Abstract

The Iraqi crisis of the early 1990s focused IAEA attention on the need to identify undeclared nuclear activities. The 93+2 program and many related initiatives sought to develop processes that would increase the chances of identifying undeclared nuclear sites. Most efforts and proposals to accomplish this goal focus on obtaining increased information from IAEA inspections and from member states' intelligence communities. This article will explore the advantages and disadvantages of developing a "fire alarm" system for gathering information on undeclared facilities to complement the existing "police patrol" system. It also argues that benefits may accrue from allowing a broader range of nonstate actors to contribute to the IAEA's system for identifying undeclared sites. Independent analytic organizations, nongovernmental advocacy groups, corporations in the nuclear field, nuclear scientists, and other individuals could all contribute information that would help the IAEA in identifying undeclared sites sooner than they would otherwise and, perhaps, at lower cost. Such information would also run the risks of exacerbating informational "overload" at the IAEA, and would raise questions of informational credibility. This article makes an initial inquiry into what contribution, if any, nongovernmental sources could make to the IAEA's system for identifying undeclared activities, examining the opportunities, risks, and concerns raised by such a change.

1. Introduction

The Iraqi crisis of the early 1990s focused IAEA attention on the need to identify undeclared nuclear activities. The 93+2 program and many related initiatives sought to develop processes that would increase the chances of identifying undeclared nuclear sites. Most efforts and proposals to accomplish this goal focus on obtaining increased information from IAEA inspections and from member states' intelligence communities. This article explores the advantages and disadvantages of allowing a broader range of actors to contribute to the IAEA's system for identifying undeclared sites. Independent analytic organizations, non-governmental advocacy groups, corporations in the nuclear field, nuclear scientists, and individual citizens may all be able to contribute information that would help the IAEA in identifying undeclared sites sooner than they would otherwise and, perhaps, at lower cost. Such information also runs the risk of exacerbating informational "overload" at the IAEA, and would raise questions of informational credibility. This article makes an initial inquiry into what contribution, if any, nongovernmental sources could make to the IAEA's system for identifying undeclared activities, examining the opportunities, risks, and concerns raised by such a change.

This article argues that IAEA may be able to enhance its ability to identify undeclared nuclear activities by developing a system to facilitate and encourage reporting by nongovernmental actors on suspect activities. Supplementing (but not replacing) the present "police patrol" system of inspections with a system that allows nongovernmental actors to provide "fire alarms" will increase the likelihood that a clandestine nuclear program will be detected, will increase the costs of keeping such a program clandestine, and hence will decrease the incentives for a state to undertake such a program. Although the ability of such an approach to achieve these goals depends on several conditions being met, those conditions seem likely to be met, based both on the logic of the nuclear context and experience in other contexts. Whether such a program would be worthwhile, however, depends on an assessment of the costs, risks, and other disadvantages of such a program, and the feasibility of efforts to eliminate or mitigate those problems.

The argument here builds on two insights from political science. The first insight is that detecting violations of mandated rules can often be accomplished better through an ad hoc, decentralized, passive, and indirect system that relies on "fire alarms" than through a systematic,
centralized, active, and direct that relies on surveillance of a sample of potential violation sites by “police patrols” /14/. The second insight is that nongovernmental actors have shown themselves capable and willing to assist international regimes in many other issue areas by accurately and honestly monitoring and reporting violations. Although we need to be cautious before generalizing insights developed in one domain to another domain, the initial critical examination which follows suggests that these insights may well be applicable to the IAEA’s efforts to deter nuclear proliferation. IAEA’s safeguards system has often served as a model for other arms control arenas /2, 17, 19, 30, 33/. Here I ask what lessons for involving nonstate actors in the effort to identify undeclared nuclear facilities can be drawn from similar experience in other international arenas, such as human rights, humanitarian assistance, and environmental protection.

2. The problem

IAEA’s future success is going to depend on its ability to accomplish two tasks: a) establish a new verification system that, if properly implemented, would increase its ability to detect undeclared nuclear activities and b) increase the resources available to properly implement that system. Prior to the Iraq crisis, verification of material accountancy constituted the “fundamental basis” for the IAEA’s verification system. That crisis pointed major reevaluations of the most likely paths by which states would attempt to acquire nuclear weapons and the best ways to respond to and deter such attempts. Those reassessments produced “93+2” and other procedures that embodied an enhanced concern with and procedures for identifying and deterring undeclared nuclear activities, rather than simply diversion of nuclear material from declared facilities /10:19/.

The failure to detect Iraq’s nuclear program highlighted both inherent problems in the IAEA’s traditional approach to safeguards and more practical problems of having resources adequate to the task it faced. The IAEA safeguard program’s focus on inspections for material diversion and material accountancy involved an implicit assumption that states would be likely to pursue a nuclear weapons capability by diverting nuclear material from a safeguarded site /4:63/. “The IAEA was provided with . . . no clearly stated mechanism or tools to ensure” detection of undeclared nuclear activities /24:137/. Such a program structure reflected assumptions, however wrong, about the technical and financial obstacles of successfully undertaking a secret effort to develop nuclear materials. It also reflected most states’ political unwillingness to accept the more intrusive and unannounced inspections of a much wider range of facilities and activities that would have been required to reliably identify pursuit of nuclear weapons by other possible pathways. The Iraqi experience demonstrated the faultiness of the assumption and reduced (though it has not eliminated) most states’ resistance to more intrusive measures. Indeed, although the IAEA previously had no rights to gather information about facilities and activities not included within a given state’s safeguard agreement, such rights remain limited even under the “93+2” program.

The crisis also highlighted the resource constraints on IAEA’s inspection resources. Most of IAEA’s meager inspection resources were used in very few states that were not at the top of the list of likely proliferators /4:66, 24:139/. The resource problem has become exacerbated in the wake of the Iraq crisis by increasing demands for IAEA to detect nuclear activities and to do so more cost-effectively coupled with a decreasing availability of such resources, at least in real terms /4:66/. Even in the absence of such resource constraints, efforts to detect undeclared activities pose different and more difficult problems than efforts to detect diversion of material from declared facilities. The latter problem is simply far more limited in scope than the former. Detecting diversion from declared facilities involves finite inspection demands, even if those demands exceed IAEA’s inspection resources. Detecting undeclared nuclear activities faces the IAEA with the quite different problem of needing to be “everywhere all the time.”

In short, the IAEA faces a future in which states expect it to meet a broader range of more challenging demands with the same or fewer resources. Succeeding in that environment has already prompted considerable innovation and re-invention within the IAEA safeguards community. To date, however, most improvements to the safeguards system have revolved around improved detection procedures at declared and suspect facilities. This raises the question of how do suspect sites get identified so those improved procedures can be brought to bear. Efforts to redress this problem have tended to focus either on improved rights to access in the suspect state or on the government intelligence services of
other states. The sovereignty and security concerns of states raise obstacles, although arguably not insurmountable ones, to both approaches to the problem. Governments remain reluctant to relinquish to IAEA either the sovereignty or resources necessary to detect and deter undeclared facilities, and IAEA "can only do so much by itself" /11:74/. This raises the question of whether the IAEA could develop a system that would engage nongovernmental actors in identifying sites suspected of undeclared nuclear activities, thereby improving the ability to detect and deter such sites without placing large additional demands on the already-strapped resources of the IAEA or the sometimes-reluctant good will of its member states.

3. Two models of detecting violations: police patrols & fire alarms

The quite different characters of the undeclared activities that have become of most concern and the diversion that traditional accountancy and inspection approaches could detect has prompted considerable interest in alternative approaches to nonproliferation. Traditional techniques simply seem less appropriate to the new challenge. A particularly useful alternative is posed by McCubbins and Schwartz's contrast of two models of American legislative oversight. They argue that the US Congress conducts most of its executive branch oversight through reliance on "fire alarms" rather than "police patrols" /14/. Police patrols entail centralized, active, and direct efforts by Congressional staff to detect and discourage violations by executive branch agencies; fire alarms entail less centralized, less active, and less direct efforts to encourage individual citizens and interest groups to monitor and report violations by executive branch agencies. A police patrol system often proves both costly yet not particularly effective because a) it can examine only a small sample of the behavior of concern, b) it expends most of its resources examining behaviors that do not violate any rules, and c) it centralizes the cost burden for the system on the agency undertaking the police patrols /14:168/. In contrast, a fire alarm system can prove cheaper and more effective by assuming that actors who would be harmed by rule violations have incentives to monitor for and report such violations so long as they are given non-burdensome opportunities to do so. Although Congress has the choice to either "patrol for violations . . . or else wait for alarms to signal potential violations," it demonstrates "a preference - an eminently rational one - for fire-alarm oversight" /14:167 & 176/.

The traditional IAEA safeguards system corresponds relatively closely to McCubbins and Schwartz's police patrol model. IAEA inspections monitor only a fraction of declared sites only a fraction of the time, those inspections have rarely uncovered rule violations, and they use up a considerable share of the total IAEA budget. Of course, the nature of the process of diversion of nuclear material does not seem particularly susceptible to a "fire alarm" approach since those involved in and supportive of the diversion have strong incentives to ensure that no other actors are aware that the diversion is occurring. However, the Iraq crisis has made states more interested in detecting undeclared activities, a task more susceptible to a fire alarm type system. Much discussion has already occurred regarding a system by which member states' intelligence could be used to identify suspect locations or activities and thereby prompt further investigation by the IAEA. Although such proposals raise significant security and political concerns that have slowed their acceptance within IAEA, they represent a quite different, and potentially more effective, approach to detecting violations than that of traditional IAEA inspections.

Establishing new fire alarm techniques to complement the existing "police patrols" of safeguards may offer the possibility of improving detection of clandestine efforts to develop nuclear weapons. For the IAEA, a fire alarm system requires developing procedures that would encourage any actor who came across information or evidence that suggested clandestine nuclear activities to provide that information to the IAEA. The success of such a system would depend on ensuring that at least some actors have the incentives and capacities necessary to observe and report noncompliant or suspect behavior. In the nuclear weapons context, it will also require extensive organizational procedures for analyzing the information that comes in to distinguish "false alarms" from real alarms. Indeed, as explored in more depth below, the value of a fire alarm system will depend on a) the capacity of actors to detect nuclear-related activities, b) the balance of incentives and disincentives those actors have for reporting detected activities, c) the analytic effort IAEA will need to expend to discriminate false from true
alarms, and d) the impact of diverting resources from additional police patrol efforts to a fire alarm type program.

4. Nonstate actors monitoring international regimes

Most of the benefits of any fire alarm monitoring system stem from enlarging the pool of potential monitors. Indeed, those designing a fire alarm monitoring system have incentives to ensure that they do not preclude anyone with relevant information from being able to pull the alarm. To date, however, most IAEA work appears to have centered on the role that the intelligence agencies of member states could play in signaling suspicious activities /e.g., see 11:67/. However, experience in many other arenas demonstrates that nongovernmental actors have different incentives and capacities that often make them valuable contributors to the monitoring of treaty compliance. Indeed, in some circumstances, those incentives and capacities may make them as likely or more likely than states to carefully monitor and report on treaty violations.

Scholars and practitioners of international relations have paid increasing attention to the role that nonstate actors play in the implementation of international treaties. In issue areas including human rights, environmental protection, humanitarian relief, and economic and social development, analysts have found that nongovernmental actors (NGOs) often devote considerable resources to monitoring treaty violations and contribute to the identification of violations that might not otherwise come to light /6, 7, 9, 18, 20-23, 27, 28, 31, 32, 34, 35/. Despite many international treaties and much of the UN system being "almost totally dependent on NGOs to provide expertise in many areas," international organizations involved in national security areas traditionally have given NGOs far fewer opportunities to be involved in or contribute to identifying treaty violations /18:115/.

Precluding actors that have proven to be valuable partners in other areas from making similar contributions in security regimes would appear to arise from two concerns. First, nonstate actors often lack the capacity to make significant contributions to efforts to detect violations of security treaties. They often have very limited financial resources and even more limited technological resources, both of which call into question how much "value added" nonstate actors would be able to provide. Second, states view national security as particularly sensitive and understandably seek to limit transparency about most, if not all, military activities. Efforts to keep military activities secret further constrains the ability of nonstate actors to gather valuable information. In addition, even if they could do so, many governments would be reluctant to legitimize the information they collect or the processes they use collect it by allowing it to be used within intergovernmental organizations and treaty regimes. The question, therefore, is whether nonstate actors might be able to make a constructive and cooperative contribution to arms control.

5. What could using fire alarms and involving NGOs accomplish?

Combining these two streams of scholarship, what could a fire alarm system that encouraged nonstate actors to monitor for undeclared nuclear activities and to provide information of suspect activities to the IAEA accomplish? In short, what is the potential contribution of NGOs and other nonstate actors including corporations and individuals to the IAEA monitoring system, and why might we expect these actors to provide additional if not better information than would be available from state governments.

The potential advantages of encouraging NGOs, corporations, and individuals to collect and provide IAEA with information regarding clandestine nuclear activities are several. Most obviously, it increases the number of actors watching for clandestine nuclear activities and hence increases the chances of identifying peculiar or suspect locations earlier. Information provided through such a system could not unambiguously identify undeclared sites by itself, but would serve to trigger determinations of whether a suspected site deserved further investigation.

Not only would involving NGOs provide more information but it would also provide a greater diversity of sources of information. Although reports from such sources would be "opportunistic and varied, rather than continuous and standardized in format and content. This variability would limit their usefulness, but these sources could also act as 'wild cards' which could not be easily predicted even by a proliferator knowledgeable about and seeking to circumvent the Agency's analytical methods and data
sources" /11:69/. These factors increase the direct and indirect deterrent effects. More information increases direct deterrence by increasing the proliferator’s expectation of “the possible negative consequences of detection;” it increases the indirect deterrent by making “a nuclear weapons production programme more expensive, more difficult in technical terms, and longer in duration” /11:66/. A nonstate actor fire alarm system faces the potential proliferant not only with the relatively predictable efforts by other states to detect its behavior, but also with the additional uncertainty regarding the types, identities, and locations of a wide range of potential nonstate monitors. In short, maintaining secrecy from a broader range of actors, including, potentially many of its own citizens, increases the need for countermeasures and the corresponding costs. Indeed, designing countermeasures to deal with actors who are likely to monitor in far more random patterns with processes and equipment that may be quite different from the routinized IAEA inspections or governmental satellite and plane overflights. Even if the non-routine monitoring and reporting that involving nonstate actors would undoubtedly entail did little to increase the likelihood of uncovering clandestine nuclear activities, it might nonetheless help in the nonproliferation battle to increase the costs and hence decrease the attractiveness of undertaking such activities. "If we assume that proliferators will take steps to confound the known and predictable information-gathering and analysis methods of the IAEA (though these may still complicate their operations), the greatest danger of detection and location of undeclared, separate activities will come from these less routinized sources" /11:73/.

Finally, a system capable of accomplishing these tasks does so without increasing the monitoring costs and resources that IAEA must expend. Although a system for distinguishing the validity of the information collected, and responding to sites determined to be suspicious could turn out to be quite costly, the overall cost effectiveness of the system might well be improved.

What reasons are there for believing that involving nonstate actors would lead IAEA to have information that it would not otherwise have? The logic for thinking nonstate actors might provide additional information stems from a view that they have different interests, capabilities, and authorities than states do.

Nonstate actors are likely to have different incentives than state actors. Within any state, some citizens are likely to have stronger allegiances to people outside and ideas above the state than to that state’s government. “The interests of states and peoples are not necessarily coterminous” /18:126/. Individuals and substate or transnational groups may have interests that run counter to a state’s interests in undertaking nuclear weapons development and keeping it secret. Citizens opposed to their government’s nuclear ambitions have strong incentives to look for and provide information that helps uncover and hence deter those ambitions. And, indeed, recent reports regarding India and Pakistan have demonstrated less than unanimous support for their decisions. Indeed, the interests of a state’s nationals are likely to diverge most from the interests of that state’s government in nondemocratic states /18:126/. Citizens may have stronger horizontal and transborder allegiances than vertical allegiances, identifying more on the basis of class, gender, race, or religion, rather than citizenship /18:134/. These actors may have access to and incentives to provide systematically different information than that available to and provided by their governments.

Citizens from other states may also have incentives to monitor and report on clandestine activities in states that seem likely to begin nuclear programs. Nongovernmental activists often prove quite persistent, much to the dismay of many governments, at uncovering information that those governments would have preferred to keep secret. For example, Japanese violations of their commitments under the whaling treaty were uncovered by non-Japanese activists who had come to Japan precisely to evaluate whether Japanese whalers had been hunting banned species /1/.

Individuals and nonstate actors are “sovereignty-free” rather than “sovereignty-bound,” a fact that allows them to use even their limited resources more effectively in some efforts /32:153/. Nongovernmental groups and individuals “need not compromise [their] principles” /20:51/. They do not need to show diplomatic deference toward other states and can often see vociferous attacks, both verbal and otherwise, as benefits in fighting a publicity war against the issue at hand. Although states usually seek to avoid being diplomatically harangued by other states, such harangues can legitimizing a nongovernmental
actors position and demonstrate to supporters that the organization and its efforts are being “taken seriously.”

Nonstate actors’ incentives to monitor and report on nuclear activities would prove meaningless if they did not also have at least some capacity to observe such activities. In other issue areas, nonstate actors have proved quite adept at providing “alternative data” /3.57/. They often engage in efforts to monitor and expose activities they oppose using various, often innovative, means /20.51/. The revelations of whaling violations, for example, involved NGOs doing rather sophisticated molecular genetic DNA testing of meat samples from markets in Japan. Environmental NGOs also played important roles in Russian dumping off Japan and in various Russian nuclear problems /13/. Although the technology and costs of environmental sampling to detect nuclear indicators are likely to be quite high in the near term, it would not be surprising to find NGOs establishing open sampling stations or undertaking more secretive sampling missions to monitor for nuclear emissions. Certain technologies, particularly if governments or IAEA promoted their development and thus reduced their cost, could help give actors with interests to monitor for nuclear activities the technical ability to do so.

Nonstate actors have also proven quite good at gathering considerable evidence from a range of nontechnical sources. Particularly in the human rights arenas, NGOs like Amnesty International and Human Rights Watch have proved quite capable, and often better than governments, at “monitoring human rights abuses and state compliance with international standards of human rights treatment” /32:155/. Partly this reflects the fact that citizens of one country may well have more rights, or at least attract less scrutiny, when traveling abroad than governmental representatives from that same country. All IAEA and official government efforts are constrained to gathering information through means that involve cooperation of the state being inspected, a set of constraints that are less binding in certain ways on nongovernmental actors. Of course, their capacity to uncover such information may be quite limited and the disincentives of having their identities come to light may outweigh these incentives. Indeed, activists concerned about a problem may have stronger incentives to monitor the behavior of another government rather than their own. For example, Amnesty International does not permit its members to investigate human rights abuses in their own countries. By traveling to another country, collecting information, and then reporting it, such individuals can avoid the repercussions and retaliation they might experience if they undertook such investigations within their own state. Indeed, a state that is not willing to expend resources to investigate another state’s treaty violations may be willing to expend resources to defend one of their nationals who does.

Finally, nonstate actors have consistently shown themselves willing to do considerable collection and analysis of information that may have been available but had not been focused on by governments. Perhaps the most striking examples of this come in the military arena, with groups like the Stockholm International Peace Research Institute, the Monterey Institute for International Studies, Jane’s, and the Carnegie Endowment for International Peace, inter alia, doing extensive and detailed studies of nuclear capabilities that match or exceed those undertaken by governments.

6. Conditions to achieve these gains

Whether a fire alarm system involving NGOs actually achieves these advantages is likely to depend on the incentives and capacities of nonstate actors to monitor and report on nuclear activities that states are seeking to keep secret. Those incentives and capacities are composed of contextual or “exo- genous” factors that do not depend on the type of system IAEA establishes and system-specific or “endogenous” factors that do depend on the type of system IAEA establishes.

6.1. Capacity

How able are nonstate actors to detect nuclear activities that a government seeks to conceal? These actors’ capacity to observe some of the indicators of nuclear activities is an initial and crucial prerequisite for any system like the one discussed here to be of value. Of course, any single disenchanted participant in that program may have considerable capacities to observe some portion, if not all, of the relevant activities. In addition, “outsiders” may be able to observe at least three major indicators of a clandestine nuclear development program. At least the later stages of a nuclear weapons development program typically involve a convergence of large-scale industrial activity with a considerable security presence. In addition, there are likely to
be environmental indicators of nuclear radiation observable well beyond the perimeter of any nuclear-related facility because of the likelihood of accidents and the difficulty of perfect containment. Corporations may be able to monitor efforts by actors from potential proliferants seeking to acquire nuclear-related technology. In almost all nuclear programs uncovered to date, efforts to procure technology abroad has played an important role.

On first consideration, the ability of nonstate actors to observe nuclear activities seems quite limited. Almost all activist nongovernmental organizations complain that financial constraints to be a “major hindrance” to their work /25:392/. Interestingly, however, during the very periods that many intergovernmental organizations were facing severe budget constraints, “NGOs like Al and Greenpeace experienced growth in membership and subscriptions” /32/. Nor do such organizations usually have particularly strong technological skills or resources. However, the construction and other activities related to building a major industrial facility, particularly a heavily guarded one, can be easily observed by any local residents if they take place near any populated areas. Obviously, government representatives seeking to procure nuclear-related materials cannot do so without revealing themselves to the corporations and individuals from whom they seek to procure those materials.

Nor are more technologically advanced approaches out of the reach of nonstate actors. The DNA monitoring done by environmental NGOs in Japan, the ships and Geiger counters that anti-nuclear protesters have used at Mururoa, and other examples suggest that, at least in some cases, they make considerable effort to remedy their general financial and technological shortcomings. Several analytic nongovernmental organizations have shown particular skill in uncovering military information from a wide range of states. Indeed, most of the information unveiled in the UN Register of Conventional Arms had already been available for some time from such NGOs as the International Institute for Strategic Studies in London and the Stockholm International Peace Research Institute /5:54/. The Carnegie Endowment for International Peace’s series of books on proliferation most recently published as Tracking Nuclear Proliferation /26/ provides another example of considerable and systematic effort to track down information on military and nuclear activities by nongovernmental actors.

Nonstate actors also may be able to get unauthorized access to areas and sites that the higher visibility of government officials would not allow. For example, “AI and groups staffed by Argentine political exiles first brought the human rights situation in Argentina to world attention after the coup in 1976,” and uncovered information that was not available even from the US State Department /23:424/. Indeed, some have argued that the UN and Amnesty International serve complementary roles, with the UN doing better at setting standards and AI doing better at monitoring and enforcing them /32:144/. They often provide “a range of information from a broader cross-section of sources” than states /32:152/. Various technological developments may increase significantly these capabilities. Technological advances make surveillance simultaneously easier and cheaper, increasingly bringing it within the tightly constrained budgets of many NGOs. Sophisticated, high-tech surveillance gear is now available at prices that many average citizens and certainly many NGOs could afford, if they were so inclined. The cost of commercial satellite imagery has dropped tremendously over the last several years, while the quality of such imagery has increased correspondingly. Prices now are in a range at which some NGOs may well be willing to undertake efforts to monitor certain activities at their own expense. For example, ABC News was broadcasting its own satellite pictures of the Chernobyl nuclear site within 24 hours of the US Government’s revelation of the accident over a decade ago /5:55/. Environmental groups and schools have coordinated programs in which grade school children around the United States now participate in distributed data collection efforts, generating aggregate databases on various environmental parameters. Geiger counters and other environmental monitoring instruments can be purchased in many countries and could provide the foundation for citizen-based monitoring programs conducted by individuals. Water quality monitoring programs organized by such groups might discover evidence of nuclear pollution downstream from plants that other evidence suggests have nuclear capabilities.

If NGOs and individuals have the capability to monitor, many also now have the capability to make sure that any information that they have becomes available to others. In many cases, the transnational networking capacities of NGOs, i.e.,
their capacity to move information across borders quickly and without government knowledge or permission, is as strong or stronger than that of many IGOs and governments /32:154/. The advent of cheap email, web, fax, telephone, and television technologies has created an "informational empowerment" of NGOs that has influenced international events in numerous issue areas /15:1127/.

Political considerations and constraints imposed by member states are likely to prevent IAEA from going out of its way to enhance these exogenous capacities to monitor. That said, however, IAEA could do a considerable amount to make sure that NGOs that do collect or otherwise come upon information of activities that suggest undeclared nuclear activities provide such information to the IAEA. Essentially, increasing the capacity of nonstate actors to report such information would be as simple as providing the authority for the IAEA to accept information from such actors and providing mechanisms for such provision. Simply providing standard forms for reporting information and providing a mailing address, telephone and fax numbers, email addresses, a website, and contact personnel, and ensuring that these contacts are as widely known as possible would be all that was needed.

6.2. Incentives

The incentives any actor has to monitor and provide information on suspect activities depend on the strength of the actor's incentives of preventing (and being involved in preventing) the state in question from acquiring a nuclear capability and the strength of the disincentives posed by that state's ability to retaliate against that actor for having done so.

Reporting of violations under a fire alarm detection system will not occur unless those violations inflict observable, attributable, and significant harm on some individual or group. That is, some individual or group has to be harmed, has to know they are harmed, and the harm has to be sufficient to outweigh any costs of or disincentives to reporting. The harm of nuclear weapons development is likely to be either the direct harm felt by those who consider such efforts to be bad policy for strategic, financial, or moral reasons or the indirect harm felt by those who bear undesired environmental or financial costs from such efforts. Particularly given the strong incentives to keep all aspects of a nuclear program secret, citizens may well be unaware that they are being harmed in these ways. Even if a program does inflict such harms on some citizens and even if they are aware of it, they will be unwilling to report it if doing so is difficult, costly, or risks retaliation.

Actors can be divided according to whether they are nationals of the government they are reporting on or not. The threat posed to "insiders" who do not want to become exiles from their own country is likely to be quite large. Israeli and Iraqi dissidents who have helped reveal the nuclear programs of their countries have faced harsh retaliation from their governments. At the same time, opposition groups have strong incentives to reveal such information as they have, since it allows them to bring external political pressure on a government which they want ousted for other reasons. For example, the resistance group Mojahedin-e-Khalq revealed that an Iranian power reactor facility was involved in nuclear weapons /12:129-130/. Within likely proliferant states, there may be particular value in the nuclear realm of fostering linkage between the security aspects and environmental aspects of nuclear weapons programs. Even individuals that might support their country acquiring a nuclear capability may resist the notion of being the environmental victims of such a program. These individuals may have strong incentives to monitor and report nuclear releases of any sort, particularly if they have been educated about the possible risks and provided with the means of identifying such releases.

Outsiders have stronger net incentives to monitor and provide information, although they may have more limited capacities, since the risk from the suspect government is far less. Indeed, most governments would consider any effort to retaliate against their citizens for helping to reveal clandestine nuclear activity as warranting severe sanctions. Thus, these actors face far less risk of retaliation, assuming they are outside the suspect country at the time the information becomes public. Indeed, NGOs have shown considerable willingness and ability to contribute to the searching out and identifying of national violations of human rights and environmental treaties in most countries around the world.

Although NGOs face greater financial constraints than governments and IGOs, they face fewer political constraints. Most such organizations assiduously avoid "the political entanglements of government" /15:1129/. By avoiding accepting any government funding they
can avoid government influence and interference in their investigations and behavior while simultaneously increasing their credibility with their members /32:150/. Avoiding governmental contributions to their operations, such groups gain “autonomy in their actions” /34:144/. Avoiding government contributions to their operations, such groups gain “autonomy in their actions” /34:144/. Most human rights groups cooperate extensively with the UN Human Rights Commission and other UN agencies helping in “monitoring violations or developing mechanisms for enforcing international standards are primary goals” /25:387 & 396/. Amnesty International (AI) has collected and reported evidence of human rights abuses in Tibet during periods when UN agencies and national governments have been consistently reluctant to do so /32:148/ . NGOs can be far more single-minded in their efforts to uncover and report violations, and do not face the tradeoffs that NGOs and governments often face /32:148/. It is precisely their freedom from governments and the cross-cutting goals that provides such groups with the freedom of action necessary to be “effective watchdogs” against human rights abuses /32:143/ .

In the corporate arena, major American, German, and Japanese companies contacted by foreign nationals have shown that the profit motive overpowers their interest in revealing suspect activities. On the one hand, corporate actors who stand to make large sums by providing requested equipment have strong incentives to avoid looking for, let alone revealing, any suspicious potential uses of the products being sold. Of course, the negative threat of fines and other punishment for such transactions are already in place in most countries. These might be enhanced, however, by providing more positive incentives for corporations to provide information of suspicious contacts. For example, corporations might be placed on an IAEA “white list” of proliferation monitors who voluntarily provide IAEA with information regarding all contacts and sales to foreign nationals of certain lists of equipment. Such a list would promote those companies reputations while also signaling to proliferants a declining number of available sources for required technologies.

The core endogenous factor influencing the incentives for actors to monitor and provide information to the IAEA will be the credibility of the IAEA’s offer of anonymity. Actors will only be forthcoming with information at their disposal if they can provide that information without having to reveal their identities. The most credible offer of anonymity will involve processes for the submission of information that ensure that identifying information never makes it into the IAEA information system. This requires not only allowing actors to submit information without requesting identifying information, but also must ensure that such information is not collected by other means, such as through identifying fax numbers, web addresses, etc. This problem does not seem insurmountable, however. In the face of major threats to informants if their identities are revealed, human rights NGOs have provided the requisite anonymity to ensure a continuing flow of information about human rights abuses in most countries of the world. Similar procedures for anonymity to defend against governmental retaliation can be seen in the International Chamber of Shipping’s periodic compilations of tanker captains’ reports on governments that have not provided pollution control facilities in their ports /16/.

6.3. How likely are NGOs to be involved?

Considerable empirical evidence from other fields suggests that nongovernmental actors may monitor and provide information to intergovernmental organizations that facilitate compliance management and violation detection. In a wide variety of arenas, NGOs have become “internationally known for their role in providing services that governments have failed to provide,” most frequently providing the international public good of information /15:1128/.

In the military arena, the recent increase in efforts by military authorities to provide humanitarian assistance have provided experiences that have broken down traditional barriers and animosity between military organizations and activist relief organizations. Those experiences have demonstrated the benefits of cooperation between NGOs and military forces, particularly in the realm of information sharing /15, 31:34/. Although military and nongovernmental organizations often have widely-divergent goals, outlooks, mindsets, and organizational structures, both groups have increasingly sought out and benefited from positive interaction that take advantage of those differences /31/. In many missions, military organizations are seeking rather than rebuffing informational input from and coordination with NGOs, including information from NGOs regarding the location of landmines and other hazards and “an Internet-based, multi-media, information-sharing system to enable unclassified,
crisis-relevant information exchange among policy makers, commanders, international agencies, relief organizations and media" /31:37/. Indeed, "military leaders must begin to view the NGO community as a combat multiplier during [humanitarian assistance] operations. NGO expertise is vital to the military's success" /31:37/.

In the human rights realm, groups like Amnesty International and Americas Watch played crucial roles in uncovering and publicizing human rights abuses in Argentina and Mexico /23/. They have played important roles in helping collect information on most of the human rights conventions under the UN system /18, 32/. In these and other human rights settings, "international human rights NGOs devote a great amount of their attention toward working with international institutions" /25:412/. "NGOs like AI continue to play a more effective role than the UN in human rights monitoring" /32:158/. In many cases, governments and IGOs have based their human rights reports on information provided by NGOs /23:435/.

In the environmental realm, Greenpeace International, the Natural Resources Defense Council, the World Conservation Union and many other NGOs monitor "environmental quality, as well as national compliance, and are becoming involved as a source of shadow verification of government obligations in the EU and elsewhere," increasingly "replacing or supplementing the monitoring activities of national enforcement agencies" /8:25/.

7. What are the costs, disadvantages, and risks?

Even if a fire alarm system that involved NGOs helped increase the chances of detecting undeclared nuclear facilities, the value of creating such a system would depend on questions regarding its costs, its disadvantages, and its risks.

7.1. Information processing costs

The largest specter that such a system raises is the issue of costs. Even if NGOs pick up all the monitoring costs, the IAEA would still face considerable costs of processing the information. The IAEA already operates under a heavy information load, and providing opportunities for many more actors to provide information to the system could well produce an information glut and information overload. "Would the information gathered and the analytical routines used be able to lead to reasonably convincing, even if still uncertain, conclusions, or would much either be lost in an unfavourable signal-noise ratio or be very readily explained?" /11:69/. If the new information simply produces more input without producing better output in terms of 'undeclared sites detected, such a system would be a waste of effort. However, there is considerable reason to believe that more information may be "a significant benefit rather than adding substantially to management problems and ambiguity" /11:67/.

The real problem for such a system is the problem of false alarms. If all the incoming information were truly related to nuclear activities, or indicators reasonably suspect as nuclear activities, the system would be worthwhile. However, as the percentage of all information that involves false alarms increases, the more difficult the analytic task IAEA will face. True alarms are likely to be numerically rare for three reasons. First, few governments have the incentives and/or capacity to attempt to develop nuclear weapons. Second, those that do will make every effort to prevent anyone from observing such an attempt. Third, those who observe such an attempt may well have strong reasons, in the form of harsh sanctions by the relevant government, not to report it. Of course, a system that prompted any such true alarms would be incredibly and unambiguously valuable so long as every alarm received could be known to be true. Unfortunately, the value of any real system will depend on the ability and cost of the system to distinguish any true alarms that are received from the false alarms that undoubtedly will be received. Therefore, assessing the value of instituting a fire alarm type system depends on assessing the likely number of false alarms and the likely cost per alarm of determining whether it is true or false. The system will need to be able to tolerate some false alarms, since they are inevitable. If the "signal-to-noise" ratio becomes too low, the analytic cost of finding true alarms will become
excessive /11:69/. The system's value, of course, depends on false alarms and their associated costs not being excessive.

7.2. Political costs of false alarms

False alarms also pose significant political costs if they prompt any response by the IAEA, a necessary condition for the system to be effective in the first place. Even inquiries, let alone more intrusive actions, regarding activities are likely to be quite costly diplomatically. Reports from NGOs in a fire alarm type system are very subject to "problems of credibility, ambiguity, bias, and their inherent occasional nature" /11:70/. The IAEA will be caught between the need to conduct follow-up inquiries on suspect activities reported by various actors, in order to build the credibility needed to prompt NGOs to provide the information in the first place, and the need to avoid follow-up inquiries to maintain good relations with the member states. Much of this balancing will require that no follow-up inquiries of a government be undertaken until the credibility of any information suggesting suspect activity is verified, either by reference to the source of the information or by corroboration from other sources.

7.3. Likelihood of false alarms

Although the cost of false alarms, if they occur, will be quite high, there are some reasons to believe that they will be relatively infrequent. One the one hand, "NGOs may certainly have their own agendas" /3:67/. Although they will contribute to efforts to implement treaties, they are likely to do so "in ways consistent with their own environmental and political agendas" rather than the goals of the IAEA /20:51/.

That said, NGOs are unlikely to provide excessive amounts of information or false information for two reasons. First, the very nature of nuclear activities means that while NGOs will have some information and evidence of behaviors that may constitute suspect activities, they are not likely to have a wealth of such information. Essentially NGOs and other nonstate actors are likely to have some, but not much, information relevant to the issues that IAEA addresses.

Second, and far more important, NGOs have quite strong incentives to make sure that any information that they provide is supremely accurate. The biggest asset most NGOs have is their impartiality and accuracy. Crucial to the success of NGOs is their ability to serve as "credible independent sources of human rights information" /23:429/. Their very distinction from governments is that they have "sufficient independence from government to serve as a watchdog" /23:433/. For example, Amnesty International maintains "scrupulous neutrality" in its human rights work, even deliberately "precluding AI chapters from investigative and lobbying activities in home countries" /32:149/. This helps prevent these chapters from "becoming the targets of hostile attention from home governments" but also builds detachment, objectivity, and, hence, credibility /32:149/. Indeed, NGOs may be more even-handed than IGOs: "AI is more willing to investigate possible human rights abuses by any government while the UN confines itself to selected governments" /32:51/.

Impartiality is crucial not only to the influence of NGOs but also to their continued existence. "Nonprofit NGOs need a trustworthy reputation to continue receiving donor funds and from a long-run standpoint, their best interest rests in maintaining an honest, open environment" /15:1136/. This is evident in the efforts made by many, although certainly not all, NGOs to preserve the veracity of their information as the basis for their credibility. "The entire structure of the AI movement is designed to collect, distribute, and use information that has been cross-checked and will withstand determined efforts by governments to discredit it" /32:150/.

7.4. Reducing the incentives for false alarms

Requiring several sources of corroboration prior to taking any action will be both a political necessity and help alleviate some of the problems already addressed. If nonstate actors know that the ability to prompt IAEA action will depend on information coming from multiple, credible sources, most are likely to be exceedingly cautious in what claims and accusations they make to the IAEA. Making claims that have little or no substantiation reduces the credibility of any future claims from the same organization, thus quickly reducing the nonstate actor's influence with the IAEA. Even without any explicit sanctions for providing false or unsubstantiated claims, the very desire for influence over IAEA activities will tend to lead nonstate actors to contact the IAEA only with their most solid and well-documented evidence.
8. Other links in the chain

Creating such a new system for including information from NGOs would also pose IAEA with at least three additional tasks. First, adopting such a system would likely require that the IAEA and supportive members overcome the resistance of many states that would resist move to involve NGOs in IAEA activities. In the human rights arena and in environmental arenas, many governments have opposed efforts to increase NGO involvement, precisely because of their ability to monitor human rights or environmental violations /18:121/. There is also concern that they will provide inaccurate information that will lead to excessive burdens on the IAEA resources and to false accusations. The goals of NGOs will not always be consistent with the goals of the IAEA or those of its member states. The concerns, raised by this problem will require the IAEA to design the system to overcome these problems.

Second, as already noted, the IAEA would need to create a system not only for collecting such information but also for processing the information. Data processing and analysis to determine and assess information to distinguish false from true alarms will be an important component of the system. Much of the success of this sort of system will depend on the analytic capabilities of IAEA to cull down the information into a form that makes a convincing case for some form of further action, whether request for clarification, requested surveillance by third parties, or direct inspection.

Third, the IAEA will need to develop procedures for how it will respond to information. To the extent that high-quality reports do come into the IAEA system initially, whether they continue to do so will depend on what it does with the information. The information prompted by such a system rarely will identify an undeclared site unambiguously. Rather, that information will need to help initiate activities by IAEA and member governments to determine whether a site is an undeclared nuclear facility or something more benign /32:153/. When apparently credible information has been corroborated against other information already available to the IAEA, the IAEA will need to have a graduated set of steps for reducing the ambiguity of the activity. The sequence and timing of requests for clarification, surveillance by other parties, direct IAEA inspections, and other possible responses will need to be laid out. Partly, this will also require that the IAEA and its member states overcome “the refusal to accept circumstantial evidence or the balance of evidence as an indication of compliance” /24:138/. Over time, however, if information provided to the IAEA system appears to go into an informational “black hole,” those information sources will tend to dry up and the value of the system will be wasted.

9. Conclusions

This article has suggested that nonstate actors may constitute an untapped resource capable of helping the IAEA in its current efforts to uncover undeclared nuclear activities before they become a problem. By creating a “fire alarm” type system to which NGOs and other nonstate actors could contribute information with the assurance of anonymity, the IAEA might be able to increase its chances of identifying suspect activities.

The value of such a system will depend on a closer assessment of the capabilities and incentives of relevant nonstate actors to monitor areas and behaviors where undeclared nuclear activities could take place. It will also depend on their capabilities and incentives to report that information to the IAEA.

At present, the time may not be right. The technical capacities of nonstate actors to detect nuclear activities may not significantly enhance the chances of detecting undeclared nuclear activities. However, satellite surveillance imagery and environmental sensing technologies appear to be increasing in resolution while decreasing in costs, and may increasingly be widely available to nonstate actors concerned about nuclear activities by their own state or other states and willing to dedicate considerable resources to identifying such activities. Even if the time is not right today, then, the question of whether nonstate actors can provide a useful contribution to the efforts to deter nuclear proliferation deserve further consideration in the future.

10. References


17/ Green, Andrew and Ann Matthias. 1996. "How should governments view nongovernmental organizations?" World health forum 17:1, 42.


