Science in an Age of Terrorism

The scientific and engineering communities have responded to the September 11th tragedy with offers to help address the threats to the U.S. homeland and the American people.* Yet, at the same time, concerns about terrorist access to information on weapons of mass destruction (WMD) have generated renewed government concern about the open communication of scientific advances and technological know-how relevant to the development of such weapons. The Department of Defense (DOD), for example, has proposed new rules that would require prior government review of certain nonclassified research deemed critical to national security.† Perhaps in anticipation, a faculty committee at MIT recently recommended that MIT retain its policy barring classified research from the campus but "consider expanding off-campus laboratories to handle expected growth in classified work."‡

Both the new government rules and the universities' responses are strongly reminiscent of the situation that existed during the first Reagan administration, which was in response to Soviet efforts to "vacuum" up unclassified science and technology (S&T) information communicated in the West. The scientific and engineering communities reacted with alarm to those proposals, which would have restricted the dissemination of unclassified basic research results and denied foreign nationals access to "sensitive" research facilities on campuses.

The world political system has changed profoundly in the ensuing 20 years, and with it the nature of the security threats facing the United States and other industrial democracies. Today's primary concern focuses on terrorist groups that might gain access to the materials and know-how necessary to build crude but deadly WMD, rather than state actors. The danger that terrorists might acquire sensitive S&T information differs markedly from state-related threats. Terrorists generally are not seeking to acquire, nor could they readily use, the results of most basic research. In Soviet times, for example, we worried about how to protect the physics knowledge and engineering know-how related to engineering smaller, faster computer chips. Terrorists, however, are neither designing chips nor manufacturing weapons systems on an industrial scale. They typically lack the necessary economic resources, technically qualified personnel, and physical infrastructure.

The domain of science in which acquiring information and technical know-how could directly benefit terrorist organizations is that of biological weaponry. Information that improves knowledge of dangerous pathogens, their safe handling, and their weaponization increases the likelihood that such weapons could be produced covertly on a small scale. It is also important to avoid conveying "hands-on" knowledge of bench-level techniques.

Given these new circumstances and concerns, what principles should guide the communication of S&T information in an age of terrorism? (i) Open access to scientific knowledge on university campuses remains as important today as it was 20 years ago, and the dependence of the U.S. research system on foreign nationals has only grown in the interim. But there is a need for increased vigilance in regulating entry into the United States and access to its research facilities, including some on university campuses. (ii) The areas of scientific knowledge and/or technological application that are immediately applicable to the development of WMD are well known. Because we are not dealing with a broadly capable adversary, advances in most disciplines can be communicated with only minimal restrictions. Work with potential applications to WMD must be subject, however, to a different set of rules; and, as the MIT committee has recommended, may best be undertaken off campus. (iii) Carefully conceived restrictions on scientific and technical communications remain necessary but should be applied to substantially fewer areas of scientific inquiry and technology development than during the Cold War. A generic exception would be communications that permit terrorist groups to "leapfrog" steps in the R&D process, in part by avoiding technical dead ends. (iv) Finally, university faculties have long resisted calls for the adoption of codes of conduct and other efforts to address normative concerns about how foreign nationals use the advanced training they receive once they return home. Those working in sensitive areas must take responsibility for imparting values that emphasize the positive role of S&T in addressing human needs, and the immorality of their use to cause mass casualties and human suffering.

Mitchel B. Wallerstein

Mitchel B. Wallerstein served from 1993 to 1997 as Deputy Assistant Secretary of Defense for Counter-Proliferation Policy and Senior DOD Representative for Trade Security Policy. Before joining DOD, he was affiliated for a decade with the National Academies/National Research Council (NRC), where he directed a number of influential studies on scientific communication, export controls, and national security.

*See, for example, Committee on Science and Technology for Countering Terrorism, NRC, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (Washington, DC: National Academies Press, 2002). †U.S. Department of Defense; *Mandatory Procedures for Research and Technology Protection Within the DoD* (draft, DOD 5200.39-R, March 2002). ‡*Science* **296**, 1949 (2002).