Defense Analysis Vol. 5, No. 3, pp. 260–262, 1989
Printed in Great Britain.

0743–0175/89 $3.00 + 0.00
Brassey's Defence Publishers Ltd.

"Inscrutable" Badges for Verifying a Mobile Missile Quota

NIMROD MEGIDDO*
School of Mathematical Sciences, Tel Aviv University, Tel Aviv, Israel

and

BARRY O'NEILL*
Northwestern University, Evanston, IL 60201, USA

An unusual verification problem may arise if the US and USSR negotiate a reduction of strategic missiles. If, as seems likely, the US comes to accept a quota on mobile missiles, the verification system will probably involve a badge attached to each missile to prove it is legitimate.[1] The US may want badges that cannot be forged for attachment to illegitimate missiles, yet do not reveal a missile's movement pattern should the same one be examined several times.

A typical verification plan for a mobile missile quota involves the inspecting country attaching a badge to each of the inspectee's allowed missiles, which are then sent to the agreed deployment area. This area is divided into sectors and at each scheduled inspection time the other government chooses one sector, the inspectee reveals the locations of all missiles in the chosen sector(s), and an inspector checks that each has a valid badge. If a missile is badgeless or if an undeclared missile is spotted inside the sector (by satellite or other intelligence means), or if a missile is noticed outside the deployment area, the inspector can declare a violation.

Since the inspecting government knows the location of only a fraction of the force at any time, the whole would never be vulnerable to attack. An evader might respond to the announcement of a target sector by trying to shift illegal missiles out of that area, but to block that move, the sectors are chosen sufficiently far apart. There is no requirement that the owner assign equal numbers of missiles to each sector. They can be shifted back and forth, but all must be inside a sector at an inspection time.

Pentagon analysts were averse to any system that tells Soviet inspectors about the missiles' pattern of movement. They insisted that if one is by chance chosen twice in a row it should not be recognizable as the same. Randomizing the

*Nimrod Megiddo is a Research Staff Member at the IBM Almaden Research Center, San Jose, and Professor at the School of Mathematical Sciences, Tel Aviv University, Israel. Barry O'Neill is Associate Professor of Industrial Engineering at Northwestern University, and contributed to this paper while a Visiting Scholar at the Center for International Studies, Massachusetts Institute of Technology. The authors would like to thank Steve Fetter for calling their attention to this problem.

movements is seen as organizationally infeasible. In the standard system identifying badges would function like fingerprints, carrying so much detail that the inspectee could not duplicate them without the inspector noticing. How could such a badge by made "inscrutable?" That is, how could it be designed to avoid revealing movement patterns? The inspector would have to examine it thoroughly enough to spot a forgery and yet not so closely to recognize it as identical to a past observation. This is a dilemma for a badge system.

At first thought one might limit the inspector's access, to allow only feeding an electronic password into the badge, whose internal programming would then respond with a signal identical for all missiles. Such a system would be vulnerable, however, in that the inspectee would possess the badge between inspections and could disassemble it to learn its software. One might propose adding a mechanism that erases the program if someone tries to break in, or a scheme to detect tampering, such as Richard Garwin's clever suggestion in another context of surrounding a badge with a fine net of material through which is woven a long optic fibre, making it impossible to enter without breaking the flow of light. However, these methods are complex and aggravate the problem of false alarms. Furthermore, the badges must be designed to allow the inspectee thorough access to their inner workings since the inspectee must feel assured that the inspector has not programmed individual badges to identify themselves in some way.

To be politically acceptable, the method should be transparently simple. We propose the following, which we call the Sequential Random Display System. For definiteness assume the treaty allows 100 missiles in a total of 10 sectors, divided among the sectors however the inspectee wishes. It provides for monthly inspections for a duration of 20 years, 240 inspections in all.

For the Sequential Random Display System the inspector manufactures 100 badges, each comprising a clock, a simple memory and a digital display. The inspectee devises 100 strings of numbers for them, each including 240 integers in the range 1–100. The strings are also given a further property described below. The badges are affixed to missiles in a way that removing them would destroy them, and the strings of numbers are fed in, one string to a badge. Thus at the start of the treaty any badge contains its entire 20-year list of monthly numbers. The badges automatically change their displayed numbers each month. The strings were also constructed with the feature that in any month every missile is displaying a different number. That is, the set of first numbers of the strings is a random permutation of the numbers 1–100, as is the set of second numbers, third numbers, etc. Month by month one badge might display 29, 78, 15 on to 240 numbers and another might show 15, 36, 52, . . . and so on.

For inscrutability the inspector should not be able to infer past numbers from the present one. Therefore they should be generated nonalgorithmically, perhaps by the traditional method of gamma rays arriving at a detector. If the inspectee has built extra missiles with forged badges, two missiles somewhere will be displaying the same number. At a scheduled inspection the inspector selects two sectors, learns from the inspectee where the missiles are, and makes sure that all displays are different. Inspecting two sectors at a time is necessary since an evader could thwart a single-sector inspection by keeping missiles with duplicate badges in separate sectors.

With the Sequential Random Display System cheating will surface in an uncertain but reasonably short time. For example if the violator has built 10 extra missiles and divided the force evenly, 11 per sector, with all illegal missiles in one sector and all missiles whose numbers they duplicate in another, then detection occurs when those two sectors are

chosen, an event whose likelihood is 1/45, so that within 1 year the chance of detection would be 24%, within 2 years 42%, following the formula $1 - (44/45)^{12t}$. These probabilities would seem adequate to deter a violation of such little value. Inspecting three sectors at a time would boost the probabilities further: within 1 year 56% and within 2 years 81%, according to the formula $1 - (14/15)^{12t}$. If more than 10 illegal missiles were built, the evasion could still be exposed only by choosing the right two sectors, but probabilities would be higher if the inspector selected sectors using other intelligence about where contraband missiles might be. The inspector might, for example, use the strategy of choosing a sector with higher probability if more missiles were noticed there.

Another evasion tactic would be to give each illegal missile a fake badge that accepts instructions from the outside. When the inspector announces a choice of two sectors the inspectee immediately changes the visual displays so that all badges read differently. This could be thwarted by removing a badge for close inspection from time to time. Evidence of a violation would be tangible and thereby carry greater deterrent power, so removing a badge could be used seldom enough that no significant information would be gained about missile movements.

Research on verification has generated much literature analyzing the statistical properties of different schemes.[2] It has considered the informational properties of systems constrained by cost or size, rather than by the need to protect a specific type of information. Until recently verification has been simply a tug-of-war, the US demanding more and the USSR resisting. Now the two parties acknowledge more realistically that they have interests on both sides. The question becomes how to design verification that gives the information it should give and withholds information it should withhold. This may be a productive area of study.

NOTES

1. S. Fetter and T. Garwin, Using tags to monitor numerical limits on weapons in arms control agreements. Mimeo, Johns Hopkins University Foreign Policy Institute (1988).
2. B. O'Neill, *Why a Better Verification System May Give More Ambiguous Evidence.* Center for International Studies, Massachusetts Institute of Technology (1988).