Chapter 3

Interagency and International Communication and Cooperation

Contents

Chapter 3
Interagency and International Communication and Cooperation

INTRODUCTION—EXAMPLES OF PROBLEMS

About 25 U.S. Government agencies deal with aspects of terrorism.[1] They are represented on the Policy Coordinating Committee on Terrorism, its technical subcommittee, the Technical Support Working Group (TSWG), and other interagency working groups. Coordination of activities among these participants has improved over the last several years, at least in part due to the availability of the TSWG as a forum. This chapter deals with problems of assuring adequate communication and coordination in the fight against terrorism.

Examples of difficulties in communication and coordination extend over a multitude of areas, from the relatively straightforward matter of exchanging information on current research or on terrorist organizations and threats to crisis coordination. OTA has not performed a detailed study of all aspects of interagency communication among the 25 (or so) government agencies that participate in counterterrorism work. However, during the course of the project, OTA has become aware of a number of problems, past and present. This chapter will provide examples of these problems. Some have been successfully resolved; others have not. Following the exposition of examples, which indicates the scope of the problem, OTA presents a series of options for improving interagency coordination for Congress to consider. In addition, there is a brief discussion on international coordination of counterterrorism R&D.

Interagency Exchange of Information

Some difficulties in communication simply involve red tape. During the course of this study, OTA staff were asked on two occasions to facilitate transfers of R&D information between one agency and laboratories belonging to another. It was not that the information was otherwise unavailable to the requester, but it was felt that due to lengthy bureaucratic procedures, going through established channels would delay information transfer by months.

There are problems regarding the dissemination of vital data of relevance to terrorism. A useful and interesting source of information, the TECSII database, is managed by the U.S. Customs Service and the Immigration and Naturalization Service (INS). It contains information, such as description and passport number, regarding individuals who may have excited suspicions on the part of Customs or INS agents when they presented themselves at a U.S. port of entry. Some may have been found carrying contraband, others may have violated other laws, and still others may have matched a suspicious profile, based on their recent travels or on other factors.

This database is available to various government agencies. However, only a very small number of terminals connected to TECSII are available to the agency with chief responsibility for domestic counterterrorist activities, the Federal Bureau of Investigation (FBI). Further, this source of information does not appear to be frequently accessed by the FBI, even during time of increased international tensions, such as during the period prior to the Gulf War in late 1990 and early 1991. True, this source of information is limited: no one who does not appear at a port of entry is included. Nevertheless, the database may contain much valuable information, particularly at times when there is reason to think that an effort may be underway to introduce terrorists into the United States.

Interagency Arguments

Another category of communication difficulties involves turf protection and institutional disputes among agencies. On one occasion, two different agencies were funding closely related research by the same contractor into explosives detection. The two agencies had different applications for the technologies, and, consequently, different specifications for a workable system. One agency ran a test on

[1] See U.S. Congress, Office of Technology Assessment, *Technology Against Terrorism:* The *Federal Effort*, OTA-ISC-481 (Washington, DC: U.S. Government Printing Office, July 1991), app. E for a listing of Federal participants in counterterrorism R&D.

a prototype that did not yield very favorable results. The second agency had run tests on similar equipment that looked significantly better, at least for that agency's purposes. As a result of the first agency's negative results, however, the research program of the second agency was nearly canceled by higher officials. This eventuality was averted but the upshot was a bad feeling between the program monitors of the respective agencies that became counterproductive. Fortunately, this dispute was resolved fairly quickly, but the fact that it occurred at all (in spite of the existence of the TSWG, which should have provided a natural path of communication among the individuals) is disturbing. This episode represents a serious problem of coordination among agencies involved in related research.

Turf problems, now happily resolved, were evident in another arena. The Federal Aviation Administration (FAA) is responsible for overseeing security procedures at U.S. airports. Some regulations require the display of identification badges by all personnel in protected areas at airports, particularly those areas with access to aircraft. This is to facilitate the detection of unauthorized personnel in those zones. However, the Customs Service considered that Customs officials in uniform were not required to obey such regulations. The problem, from a security point of view, is that a malefactor could conceivably obtain a reasonable facsimile of such a uniform, and would then be immune to challenge by airport authorities or local police. The refusal of Customs officials to display airport identification led, at least on one occasion, to a confrontation, with guns drawn, between a Customs agent and a local policeman.

This problem has since been resolved by discussions at high levels among leading officials in the responsible agencies. However, matters should not have been allowed to deteriorate to that point.

Classification Issues

Another example of a snafu in interagency R&D coordination involves Imatron Corp., the manufacturer and developer of a promising device to detect explosives—a rapid computertized tomography machine. Imatron performed some tests in late 1990 under contract with the FAA. The results appeared interesting and deserving of more rigorous evaluation. However, during this period, classification guidelines were promulgated by the Department of Transportation that labeled information on the effectiveness of potential explosives detectors as ''confidential. ''

A problem then arose because Imatron has some foreign minority shareowners (Italian and Japanese). Even though the company is over 50 percent U.S.-owned, foreign participation was enough to prevent Imatron's laboratory facilities from being designated as capable of handling classified data. Imatron has had to cease testing and other related work for the FAA until the problem can be resolved. The legal solution, spinning off an entirely U.S.-owned subsidiary to do the classtified work, will take months to accomplish, resulting in months of time lost.

In addition, there are some examples of redundancy of effort in some lines of research applicable to counterterrorism (and to counternarcotics). One case is the existence of several projects in different agencies developing the same technology (using relatively high-energy garoma rays) to examine large cargo containers for contraband, including narcotics, weapons, or explosives.

The existence of the TSWG has reduced the incidence of this type of duplication, but has not eliminated it. The TSWG tried, on one occasion, to assemble an updatable database of relevant R&D progress. The availability of such information would make such redundancies of effort considerably less likely. However, due to limited funding, this database was never set up.

OTA considers the establishment of an interagency database on the state of the art in technology and R&D applicable to counterterrorism to be an important part of the development of adequate coordination of the Nation's counterterrorism effort.

Scrabbling for Funds

Some agencies with limited R&D funding resources are currently forced to seek funds from more affluent agencies in order to pursue research projects that they feel are essential. An example is the INS, which has only $400,000 per year available for R&D. In addition, the Forensic Laboratory of INS, even though highly regarded, is barely able to purchase the chemicals it needs to function normally, and has no funds at all for R&D.

An area of interest to INS is automated facial recognition. Pattern recognition technology, using video images and sophisticated software algorithms, has progressed to the point where useful and interesting facial recognition equipment may be feasible to develop. The object would be to provide assistance in identifying individuals at ports of entry, when applying for U.S. visas, using photographs or direct observation. In the counterterrorism area, comparison could be made with a file of pictures of known terrorists, because facial measurements preserve a number of known parameters in spite of attempts at disguise and changes due to the aging process.

Although INS has need and use for such work (as do other parts of the Government), it was unable to fund it adequately alone. Therefore, it was forced to seek the assistance of other agencies to find resources to keep such research alive. While INS officials have been somewhat successful in this particular effort, at least up to the present (enabled by informal contacts among scientists working in the field), the haphazard nature of such means of funding is not conducive to an efficient and effective research program. This anecdote, like others previously mentioned, argues for the existence of a better endowed interagency R&D funding group with more effective coordination than now exists.

EXAMPLES OF IMPROVEMENTS IN INTERAGENCY COORDINATION AND COMMUNICATION

Interagency Communications Links

Perhaps the most literal example of lack of effective communication involved the lack of common, secure communications channels among different elements in law enforcement operations (e.g., FBI, Coast Guard, Customs, INS). This deficiency could result in difficulties during combined operations against relatively sophisticated narcotraffickers trying to run contraband into the United States. The efforts of an interagency working group on the topic have resulted in the establishment of secure, common channels that are now available for use.

Redundant Research

In one area of counterterrorism, several highly classified projects were underway in diverse agencies to develop a vital protective tool. There was little communication among the specialists working on the problem, so there was not only a duplication of effort, but also a rate of progress slower than would have been the case if there had been adequate interchange of ideas and information. However, in part due to the forum created by the existence of the TSWG, and in part due to an informal network of contacts among agencies, the problem was identified, and an interagency working group set up in 1990 to coordinate R&D efforts.

As a footnote, an overseas firm and a domestic one are openly marketing a device similar to the one being developed in great secrecy within the government.

Response Plan for Chemical or Biological (CB) Terrorist Attacks

Extensive interagency plans for coordinating a Federal response to nuclear or radiological attacks by terrorists have existed for many years under the leadership of the Department of Energy, with support from the Department of Defense. The implementation of these plans is aided by an array of sophisticated technical equipment. Cooperation among a number of highly specialized response teams from different government agencies has been a principal element in devising these systems.

Until very recently, however, there had been no plan for preparing and coordinating such a response in the case of attack by means of chemical or biological agents, beyond designating the FBI as the response agency and providing for some support by the U.S. Army. This was in spite of assessments by many experts that a CB terrorist attack would be much more likely than a nuclear one.

Fortunately, this deficiency is now being remedied by the development of a response plan involving a large number of agencies, under the leadership of the FBI. Other participating agencies include the Environmental Protection Agency, the Department of Health and Human Services, the Department of Defense, the Department of Agriculture, and the Federal Emergency Management Agency. Appropriate expertise from the most knowledgeable agencies is now being brought to bear on the subjects, and

trained and equipped response forces are being assigned responsibilities in case of such an event. Procedures for rendering assistance to local authorities have been developed. While the plan has not yet been finally implemented, the Nation now has a capability for dealing with this eventuality.

Special Operations Expo '90

In order to stimulate communications among scientists and engineers of the National Laboratories and the military professionals responsible for special operations, the Department of Energy and the U.S. Special Operations Command (SOCOM) of the Department of Defense held a joint exposition in March 1990. Each of the Laboratories working on related technical questions set up exhibits to demonstrate their capabilities to military and technical personnel of SOCOM.[2]

Although this field is not identical to counterterrorism, special operations do include military actions against terrorism, so many of the technologies being researched would apply directly to the topic of this study. Further, other technologies (e.g., sensors) that are useful for low-intensity conflict (the main concern of special operations) would also have applications in the counterterrorist arena.

Many of the participants felt that the exposition was useful in bringing together for the first time technical experts from the laboratories with experts in the operational field. Another such conference was held in November 1991.

Findings and Summary

Direct contact of the above sort between the technical and operational cultures is often an efficient process that cuts through red tape and facilitates transferring information on operational requirements to scientists and information on technological possibilities to the military professionals. This principle could be profitably extended to other fields of counterterrorist endeavor, especially in the relevant areas of the behavioral sciences (in which interagency communication **could be improved, see ch. 5) and in aviation security. Periodic symposia and conferences, bringing together experts from different agencies to exchange ideas and information, are useful and should be increased. There should be an effort to arrange such conferences at least on an annual basis. This might be another function that the TSWG could perform.**

In fact, some such conferences do take place.[3] However, there is a need for more of them sponsored by government agencies in the counterterrorism field, so that technical experts from diverse agencies who rarely communicate with each other could interact. When necessary, they could be held in classified formats.

In summary, there have been a number of recent improvements in interagency coordination. However, there are several areas where coordination of counterterrorist efforts could be upgraded. This applies both to R&D and to technology related to operations.

OPTIONS

In counterterrorism research and development, **two** institutional phenomena are salient. First, in some fields, there is redundancy in research projects. Typically, different agencies spend significant funds, sometimes paying the same vendors, in order to develop similar hardware. Second, some agencies (e.g., INS, the Secret Service, and the FBI), suffering from virtually nonexistent budgets for R&D, yet needing to develop tools for **counterterrorist missions**, are forced to shop around for well-heeled agencies to provide funds to support these efforts.

Both these difficulties should, in principle, be avoided because of the existence of the TSWG and its parent, the Policy Coordinating Committee on Terrorism. These interagency committees are meant to coordinate activities in this area in a way that avoids redundancies and assures that needed work gets done, even if no agency can alone find the funds to perform it. However, as noted in the previous OTA report on technology and terrorism,[4] funding

[2]The DOE Laboratories included were Argonne National Laboratory, Remote Sensing Laboratory/Las Vegas, Idaho National Engineering Laboratory, Los Alamos National Laboratory, Lawrence Livermore National Laboratory, OakRidge National Laboratory, Pacific Northwest Laboratory, Sandia National Laboratory, and the Special Technology Laboratory.

[3]For example, the American Defense Preparedness Association (ADPA) has been organizing annual meetings on security technology fOr 7 years. Also, the Department of Transportation, together with private sector organizations, has presented yearly meetings on transportation security, and the Federal Bureau of Investigation has periodically put together meetings on explosives detection.

[4]U.S. Congress, Office of Technology Assessment, op. cit., footnote 1.

for the TSWG has been problematic, declining by 80 percent in fiscal year 1991 relative to the level at its inception 5 years ago. Shortage of money apparently increases turf protection and discourages communication among the agencies doing the R&D. It also encourages scientists to use their own informal networks of colleagues and friends in other agencies to seek funding for needed projects-funding that should be assured and coordinated through the interagency group for such research. This approach, while practical for the individual, results in a haphazard allocation of resources.

Politically, it will not be easy to put all counterterrorism R&D under one umbrella, and that should not be the goal. Some agencies (in particular, those of the Intelligence Community and the Defense and Energy Departments) would likely not be interested in having those counterterrorism projects specific to their own missions controlled or subsumed by an interagency group. But those projects with interagency applications, and there are many, both ongoing and proposed, should be coordinated by a central entity. This measure is needed to avoid redundancy of effort and to increase contacts and interaction among scientists doing similar work. Otherwise, current inefficiencies and barriers to communication will continue, hurting the national counterterrorist R&D effort.

The coordinating group should have sufficient funds, respect, and, thus power, to run an efficient program. If substantial research funds are not under control of the coordinating group, it will not be taken as a serious player by the member agencies. To improve communication among participating experts, a larger fraction of the Nation's counterterrorism research should be subject to coordination from a single source than is currently the case. Now, the TSWG represents only $2 million out of over ***$70*** million. Even if expanded to $10 million, this fraction would still be only about 15 percent.

Effective interagency coordination would avoid significant redundancies in research projects. However, coordination is also needed beyond the R&D arena. Efficient interagency exchange of information needs to be implemented. On the R&D plane this could be accomplished by holding interagency technical seminars, for example, and on the operational level by establishing, maintaining, and using interagency charnels of communication. Effective coordination should provide databases on technology and databases and alerts on terrorists and their activities. These should be accessible to all agencies with need for the information.

OTA has identified four options for improved coordination among the many agencies that have R&D interests in counterterrorism.

Option **1: Continue with the TSWG and its parent Policy Coordinating Committee on Terrorism as now funded, run through the Department of State, with a large increase in funding, as now planned, mostly originating from Department of Defense funds. Give the TSWG its own line item in the State Department budget.**

Advantages. This continues the present institutional situation, which has worked until now, although hampered by funding constraints. Many of the participants are familiar and comfortable with it. The increase in funding (proposed to $10 million from $2 million), if implemented, should be sufficient to assure that needed projects, particularly of research-starved agencies, are undertaken. This setup allows decisions on research to be made by a committee made up of representatives of all the participating agencies. It is meant to assure that the large research agencies (e.g., Defense and Energy) will not dominate or gobble up the research pie.

A line-item status will help assure that other components of the State Department do not drain funds intended for the TSWG. It may also help in providing an incentive for the State Department to give more active support to the TSWG when appealing for funds from Congress.

Disadvantages. There may remain some congressional opposition to funding a research program through State, which is not a research-oriented agency. The funding may never be assured from year to year, unless strong advocates appear, either in Congress or the executive branch. Power and decisionmaking maybe perceived as tilting towards Defense, since a large share of funds will be supplied from their budget. Defense is already managing the program for State, which has limited technical expertise.

Option 2: Place the TSWG in a major research agency, such as the Department of Defense, the Department of Energy, or the Department of

Transportation (now a major participant in counterterrorism R&D). Give it a line item.

Advantages. The Departments of Defense and Energy both have significant experience in managing R&D programs of all sizes and at all phases. Stable funding would be more likely; even if the congressional allotments were to fluctuate, the host agency could make up differences in lean years, since the whole program would constitute a minute part of the agency's research program.

Disadvantages. There could be distrust among other participating agencies, since the perception will be that the host agency will take the lion's share of projects. A committee may make funding decisions, but the power of the purse of the host agency might swing decisions in favor of research it particularly wants. On the other hand, the host agency may not want the program, since it may perceive that the cost of TSWG research, primarily done **to satisfy** other agencies' needs, would be deducted from its own in-house research.

Option 3: Replace the TSWG with **a** similar funding group **run out of a DOE national laboratory or a smaller agency with research capability. Give it a line item.**

Advantages. A laboratory would be familiar with science and engineering issues and research practices, which would help in furnishing competent oversight. An operational agency would be aware of the field requirements of the equipment. In the former case, the TSWG would be somewhat removed from interagency rivalry, although subject to interlaboratory rivalry.

Disadvantages. This would place much power, probably too much, in the hands of only one participating agency, even if accompanied by an interagency oversight board. Since the TSWG would be replaced, many old players would likely not be enthusiastic, especially State, Defense, and Energy, all of which had leading roles. If the location were a national laboratory, Energy might be somewhat mollified.

Option 4: Replace the TSWG with a similar funding group operating out of a technical office close to the President with no direct interest in doing research itself, such as the President's Office of Science and Technology Policy, or the National Security Council (NSC), or out of a new office, following the model of the Office of National Drug Control Policy.

Advantages. The coordinating body would be in a strong position of power (if actively supported by the White House) and thus able to arbitrate among agencies and deal **with rivalries** and parochial interests. A strong position would also help in eliciting information from reluctant participants and in fighting turf builders. If located in the White House Office of Science and Technology Policy (OSTP), the coordinating group would be likely to have strong technical input. It could also benefit from the perception that the OSTP would be a disinterested, honest broker. This would also apply to the creation of a new office. Also, this option might provide **a** good place to take advantage of existing talent to deal with the multidisciplinary needs of overseeing a highly varied program. A new office would have to receive separate research funding and control the power of the purse strings, otherwise participating agencies would not be interested in playing. This option might level the playing field among agencies in that more weight might be given to the needs of agencies with limited R&D budgets (e.g., Secret Service, INS).

Disadvantages. The TSWG would disappear, thus irritating the same participants as in the previous option. A new arrangement for counterterrorism R&D would exist, making long-time participants uncomfortable. Major agencies might be more reluctant to play. Congress maybe reluctant to fund anew agency or to increase significantly the budget for an existing office. The OSTP or NSC might be reluctant to take on the task of managing research, particularly in a narrow area.

INTERNATIONAL COOPERATION

The United States engages in cooperative efforts in the field of counterterrorism with a number of its allies and in some international forums. The United States works most closely with Canada and the United Kingdom. Collaboration with the Canadians is especially active in the areas of explosives detection and airline security. Several firms with competitive vapor detectors are Canadian; Canadian experts participate with U.S. agencies in discussions regarding research into airline security. Periodic counterterrorism exercises are held with the Canadians.

The United States also exchanges information with the United Kingdom in a number of areas relevant to counterterrorism. One thermal neutron analysis (TNA) machine for explosives detection, developed for the Federal Aviation Administration (FAA), is being tested at Gatwick airport near London, in cooperation with British airport authorities. There are also exchanges of information with other European allies. In all cases, however, there is technical information considered so vital to national security that no party will exchange it with another.

Some research projects in other countries are funded by U.S. agencies. For example, scientists at the Soreq Nuclear Research Center in Israel are, in collaboration with scientists from Los Alamos National Laboratory, working on developing the nuclear resonance absorption technique for explosives detection. The joint effort is funded by the FAA. This project also involves interagency cooperation, since Los Alamos is a National Laboratory of the Department of Energy: an interagency agreement between the FAA and the Department of Energy enabled this collaboration on a national level. The FAA is examining a Soreq bomb detecting device employing advanced x-ray techniques. A Memorandum of Cooperation between the FAA and the Israeli Airports Authority was signed to permit the international effort between FAA and Soreq.

There are efforts to establish research collaborations on other topics between U.S. and foreign scientists, particularly those in Western Europe. Recently, the Soviets have expressed an interest in technical exchanges on counterterrorist technology, probably reflecting a concern with internal ethnic discontent and the large number of hijackings within the past 2 years. Such collaborations and exchanges of information also may have the added advantage of saving money in research efforts.

In addition to formal collaborations at the intergovernmental level, there are periodic international conferences on explosives detection that result in useful exchanges of information.

Regarding international organizations, the International Civil Aviation Organization (ICAO), an agency of the United Nations, has recently concluded a draft **treaty** on tagging explosives during manufactures The United States and Canada, together with France, the United Kingdom, Czechoslovakia, and other European countries were particularly active in bringing this effort to fruition. ICAO is continuing efforts to examine the uses of technology to further international airline security.

Another international effort in which the United States participates is Interpol, the international police organization, which exchanges information on criminals. U.S. officials are assigned to Interpol work, both in the United States and at Interpol's headquarters in Lyons, France. Information on terrorists that is not classified is sent to Interpol by the appropriate U.S. agencies. The United States also receives such information for use when domestic action is feasible. Interpol has recently improved its communications capability and can now send specific pieces of information through secure channels to only those nations authorized to receive it.

The United States also has observer status with the TREVI group, an organization of Western European Interior Ministries, that is concerned with, among other things, exchanging vital information on terrorist activities in Europe.

Contacts between the United States and friendly states in the field of counterterrorist technologies could usefully be expanded. In particular, security practices at airports in Switzerland and Israel are, in many aspects, more advanced than those in the United States. U.S. agencies have, in fact, participated in discussions with officials of both countries, but more exchange of information would be advantageous. Moreover, researchers in other countries, notably Israel, Canada, Australia, and the United Kingdom, have made some technical advances that could be of use to the United States. Much U.S. technology could be made available to friendly states without compromising national security interests.

[5]See U.S. Congress, Office of Technology Assessment, op. cit., footnote 1, pp. 50-51.