Scientific Communication and National Security in 1984

Mitchel B. Wallerstein

In recent years, U.S. national security has come to depend increasingly on lead time over its adversaries in areas of high technology—that is, areas in which technological progress is closely related to advances in basic science. Many of these technologies (for example, high-speed electronics and computer-based encryption techniques) have commercial as well as military applications. This has led some in the past and current administrations to fear that the open U.S. research community could become a source of militarily significant technology to the Warsaw Pact.

Summary. The federal government's concern about maintaining the lead of the United States over the Soviet Union and its allies in militarily critical technology has led it to attempt to control unwanted technology transfer. Its attempts have extended to control of open scientific communication as well as the transfer of physical devices and blueprints. In 1982, the Corson Panel (an independent ad hoc committee) reviewed the evidence on the costs and benefits of controls and suggested guiding principles for government policy. This article examines the major policy developments since the Corson Panel completed its work. The stringency and the reach of government restrictions, either proposed or in force, go considerably beyond the panel's recommendations.

Such concerns were reflected both in policy proposals and public pronouncements aimed in part at the scientific community. Public statements in early 1982 included warnings by senior officials in the Department of Defense, the Department of Commerce, and the Central Intelligence Agency that Soviet military intelligence might find easy access to sensitive information through what one called the "soft underbelly" represented by the American academic community (*1*).

Conflicting Perspectives on the Problem

There are sharply differing views within our society regarding the extent of technology loss and the best solutions to the problem. Some interests speak with a louder and more effective voice than others in terms of the formulation of Administration policy, recognizing that there is a good deal of overlap in the emphasis accorded by each.

Clearly, what lies at the heart of public debate is concern over the loss of military advantage the United States might suffer if it does not block the efforts of the Soviet Union and its allies to gain access to Western science. Some who are concerned with national security believe the speed and seriousness of this technology transfer require new policies and reassessment of current regulations. The concern here is really twofold. First, by targeting Western research, the Warsaw Pact countries avoid a large part of the massive R & D investment the United States has committed to the development of sophisticated military systems. Second, the nature of the research process in nonclassified settings has changed, with the result that universities in particular are now becoming increasingly attractive targets for foreign intelligence efforts. Those sharing this concern argue that the imposition of limited controls is preferable to classification, which would remove such work entirely from the campus. They suggest that, when universities choose to accept the presence of defense-related research on campus, for whatever mix of intellectual and economic motivations, controls must be considered part of the price.

A second perspective focuses on the critical importance of maintaining vigorous, open scientific communication both within the borders of the United States and across international boundaries. According to this view, even limited restrictions on the free flow of information affect feedback, delay the discovery of errors and duplication, hinder critical evaluation of scientific efforts, and, as a result, undermine the pace of scientific discovery. The price of achieving short-term security by restricting the communication of ideas and information would be the pace and effectiveness of both our research effort and the transfer of that research into application. This perspective argues, in sum, that secrecy about existing knowledge can never replace the development of new ideas as a means of protecting national security.

Those adhering to this view also suggest that openness pays dividends of other kinds. For one thing, U.S. efforts to limit the flow of information by restricting scientific exchanges with the Soviet Union inevitably will limit the flow of information from them to us. Not only does American science benefit from these interactions, but it can also be argued that for intelligence purposes they help gauge accurately the state of Soviet scientific advancement.

A third perspective focuses on the educational impacts of restrictions on access to and dissemination of scientific and technological information. Here again there are two separate arguments. First, those who provide advanced scientific and technical training point out that it is functionally impossible to separate completely education from research activities. Moreover, if the only experience a young scientist or engineer gains is in the classroom, rather than the laboratory, the next generation of American investigators will be substantially less prepared to maintain the superior levels of productivity and achievement that have characterized the U.S. scientific effort since World War II.

But there is another important dimension to the educational perspective: the cost to the U.S. academic system of excluding foreign nationals from sensitive areas of science and technology. The number of foreign students in higher education in the United States increased substantially during the 1970's, at both the undergraduate and graduate levels. Among the factors underlying this trend were increased foreign demand and increased recruitment of foreign students by U.S. institutions in order to augment domestic enrollment (Fig. 1). The data

Mitchel B. Wallerstein is special assistant for policy and planning in the Office of International Affairs of the National Research Council, Washington, D.C. 20418. He previously served as principal staff consultant to the Corson Panel on Scientific Communication and National Security.

are even more striking at the postdoctoral level (Fig. 2). The postdoctoral sector is particularly significant because it is a major source of junior faculty and research talent in many American universities.

A fourth major view is that expressed by private industry. Many leaders of U.S. technology-based industries have argued that if industries are to adapt to rapidly changing business conditions, they must have access to scientific and technological information from all parts of the world. Beyond the loss of information, industrial leaders express concern about other economic impacts resulting from a lack of openness, including regulatory costs, loss of sales, loss of reliability as a trading partner, and reductions in the pace of innovation.

A fifth voice in the debate may be characterized somewhat broadly as the constitutional and cultural perspective. Many concerned about the continued vitality of the American political system believe it can flourish only in an atmosphere of openness. First, they point out that fundamental constitutional questions may be raised when the government seeks to restrict the rights of citizens to speak or to publish. It is argued that freedom of speech is not just a legal right, it is essential to the maintenance of an informed electorate. Second, it is suggested that visits by Soviet and East European scientists expose them to the U.S. culture and political system which, over time, may contribute to political and social change within the Warsaw Pact.

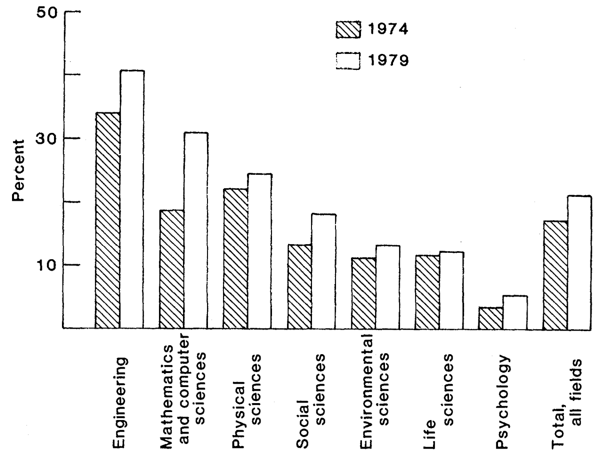

Fig. 1. Percentage of foreign students in full-time, graduate science and engineering programs in doctorate-granting institutions, 1974 and 1979 (*16*).

Key Findings and Recommendations of the Corson Panel

In spring 1982 discussions between representatives of the National Research Council and the DOD led to the establishment of an ad hoc panel of the Committee on Science, Engineering and Public Policy (COSEPUP), chaired by Cornell University president-emeritus Dale R. Corson. The panel included scientists, former defense and national security officials, and research administrators in industry and universities (*2*). Its mandate was to examine the evidence of technology leakage and methods for controlling it, and to seek policy measures by which the competing national goals of national defense and intellectual freedom could be accommodated satisfactorily.

After reviewing evidence on the benefits and costs of control measures, the panel concluded that a national strategy of "security by secrecy" would weaken American technological capabilities, because there is no practical way to restrict international scientific communication without also disrupting domestic scientific communication. A national strategy of "security by accomplishment"—one that emphasizes protecting the U.S. technology lead by promoting scientific productivity—has far more to recommend it (*3*).

The panel heard extensive briefings by the intelligence community, some at high levels of classification. While noting that the available evidence left much to be desired, the panel reported that it had found no case of significant damage to security associated with research dissemination (*3*, pp. 13 and 41). The panel also added two caveats. First, it observed that the evidence on leakage and the associated damage to U.S. security was still only fragmentary and anecdotal, in part because the problem had only recently been identified (*3*, p. 14). Second, it pointed out that Soviet intelligence efforts were extensive and that universities and other research sites were indeed targeted. It also noted (but took no position on) intelligence community arguments that research facilities are likely to be more heavily targeted in the future (*3*, p. 21).

The panel suggested that the class of research information of greatest potential concern is not the explicit findings in research reports but rather know-how—the detailed understanding of equipment use or operational procedures normally gained only by direct participation in a research project (*3*, p. 42). It follows that protection of sensitive research information is achieved better by preventing sustained access to research projects than by preventing dissemination of written research reports.

The Corson Panel examined five types of control mechanisms: (i) classification, (ii) export control regulations, (iii) controls on foreign visitors, (iv) restrictions on government contracts, and (v) voluntary prepublication clearance. Its general review of these mechanisms led the panel to two broad conclusions:

1) Where controls are deemed necessary, the government should use contract restrictions in preference to export control regulations. The contract mechanism has the advantage of informing a researcher of his or her obligations in advance while leaving application in the hands of the most technically qualified government personnel. Export controls, devised for controlling the movement of tangible objects, are ill-suited to the control of information flow.

2) The government's effort is uncoordinated and spread too broadly across too many diverse technologies to be practicable. An effort spread this thin cannot be effectively administered, and it raises unnecessary fears among researchers working in areas with no military relevance. The panel suggested that the government adopt a strategy of building "tall fences around narrow areas"; contract controls, for example, should be restricted to a few gray areas that justifiably cannot be either classified or completely open. It defined such technologies as those in which all of four criteria apply (*3*, p. 49).

- the technology is developing rapidly, and the time from basic science to application is short;
- the technology has identifiable direct military applications; or it is dual-use and involves process or production-related techniques;
- transfer of the technology would give the U.S.S.R. a significant near-term military advantage; and
- the United States is the only source of information about the technology, or other friendly nations that could also be the source have control systems as secure as ours.

The Corson report was released on 30 September 1982, and it was received favorably by top Administration officials, university administrators, and other members of the U.S. science policy community.

The Situation in 1984

More than 18 months have elapsed since the Corson report was issued. Much of the hope that surrounded its release has faded and there have been at least four attempts to formulate a new policy:

1) An interagency review of the Corson report's implications has yet to be completed. The effort began with National Security Study Directive 14-82 (now renumbered as NSSD 1-83), which was signed by President Reagan and issued by then National Security Advisor William Clark in December 1982. The terms of the review have twice been altered, and there have been multiple changes of personnel at the Office of Science and Technology Policy (OSTP), which is responsible for coordinating a major section of the report. In addition the study has been conducted at the classified level without the benefit of outside input. It is not known how the product, reportedly near completion, compares in scope or substance with the effort originally requested by the President. OSTP officials see an advantage in the release of some sort of unclassified document, but they are unsure as to either the date of its public availability or its comprehensiveness.

2) Given the delays in the interagency policy review, the Department of Defense (DOD) has moved to complete an internal policy review that was begun in 1981. Accordingly, a Steering Committee on Technology Transfer was established within DOD to focus on contracts, visa controls, emerging technologies, scientific conferences, publications, and rules for exemption to the Freedom of Information Act. The work of the Steering Committee and its subpanels has now been largely completed and its recommendations are being implemented.

3) A provision included in the 1984 Defense Authorization Act permits the Secretary of Defense to protect certain kinds of unclassified technical data in the possession or under the control of the DOD that otherwise would be subject to release to foreign nationals under the terms of the Freedom of Information Act. Additional proposals have been circulated within the DOD to seek broader authority to protect sensitive technical data produced by other federal agencies (for example, NASA or the Department of Energy) by facilitating their transfer to DOD control.

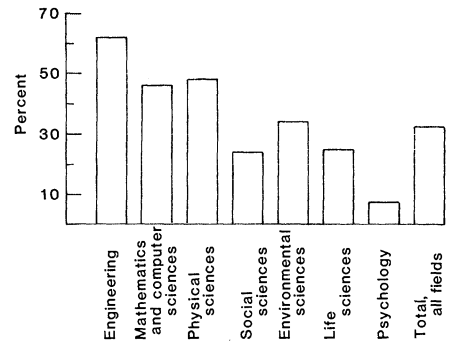

Fig. 2. Percentage of foreign postdoctoral researchers in science and engineering programs in doctorate-granting institutions, 1979 (*16*, p. 21).

4) A Presidential directive, "Safeguarding National Security Information" (NSDD 84), was issued in March 1983. That directive would have required both government officials and those under contract to the government with access to sensitive compartmented information, which is information classified at levels above top secret, to submit for prepublication clearance anything they write that bears upon national security matters. The directive was withdrawn in February 1984 after substantial opposition arose in the Congress and among the general public.

While the various intra- and interagency policy studies have been under way, a series of incidents have occurred over the past 16 months similar to those that provided the original impetus for creation of the Corson panel. The principal distinction between now and the pre-Corson environment is that most of the incidents relate to the withdrawal of papers from meetings, rather than the denial or restriction of visas or other restrictions.

The Development of Controls

Since the early 1940's, the federal government has added steadily to the means by which it can prevent—or at least slow—the loss of militarily sensitive scientific information. For example, the government has the authority, established through a series of executive orders, to impose security classification on sensitive research conducted by its own employees or undertaken by private parties at public expense. The Executive Branch has also been assigned a substantial amount of legislative authority over the years through which it can attempt to control all aspects of scientific communication.

The Atomic Energy Act of 1946, for example, precluded public dissemination of most of the results of the Manhattan District Project or subsequent atomic research, particularly through a "born secret" provision that automatically classifies research on atomic energy at its creation. The government has also been able to use the authority vested in export control legislation to limit the release of products, processes, and technical data to potentially adversary nations. The Export Control Act of 1949, which has been renewed since 1969 as the Export Administration Act, required the Department of Commerce to prevent the export of goods that might enhance either the economic or military potential of communist countries. The Export Administration Act is implemented through the Export Administration Regulations and through a comprehensive list of products and processes known as the Commodity Control List. Since 1979, the Department of Commerce administrators have also relied for guidance on the Militarily Critical Technologies List, which is prepared by the DOD and based on a 1976 report of the Defense Science Board, commonly called the Bucy report (*4*).

Another method of controlling the export of security-related data is the Arms Export Control Act of 1976. This Act is implemented by the Department of State through the International Traffic in Arms Regulations. These regulations control the export of military systems, including technical data relating to the "design, production, manufacture, repair, overhaul, processing, engineering, development, operation, maintenance or reconstruction . . . of implements of war on the U.S. Munitions List" or "any technology that advances the state of the art or establishes a new art in any area of significant military applicability" (*5*).

In order to control the movement of militarily sensitive goods at the international level, the Coordinating Committee for multinational export controls (CoCom) was established by informal agreement in 1949. It comprised all the NATO countries except Iceland and Spain, plus Japan. CoCom has provided a forum for the voluntary coordination of trade controls on exports to the Warsaw Pact countries. The United States is currently engaged in efforts to strengthen the effectiveness of the CoCom mechanism.

An Update of the Key Issues

Evidence on the extent of technology leakage. Knowledge about technology leakage and its effects on national security has not changed significantly in the 18 months since the Corson Panel was briefed by the U.S. intelligence community (*6*). In recent months the principal activity has been the identification of the ways in which technology leakage can occur so that a comprehensive control effort can be fashioned. No major initiative has been undertaken to better characterize the relative importance of sources, channels, or types of information that leaks out or the relative significance of scientific communication within the large picture. The intelligence community reports no cases during this period in which loss through the U.S. scientific community has led to identifiable damage to national security. However, intelligence officials remain concerned about the small percentage of Soviet intelligence acquisitions that involve the American research community.

Classification controls. There is now better information on the extent to which military research is classified or otherwise restricted. As part of the report of its subcommittee on publications, the DOD Steering Committee on National Security and Technology Transfer determined how publications in federal information centers were classified or disseminated in terms of their subject area or source (Tables 1 and 2).

The data support the contention that universities are responsible for less sensitive research than is done in other settings, no matter what field of technology is involved. The study also found that all classified reports from universities and approximately 50 percent of the limited reports from universities were generated in off-campus facilities affiliated with the universities. Meanwhile, through Executive Order 12356, issued in April 1982, the Administration changed the thrust of its classification policy, stating that restrictions are to be imposed in all cases where reasonable doubt exists about the need for classification. It also expanded the number of categories of potentially classifiable information and made it possible to reclassify information previously made public.

Export controls. The Export Administration Act, and the attendant Export Administration Regulations (EAR), remains the principal regulatory instrument for controlling the flow of sensitive technical data, particularly that of a proprietary nature across our borders. The Export Administration Act came up for renewal during the first sessions of the 98th Congress. Bills were passed in both Houses early in the second session, with the Senate version tending to be more restrictive than that of the House. A conference version of the Export Administration Act of 1984 is expected before the end of the current session.

While the language of the new export act has been debated, the Administration has proceeded with vigorous efforts to control unwanted technology transfer. It can be stated that, in general, the Department of Commerce presently considers scientific communication to be a relatively small—albeit significant—aspect of the overall technology control problem. Since 1982 the EAR have not been invoked to prevent the dissemination of the results of academic research. On the other hand, modifications to the technical data regulations under consideration for incorporation into the EAR could significantly alter this situation. If implemented, they would eliminate the general licensing exemption granted to some "scientific and education data." They would also require a validated license for the export of virtually all "critical technical data," a new term identified in the draft wording, which is not publicly available. Since the definition of "export" in this draft includes presentation of papers at symposia where foreigners were present, the hiring of a foreign researcher, and so on, the proposed rules, if adopted, would have a significant impact on U.S. scientific intercourse.

The Administration has also stepped up its export control enforcement effort, principally through two channels. The first, Operation Exodus, is an effort by the Customs Service since late 1981 to spot-check high-technology goods being readied for shipment. It has resulted in the detainment and seizure of some 2300 foreign-bound shipments worth approximately $149 million and eventual indictments in 221 cases, only 28 of which involved so-called dual-use technology (*7*). The second effort to enforce controls involved creation of a new post within the Department of Commerce, known as the Office of the Deputy Assistant Secretary for Export Enforcement, which referred 37 dual-use technology export cases to the Justice Department for prosecution in fiscal 1983 (*7*). This two-track approach reflects uncertainty between the Customs Service of the Treasury Department and the Export Administration of the Department of Commerce over which agency has lead responsibility for export enforcement.

The other principal export control

Table 1. Distribution restrictions on DOD reports by source, 1979 through 1983 (*13*).

Source	Total	Classified (%)	Limited (%)	Public (%)
DOD laboratories	61,694	12	44	44
Universities	23,119	1*	4	95
Industry	32,806	21	35	44
Nonprofit	5,609	17	15	68
Total	123,228	13	33	54

*Generated at research institutes associated with universities.

Table 2. DOD reports withheld from public release, by subject (13).

Field	Total	Classified (%)	Limited (%)	Public (%)
Missile technology	2,524	57	32	11
Ordnance	6,740	32	47	21
Military sciences	8,099	38	33	29
Navigation, communication, detection and countermeasures	13,490	40	28	32
Aeronautics	5,082	13	53	34
Propulsion and fuels	3,252	14	48	38
Space technology	905	17	44	39
Nuclear science and technology	1,259	24	34	42
Energy conversion (nonpropulsive)	1,055	3	54	43
Electronics and electrical engineering	12,424	3	50	47
Materials	5,643	1	46	53
Methods and equipment	2,288	3	42	55
Agriculture	82	1	44	55
Mechanical, civil, industrial, and marine engineering	9,284	5	35	60
Biological and medical sciences	10,093	1	32	67
Physics	12,812	6	25	69
Behavioral and social sciences	10,529	2	20	78
Earth sciences and oceanography	4,671	1	21	78
Atmospheric sciences	3,078	1	16	83
Chemistry	4,042	—	14	86
Astronomy and astrophysics	584	—	13	87
Mathematics	5,292	—	5	95

mechanism is the Arms Export Control Act and the attendant International Traffic in Arms Regulations (ITAR). Revision of the ITAR, which has been pending for more than 2 years, still has not been completed, although a draft of the revised regulations is now said to exist. A likely target period for release of a new ITAR is mid-to-late 1984. The ITAR is administered by the State Department on the basis of the Munitions Control List, which is maintained by the DOD. However, there appear to be no instances in which the ITAR has been applied to written or oral scientific communication since the release of the Corson report.

Controls on foreign visitors. In May 1983, after an interagency review, Under Secretary of State William Schneider announced a new visa policy for handling cases of individuals suspected of technology acquisition. Schneider essentially reaffirmed that the existing visa law can and should be used to limit the loss of information obtained by foreign visitors. Moreover, he indicated that action may now be taken on a visa solely on the basis of a visitor's potential to be a source for technological loss. Therefore, depending on the nature of the risk identified, an applicant may be (i) denied a visa, (ii) offered a conditional visa, or (iii) given an unconditional visa. In cases of conditional visas, the restrictions may be imposed either by the relevant department or by the Immigration Service of the Department of Justice—outside of the visa process—as a condition of entry.

The State Department's principal concern is commercial trade visits, with only secondary attention paid to those involved in academic research. Again, depending on the assessment of the risk involved, a sponsor may be asked to modify a visitor's program, or alternatively, the visitor's freedom to travel may be restricted. Because the Visa Bureau does not track technology transfer cases per se, it is not possible to provide a quantitative assessment of scientific visits approved, denied, or made conditional. However, Table 3 provides an indication of the trend in advisory recommendations made between 1981 and 1983 by COMEX, the interagency Committee on Exchanges. This period may be somewhat anomalous, due to rising tensions with the Soviet Union and East Europe over Poland and other matters, but the data reveal (i) a decline in the total number of cases reviewed, (ii) a slight decline in the percentage of cases in which significant concern was expressed, (iii) a decline in the percentage of cases recommended for program denial, and (iv) an increase in the percentage of cases recommended for program modification. COMEX recommendations are not necessarily adhered to by the State Department, but they prevail in a majority of the cases.

Table 3. COMEX recommendations for visiting scientists' programs, 1981 to 1983 (*14*).

Programs recommended	1981	1982	1983
For approval	92	56	33
For approval with modification	225	57	133
For denial	55	35	28
Total	372	148	194

An interesting aspect of the visa and scientific exchange matter involves the People's Republic of China. The COMEX data reveal that between 11 and 25 percent of the cases from 1981–1983 in which significant concern about technology loss was expressed by the committee involved Chinese students or scientists. But, because visa and export control policies toward the People's Republic have been liberalized substantially, none of the COMEX recommendations for program denials involved the Chinese. The programs of some visiting Chinese were, however, modified.

Contract controls. The Corson Panel recommended that where controls on unclassified scientific information are warranted, they can best be accomplished by means of a priori contract constraints. This mechanism was examined by the DOD Steering Committee on National Security and Technology Transfer, and a new policy has emerged on "international transfers of technology, goods, services and munitions" (DOD directive 2040.2) (*8*). This directive articulates a number of new mechanisms for establishing standard definitions of what is militarily sensitive and for resolving appeals of contractually imposed restrictions. It also establishes the Panel on International Technology Transfer, as the highest level appeal mechanism for resolving differences within the DOD on technology transfer policy, and it creates two subpanels: (i) Export Control Policy—a first-level appeal structure for resolving differences on export control policy matters, and (ii) Research and Development—a first-level appeal structure for resolving differences on technical standards, definitions, and the dissemination and exchange of technical information, including appeals of "technology transfer research cases."

With regard to sensitive research undertaken in academic settings, the DOD Steering Committee has made a number of additional recommendations. First, it has clarified its policy on review of research papers produced by DOD contractors, distinguished by budget category and the nature of the research (Table 4). The point of these policies is to give the researcher written notice of review procedures before he or she signs a DOD contract.

Two aspects of Table 4 merit special attention: (i) the 60-day prior review requirement for basic research is more restrictive than recommended by the Corson Panel, which called for simultaneous review by the publishers and DOD, and (ii) the 90-day prior review and right to require changes for sensitive exploratory research or development are also far more restrictive than the Corson Panel's recommendation of simultaneous review for both basic and applied research.

In addition, the DOD Steering Committee has recommended the permanent implementation of a series of six dissemination-control stamps, already approved on an interim basis by Secretary of Defense Caspar Weinberger, that clarify the standards used in circulating unclassified documents produced through DOD contracts (or at government laboratories) and held by the Defense Technical Information Center (DTIC) and other secondary distribution facilities (*9*).

Finally, COMEX is updating an existing DTIC database in order to inform researchers of each other's work and to determine quickly the number and type of DOD contracts in force on a given university campus plus their level of classification or restriction.

Voluntary prepublication review. An agreement for voluntary submittal of papers for simultaneous review by the National Security Agency (NSA) and professional journals, developed by the Public Cryptography Study Group of the American Council on Education and the NSA, appears to be working in a manner that is reasonably satisfactory to all parties. The NSA reports that 200 papers have been submitted for review since completion of the agreement. Of this total, nine papers have been challenged, six have been modified, and three have been withdrawn. Pursuant to the agreement, a six-member appeals committee has been established, consisting of four academic researchers and two former NSA officials. To date, there have been no appeals of the NSA review decisions (*10*).

Implementation of gray area criteria. Perhaps the most important recommen-

Table 4. Review policy for research papers produced by DOD contractors (*15*).

Budget items	Nonsensitive research	Sensitive research
Basic research*	Simultaneous submittal to contract officer and to publisher. DOD has no right to require changes or to restrict publication.	Manuscript must be submitted to contract officer 60 days prior to submittal to publisher. Researcher retains option of whether or not to publish.
Exploratory research and advanced technological development†	Same rules as for basic research.	Manuscripts must be submitted to contract officer 90 days prior to submittal to publisher. DOD retains the right either to require changes before allowing publication or to block publication outright.

*DOD budget category 6.1. †DOD budget categories 6.2 and 6.3.

dation of the Corson Panel concerned the need to build tall fences around narrowly circumscribed technologies that could be identified as meeting the four principal criteria set forth in the report. Pending the public release of the interagency NSSD report, which was coordinated by the OSTP, it is impossible to determine with certainty the extent to which these recommendations have been adopted as official policy.

There are indications, however, that the government is moving toward the adoption of a broader approach than was recommended by the Corson report. Consider the following factors: (i) there has been little progress in streamlining the Militarily Critical Technologies List; (ii) a new, unclassified Militarily Significant Emerging Technologies Awareness List (METAL) is being created that will identify for purposes of monitoring certain frontier technologies just appearing on the horizon but not yet embodied (*11*); (iii) the definition of "threat assessment factors" proposed to the DOD Steering Committee on National Security and Technology Transfer for identifying militarily significant emerging technologies are substantially more comprehensive than the Corson Panel criteria; and (iv) continuing efforts are under way within the Coordinating Committee for multinational export controls to identify additional technologies that are to be proscribed or restricted for export to Warsaw Pact countries.

Conclusions

This review of the current status of scientific communication and national security suggests three major conclusions.

1) The government has not found it possible to act in a manner compatible with the major principles set forth in the Corson report. Although the DOD appears to be implementing the panel's recommendation that the best form of control is the research-funding contract, both the stringency and the reach of restrictions either proposed or in force go considerably beyond the panel's recommendation. Moreover, if the draft wording for new technical data regulations were incorporated into the EAR, then export controls could come to supplant DOD-imposed contractual restrictions as the principal mode of control contrary to recommendations of the Corson Panel.

2) The continuing lack of effective government-wide coordination raises important risks, including (i) disparate agency policies that do not adequately balance national goals, (ii) wasteful allocation of national resources among programs of varying effectiveness, and (iii) confusion and skepticism in the research community. Given the successive delays in the National Security Council review, policy initiative has reverted back to the individual agencies (most notably DOD), whose missions typically reflect only one among the many relevant national objectives. Once put into place, these uncoordinated initiatives will be difficult to adjust. The government's lack of central coordination also represents a missed opportunity to set reasonable priorities among the many offices (OSTP counted 44 of them) responsible for addressing the many parts of the technology transfer problem. There is a danger that the lack of effective government-wide coordination will undermine the perceived legitimacy of government programs among the research community.

3) There is little progress toward an objective understanding of the technology leakage problem and the effects of control measures. This research failed to demonstrate any improvement in knowledge about the actual effectiveness or adverse effects of control on scientific communication.

One feature that makes the policy dilemma in this area particularly difficult is that the costs of being wrong, which are potentially great, accrue only after a delay and in ways that are difficult to measure accurately in the short term. If U.S. controls on scientific communication are too lax, the extensive Soviet intelligence effort may obtain at relatively low cost information not otherwise accessible. Even then, however, it may be difficult to determine precisely how the transferred data have contributed to the Soviet military posture. On the other hand, excessively tight controls may have effects that, while subtle and indirect, are also pervasive. Perhaps the largest risk in this regard is the long-term changes that controls are likely to cause in the demographic distribution of scientists and engineers among the various disciplines and subfields.

The threatened or actual government intervention has already had an impact on the number of papers put forward for publication or presentation at conferences in certain fields (*12*). If the present climate of uncertainty continues, we may witness an increasing migration of the best minds away from those areas of science and engineering where controls are (or may be) imposed—the very fields where new talent is most critical to U.S. technological lead time. Furthermore, if the United States acts to restrict further the flow of people and ideas in frontier areas of science and technology, other advanced industrialized countries may find it necessary to do the same. In this respect, to the extent that U.S. national security continues to rely on technological superiority, by disrupting the invisible colleges, the channels of informal communication that speed the pace of innovation and scientific discovery, the nation may risk sacrificing its best hope for continued long-term security in the belief that controls are necessary to maintain short-term strategic advantage.

References and Notes

1. B. R. Inman, "National security and technical information," paper presented at the Annual Meeting of the AAAS, Washington, D.C., 7 January 1982; L. J. Brady, "Taking back the rope: Technology transfer and U.S. security," statement before the Association of Former Intelligence Officers, 29 March 1982; F. Carlucci, *Science* **215**, 140 (1982).
2. The members of the Panel on Scientific Communication and National Security were Dale R. Corson (chairman), Richard C. Atkinson, John M. Deutch, Robert H. Dicke, Edward L. Ginzton, Mary L. Good, Norman Hackerman, James R. Killian, Franklin Lindsay, Richard A. Meserve, Wolfgang K. H. Panofsky, William J. Perry, Samuel C. Phillips, Alexander Rich, John D. Roberts, Harold T. Shapiro, Charles P. Slichter, Michael I. Sovern, and Elmer B. Staats.
3. Committee on Science, Engineering, and Public Policy, National Academy of Sciences, National

Academy of Engineering, Institute of Medicine, *Scientific Communication and National Security* (National Academy Press, Washington, D.C., 1982), p. 45.
4. Defense Science Board Task Force on Export of U.S. Technology, *An Analysis of Export Control of U.S. Technology—A DOD Perspective* (U.S. Department of Defense, Office of the Director of Defense Research and Engineering, Government Printing Office, Washington, D.C., 1976).
5. International Traffic in Arms Regulations, section 125.101.
6. This assessment is based on briefings at the Top Secret level of classification, which the author received from the interagency Technology Transfer Intelligence Committee (composed principally of representatives from the Central Intelligence Agency, Defense Intelligence Agency, and Federal Bureau of Investigation) and the National Security Agency, in January 1984.
7. J. Zonderman, "Policing high-tech exports," *New York Times Sunday Magazine*, 27 November 1983, p. 103.
8. C. W. Weinberger, "International transfers of technology, goods, services, and munitions," DOD directive 2040.2, 29 December 1983.
9. The range of classifications is as follows: (i) release only on approval of originator; (ii) release within DOD only; (iii) release to DOD and DOD contractors (who must apply for formal approval) only; (iv) release to U.S. government only; (v) release to U.S. government and U.S. government contractors only; and (vi) release to the general public. This system will replace the previous arrangement that allowed only two options: public release or U.S. government only.
10. Office of Policy, National Security Agency, personal communication, 15 March 1984.
11. Creation of METAL was recommended by the subcommittee on the monitoring of emerging technologies of the DOD Steering Committee on National Security and Technology Transfer. The subcommittee urged the establishment of an unclassified watchlist to which a technology might be assigned during the period that it was still at the stage of basic research. Subcommittee on monitoring of emerging technologies, "Report to the DOD steering committee on national security and technology transfer," Department of Defense, Washington, D.C., 29 December 1983.
12. The Fusion Technology Division of the American Vacuum Society reports the following statistics on papers presented at its meetings: 78 papers in 1981, 58 papers in 1982, and 35 papers in 1983; Office of Public Affairs, American Physical Society, personal communication, 29 December 1983.
13. Steering Committee on National Security and Technology Transfer, "Report of the subcommittee on publications," Department of Defense, Washington, D.C., 9 November 1983, pp. 23 and 24.
14. From data provided by the interagency Committee on Exchanges, Technology Transfer Intelligence Committee, 5 January 1984.
15. Office of Research and Laboratory Management, Deputy Under Secretary of Defense for Research and Engineering, personal communication, 20 December 1983.
16. Division of Science Resource Studies, *Foreign Participation in U.S. Science and Engineering Higher Education and Labor Markets* (NSF-81-316, National Science Foundation, Washington, D.C., 1981), p. 5.
17. I thank Lawrence E. McCray for his thoughtful contributions to this article, and also for their helpful comments Dale R. Corson, Rosemary Chalk, Ruth L. Greenstein, Allan R. Hoffman, John M. Logdson, Richard A. Meserve, Robert L. Park, Victor Rabinowitch, Harold C. Relyea, Walter A. Rosenblith, Eugene B. Skolnikoff, and Philip M. Smith. The views expressed are those of the author and do not represent a deliberative process of or a position taken by the National Academies of Sciences or Engineering, the Institute of Medicine, or the National Research Council.