt on treaty compliance, although it would not constitute direct evidence of a violation.

Another example of a natural choke point can be found in the deployment of nuclear-armed cruise missiles on submarines. Because the portals for bringing cruise missiles on board submarines are likely to be limited, one could deploy sensors that would detect the presence of fissile material at each portal. Every time the sensors detected fissile material, they would also expect to read a valid tag. This scheme is clearly not foolproof, but it might be better than allowing the number of submarine-based cruise missiles to remain unrestricted. This scheme is unlikely to work with surface ships, since there are too many ways to bring missiles (and heavily shielded warheads) on board. (Given the possibility of underway replenishment of submarines, the scheme may be unworkable for them as well.)

If a natural choke point could not be found, one could be created by surrounding declared facilities with monitored fences that force the movement of

mobile missiles or critical components through a gate where they could be observed and counted. The declared facilities could be any combination of production, assembly, storage, testing, training, repair, and deployment areas. The fence, or perimeter, would be a two-dimensional barrier around the monitored party's facilities that could not be violated without detection. A wide variety of fence sensors could be used, including seismic detectors, microwave intrusion detectors, acoustic sensors, video and infrared cameras, metal detectors, short-range radars, or pressure sensors. Possible monitoring devices at the gate, or portal, might be video or infrared cameras, weighing scales, x-ray, gamma-ray, neutron, or ultra-sound imaging devices, metal detectors, and human inspectors. The perimeter/portal data could be transmitted to the monitoring party in a secure mode or interpreted by human inspectors stationed at the site.

Consider the case of a perimeter/portal system at an assembly plant. If a limited weapon had not yet been produced, this would be the ideal point to verify limits on the weapon so long as it could not easily be assembled without detection at other unidentified or undeclared facilities. When a finished weapon was ready to leave the assembly plant, the monitored party could simply declare the weapon and the count of deployed systems would be increased. If the monitored party did not declare the weapon, monitoring devices at the portal would determine that the object *could* be a limited weapon. Unless further inspection was permitted to determine that the object were *not* a limited weapon, the monitored party would be in violation of the treaty when the weapon left the facility.

This system would have the advantage that declared weapons would not be inspected by intrusive devices at the portal. But to retain this advantage, declared weapons would have to be tagged before leaving the facility so that they could be returned for maintenance. Without tags, the monitoring party would have to inspect any returned weapons to ensure that the monitored party was not returning bogus weapons and replacing them with real weapons. Tags also would prevent covertly-produced weapons from having access to declared production and assembly plants.

It is much more likely, however, that a substantial number of weapons would already have been deployed before limits could be placed upon them, in which case a method to establish the initial inventory would be needed. On-site inspections at declared facilities could help establish the initial inventory, or perimeter/portal systems could be constructed at these facilities. In the latter case, all existing allowed weapons would be tagged. The tag would be queried at the portals of testing, storage, training, repair, or deployment facilities, and only weapons with valid tags could enter the facility. As before, sensors at the portal would detect any undeclared object that could be a limited weapon; such objects would be subject to further inspection, or be denied passage within the terms of the treaty. If desired, weapons could be moni-

tored even while in transit between declared facilities by installing tag readers along commonly-traveled routes or by attaching a tag containing a navigation receiver or inertial-guidance package to the weapon.

In the absence of tagging, deployment areas present a serious problem for perimeter/portal systems for most weapon systems: the perimeter would have to be very large and therefore expensive to instrument. For example, if there were ten deployment areas of 100 mobile missiles each, and the missiles and launch vehicles were hardened to an over-pressure of five pounds per square inch, the total perimeter length would be at least 2,000 kilometers. Instrumented fencing may cost a million dollars per kilometer to build and install, with the entire perimeter system requiring the expenditure of billions of dollars. In addition, many of the sensors considered for the fence, especially seismic detectors, radars, and video and infrared cameras, are unlikely to be allowed unless the monitored party could be absolutely sure that the information collected could not be used for targeting. In such deployment areas, remotely-read tagging systems (or those requiring occasional access by tag-checkers) could make a huge difference in the cost and reliability of count of controlled weapons.

There are several disadvantages to perimeter/portal systems, especially when they are applied to a wide variety of declared facilities. First, both sides may be reluctant to allow the other to construct a perimeter composed of a wide variety of sensors around some of their most sensitive military areas and allow intrusive inspections of any entering or exiting objects that the monitoring party claimed could be a limited weapon. The potential for gathering intelligence information that was not required for verification purposes would be obvious. Second, the perimeter/portal systems would be expensive—even more so if supplemented by a human presence. Third, such a system would necessarily be very complex, requiring perhaps hundreds of agreed rules governing the interpretation of data. Finally, perimeter/portal systems probably would disturb the normal functioning of declared facilities. However, tagging provides a natural complement to perimeter/portal systems, allowing reduced intrusiveness within the controlled facilities.

Tagging and the Negotiation Process

Any tagging system must be carefully designed to fit both the characteristics of the weapons being controlled and the degree to which the parties are willing to divulge certain types of information (such as past position information). Because some aspects of tagging are likely to be technically complex, tagging could introduce a further element of difficulty into arms control negotiations. This technique, which is intended to increase confidence in treaty compliance, could have the opposite effect if the hardware and protocols were not devised with great care. The very act of introducing the possibility of tagging into a negotiation could delay agreement. Substantial

research and development on tagging, together with focused technical discussions among the potential parties to an agreement, may be necessary in advance of any attempt to include tagging in the negotiations aimed at a specific limitation.

General Secretary Mikhail Gorbachev has suggested that a special Soviet-American committee of scientists could put forward their views on verification to the leadership of the United States and of the Soviet Union. Although setting up such a committee could be an important step, a high degree of confidence in a proposed tagging scheme might be attained only if the prototype hardware were developed and subjected to severe testing substantially in advance of an agreement. Such activities are clearly within the charter of the U.S. Arms Control and Disarmament Administration. A relatively small amount of money, on the order of $10 million, would be required for such a technology demonstration program.

This paper has focused on tagging systems for bilateral U.S.-USSR or NATO-Warsaw Pact agreements, it also would be possible to adapt tagging to truly multilateral agreements. While various aspects of the tagging protocol and of methods for ensuring noncopying of tags would be more complex, preliminary investigation suggests that the difficulties would not be insuperable.

Conclusions

If negotiated limits on relatively small, easily-concealed weapons such as mobile or cruise missiles are important, the problem of verification will have to be solved before agreements can be completed. In general, there are three ways to go about this: ban the weapons altogether, accept a lower standard of verification than for large, fixed systems, or develop new monitoring techniques to provide adequate verification.

The first solution may be unacceptable when the weapons in question are considered to make a positive overall contribution to national security and international stability, as in the case of mobile missiles, or when dual-capable systems are already deployed, as in the case of cruise missiles. The second solution is also widely regarded as unacceptable. Many U.S. politicians are predisposed to believe that the Soviet Union will cheat on agreements whenever possible, and it is unlikely that an important treaty could withstand these suspicions unless a convincing case could be made that Soviet compliance would be verified and violations detected.

Tags could be part of the third solution. Although dozens of ideas for tags already exist, it is probably not wise at this point to spend too much time or money developing and testing tag hardware. Tags could be designed that meet all of the generic requirements outlined above: resistance to counterfeiting, spoofing, swapping, espionage, homing, etc. Instead, more work is needed to explore the feasibility of tagging concepts and to define the overall

verification system of which tags could be a part, because the tag technology needed will depend much more on the verification regime as a whole than on any general requirements that tags must meet. Once a promising verification system is defined that requires a certain type of tag, then the development of specific tagging hardware could go forward productively.

Three generic tagging concepts have been considered in this chapter: tags read during normal on-site inspections, tags that give location information remotely, and tags read at natural or artificial choke points. Each system would require a different type of tag, ranging from microchip tags with infrared transponders to navigation receivers and fissile-material detectors. Using tags as a supplement to on-site inspection may be the simplest system to implement because it places low demands on technology. Tags make on-site inspections more efficient and effective, and may also make them more acceptable by replacing humans with sensors of limited and known capacities, thereby decreasing the potential for espionage. Remote reading of tags further decreases the necessity for an on-site human presence, but places higher demands on technology and may be less effective because of its reliance on NTM to detect undeclared weapons. Using tag readers at choke points is an attractive idea, but it is often difficult to find natural choke points and constructing artificial choke points could be very intrusive and expensive. The power of the tagging concept is such that permanent choke points and perimeter/portal systems may be obviated.

Tags are a technical fix that will only aid the negotiating process to the degree that those technical difficulties with verification that tags could ameliorate are delaying the completion of treaties. Even if tags could make numerical limits on certain weapons easier to verify, there may be other barriers to agreement. To the degree that this is the case, instead of being part of the solution tags could become part of the problem—a source of endless detailed technical discussion that could be used to obfuscate more fundamental differences. An agreement incorporating tags would undoubtedly be far more detailed and more difficult to negotiate than one without tags. Although the United States and the Soviet Union have shown an ability to negotiate technically complex treaties—SALT II, the INF treaty, and the agreement limiting peaceful nuclear explosions, for example—such complications should only be introduced when an agreement would be impossible without them.

In summary, while tags are not a panacea for the problems of monitoring numerical limits on concealable weapons, they could have much to offer if part of a carefully-designed system. To be truly available for inclusion in a future treaty, tagging systems will have to be the subject of detailed previous discussion among the parties, including parallel technical research and development on both sides.