Mitchel B. Wallerstein

Remarks for the NAS/CSIS Meeting on "Scientific Openness and National Security"

January 9, 2003
The National Academy of Sciences

- I am pleased to be able to join you today to discuss this subject, which has been a principal intellectual concern of my mine for more than two decades. Indeed, this meeting about restrictions on science and scientific communications is taking place just more than 20 years after the Corson Panel of the Academies Committee on Science, Engineering and Public Policy (COSEPUP), which I had the privilege of staffing, issued its report on "Scientific Communication and National Security." Thus, in the immortal words of Yogi Berra, this workshop and this issue has a strong sense of "déjà vu all over again".

- The nature of the threat has changed, of course, over the two decades since the Corson panel issued its report, and obviously the *target* of the restrictions is now different—i.e., no longer the former Soviet Union and Warsaw Treaty nations. But the risks to scientific and technological progress and the potential negative externalities inherent in imposing restrictions on the open communication scientific findings remain very similar.

- After working on the Corson report and a number of related studies here at the Academies in the 1980s, I had the privilege—and the responsibility—of managing major aspects of these issues during the five years I spent in the Department of Defense from 1993-1997, where I had responsibility for the formulation of DoD policy on technology security policy and export controls. Even though my time in government obviously preceded the terrible events of September 1lth, I can say that we recognized during the 1990s that there were, indeed, certain areas of science, such as biotechnology, that could be enormously helpful to the so-called "proliferant states," like Iraq and North Korea, as well as to terrorist groups seeking to gain access to mass casualty weapons—or WMD.

- I had forgotten, until I went back recently to review the Corson report, that the Panel had actually *anticipated* the need to consider how restrictions on scientific communication would be different in an era when the principal security threats did not emanate from the Soviet Union and Warsaw Treaty states. This was, however, simply noted toward the end of the report as a subject that the Committee might wish to address in the future.

- Of course, the fact that the threats we worry about today no longer derive from a monolithic adversary, one with considerable S&T capabilities of its own, must alter the calculus of how we *think* about the problem. In Soviet times, we were facing an adversary that, due to the shortcomings of and economic constraints on its S&T infrastructure, undertook a systematic and sustained effort to obtain scientific and technological information from the West. They did so by taking advantage of the open Western S&T community, for example by sending agents to scientific meetings in search of specific pieces of information (or someone who could coopted to supply it), inserting supposed "students" onto university campuses where they could gain access to leading-edge research, and through many other activities, both overt and covert. These efforts were well documented by the U.S. intelligence community, and they were in some cases fairly successful.

- Indeed, in response to this growing threat, in 1981 senior officials in the in-coming Reagan administration began to call—loudly at times—for the compartmentalization of sensitive research on university campuses and the private sector, excluding foreign nationals from all but our closest NATO allies and Japan. This, in turn, caused the leadership of the S&T community, including a number of leading university presidents, to react with alarm—and shortly thereafter, the Academy presidents acted to set up the Corson Panel, under the chairmanship of Dale Corson, the president-emeritus of Cornell University.

- I dwell on this history to make a point: in the Soviet era, we were dealing with a technically sophisticated adversary which, if it was successful in its efforts to gain access to results of sensitive research and analysis, would be able to overcome the gap in fielded weapons systems that gave NATO and the West its technological dominance, which, in turn, maintained the strategic parity between the opposing sides despite the substantial numerical superiority of the Warsaw Pact forces. What

the Academy reports were so critical in pointing out, however, was that, with a few exceptions, it was (and is) not individual widgets or weapons component technology that must be protected, but the *knowledge base* and *technical know-how* necessary to design and build them. This seemingly obvious but important observation applies to virtually every major WMD threat that we face today from nuclear weapons to biological and chemical weapons, and even to more esoteric threats such as cyber warfare.

- Obviously, the most *immediate* concern that is driving the recent legislation and Executive branch actions—including the recent enshrinement in the Department of Homeland Security bill of the term, "sensitive homeland security information" (though few are clear on what this refers to)—is the fear that al-Qaeda and other terrorist groups might be able to gain access to the knowledge and materials necessary to build crude, but nevertheless deadly, mass casualty weapons for use against the U.S. homeland and/or US interests and citizens abroad. But that is not the ONLY reason for being concerned about unrestricted communication of sensitive S&T information. Let me name two others: there continues to be credible evidence that some of the so-called "states of proliferation concern"—especially Iran and Iraq—continue to seek information (and *people*) in the West to help them to develop indigenously nuclear and other weapons of mass destruction. The second concern is about China, which is, of course, already a nuclear weapons state but which is currently in the midst of a major military modernization and possible expansion of its force projection capabilities.

- I would argue, however, that *both* of <u>these</u> threats more closely resemble the old concerns about the Soviet S&T acquisition efforts of the past. We know how to deal with this, and the system of controls and research management procedures currently in place are generally adequate to cope with the problem. But the numbers of Chinese nationals working and studying today in the U.S. S&T infrastructure is very large indeed, and this could once again become a matter of concern if politico-military relations were to deteriorate later in this decade.

- The issue of *terrorist* acquisition of scientific information and know-how is, in fact, of a rather different character than these other threats that have been with us, in one form or another, for the last quarter century. As a general rule, terrorists do not need—nor, in all likelihood, could they

readily make use of—massive volumes of basic scientific knowledge or advanced techniques. In Soviet times, for example, we worried about how to protect the physics knowledge and engineering know-how related to building smaller, faster computer chips, or the extraordinarily complex computer algorithms used in designing the hot sections of high bi-pass jet engines. Terrorists, however, are neither designing nor manufacturing weapons systems. They lack the economic resources, sufficient numbers of technically qualified personnel, and the physical infrastructure to accomplish this task.

- Rather, what they are *intent* on—and apparently quite good at—is constructing (often in ingenious and unconventional ways) a relatively small number of WMDs, most often by acquiring information about the operational and design characteristics of such weapons. But the question we must consider is whether further restrictions on the communication of scientific information or on the access by foreign students to the US research system would do anything to significantly impede terrorist acquisition of WMD?

- In my view, the principal area of science where the acquisition of information and technical know-how could directly and substantially benefit terrorist organizations and proliferant states is the one that is the focus of this workshop—namely, biological science. Clearly, the communication of information that helps improve knowledge about dangerous pathogens, their effects, how they may be handled safely, etc. increases the likelihood that such weapons can be manufactured covertly on a small scale. It has been an informal rule of thumb since the cold war times that the narrower the gap between the acquisition of new scientific knowledge and efforts to embody that knowledge in technical applications, the greater the likelihood of the unintended transfer of potentially dangerous technology or technical know-how.

- Biotechnology/BW threats are of extraordinary concern for another reason as well: it does not require a huge investment in physical infrastructure or large numbers of highly trained researchers to achieve modest success. The experience of the Aum Shinrikyo cult in Japan in instructive in this regard. The AS was really the first terrorist organization outside of the United States (there was at least one inside as well) to attempt to acquire both CW and BW. After the arrest and break-up of the cult, which unfortunately did not occur until *after* the sarin

attack on the Tokyo subway and after some less successful (and not as well publicized) efforts to develop biological weapons as well, the authorities found and explored the AS R&D facility near Mt. Fuji. What they found was shocking: the cult had recruited to its ranks a small number of chemical engineers and life scientists, who were at work developing and testing CW and BW. (Investigators even discovered subsequently that the Aum had rented an abandoned sheep station in western Australia to test the weapons it had developed.) All of this, including the acquisition of equipment, precursor chemical and pathogens, etc. was financed entirely by the sect. But the key to their success was the successful recruitment of a small cadre of individuals with sufficient technical training and knowledge.

- So, where does all of the foregoing lead regarding the development of *present-day* principles for determining whether or not S&T information should be kept (or made) secret for security reasons? Having observed and worked on the problem from both within and outside of the government, I conclude that:

    1. Rational and well-conceived restrictions do remain necessary, but they can and must be applied to a substantially smaller number of areas of scientific inquiry and technology development than in the cold war days. There is simply no longer a rationale for a large, over-reaching list of controlled items and subject areas.

    2. In fields such as bio-technology, the publication of information that conveys *technical know-how* (i.e., what some would call the "recipe" of how to do things at the laboratory bench level) should be carefully considered and avoided. It is worth noting, in this regard, that as the Corson panel noted, it is often very difficult to transfer such know-how unless qualified scientists can gain "hands-on" experience at the bench level.

    3. Openness and unfettered access to scientific knowledge on university campuses remains as vitally important today as it was 20 years ago. On this point, the Corson panel surely had it right—and the dependence of the US research system on foreign national students, post-docs and faculty has only grown in the interim. But this does not mean that we cannot devise ways to be more vigilant about who is permitted to gain entry to our country and to our

research facilities. The experience with the September 11th hijackers is that they hid in plain sight in our communities before carrying out their deadly violence. Thus, sad to say, universities and private research enterprises must devote considerably greater effort to reviewing the backgrounds of foreign nationals whom they admit for graduate training or hire in their laboratories, and the Government will need to work even more closely with the universities and private sector in determining who should be granted a visa for study or work in the United States.

4. The areas of scientific knowledge and/or technological application that are immediately germane to the development of WMD are well known at this point. Because we are not dealing with an adversary that is capable of broadly vacuuming up knowledge or know-how, advances in many—perhaps most—disciplinary areas can be discussed and communicated with little or only minimal restrictions. Unfortunately, however, those areas or sub-disciplines of the life sciences that are associated with the development of biological weapons must continue to be subject to a *different* set of rules. As also recommended by the Corson Panel, as well as by a number of other studies, such work may best be undertaken at off campus facilities where the matter of excluding foreigners, when necessary, is perhaps more manageable.

5. That said, the *essence* of the scientific enterprise remains the rapid publication (whether physical or virtual) and dissemination of new results and ideas. As repeated studies have concluded, we will be damaging the very capability that has made us the world's leading techno-scientific power if we allow our new security concerns to damage or impede this process. Nevertheless, in those areas of the life sciences where the open and rapid publication of research results may have direct application to the design of biological weapons, will improve the hands-on "know how" of how to handle dangerous pathogens, or may help a terrorist organization or proliferant state to avoid long and costly dead-end lines of research, or overcome other technical obstacles, a *modest* delay before communication for the purposes of security review would not be inappropriate. Especially for research that is <u>not</u> undertaken with federal funding, I can imagine such a review conducted

voluntarily by a duly constituted body of the life sciences community.

6. Fortunately, terrorist organizations continue have difficulty purchasing so-called "enabling" technology, such as sophisticated laboratory measurement equipment, containment devices, etc. Nevertheless, it is essential that the USG and the equipment manufacturers remain vigilant regarding the end-user(s) of transferred technology.

- Before concluding, I want to comment briefly on two other aspects of the problem. First, there is the legitimate question of what the US can realistically expect to accomplish on its own? To state the obvious, the United States research system is clearly not the only place where important life sciences research is underway, research that may be of interest to terrorists and the agents of proliferant states. The research infrastructure of the European Union, Japan and certain other advanced states have institutions that are capable of producing and disseminating such information. Thus, despite a number of highly regrettable unilateral actions taken by the USG in the last year, limitations on the communication of sensitive S&T information can only work if they are adopted *multilaterally*. This is a matter requiring urgent attention, and perhaps an international expert meeting.

- Finally, and without wishing to end on a controversial note, it has been true since the cold war days that, quite frankly, universities have sought to have it both ways—seeking large amounts of public funding for the conduct of basic and applied research, while at the same time resisting periodic calls for the adoption of 'codes of conduct' and other efforts to address normative concerns about how foreign nationals use their advanced training and knowledge when they return to their own countries. This apparent contradiction has continued to perplex me over the years. It would seem today, more than ever, that faculty, research staff and administrators responsible for managing work in sensitive research areas must step up to their responsibility to be vigilant about the motivations and intentions of their students and co-workers and to impart a value structure that emphasizes the *positive* role of science and technology in advancing interests and

needs humanity, rather than its use to cause mass casualties and human suffering.