

cerning the sampling of a chemical warfare agent in the process of being destroyed, using the argument that subsequent chemical analysis of the samples might reveal sensitive information about the nature of the substance. While cognitive intrusion usually implies some physical intrusion, it is possible to conceive of a system where no physical access is needed to acquire sensitive information. The obvious examples are satellites and other long-range sensing devices.

Thus, the distinction between physical and cognitive intrusiveness has some meaning. It is also reflected in the objections raised by some states. For example, many verification proposals have been challenged on the grounds that national sovereignty is violated (i.e. physical intrusion) and that the system amounts to legitimized espionage (i.e. cognitive intrusion); presumably the latter was meant to be neutralized by the "screening of aircraft windows".

The issue of intrusion remains a sensitive problem as confidentiality appears to stay almost an obsession with a number of states in regard to their "national security" affairs. Consequently, objections over intrusion are likely to continue to arise to some extent for some states. In addition to the military aspects, fears about industrial espionage on the part of both governments and commercial enterprises will remain a consideration. As well, political objections might be raised to the question of granting major verification responsibilities to an international body. A rational analysis of modern international verification techniques suggests, however, that the significance of "intrusiveness" should steadily decrease with time.

Table 2. Percent of proposed verification methods by degree of intrusiveness

