Secrecy: Its Role in National Scientific and Technical Information Policy

STEPHEN B. GOULD

Introduction

TRUE AND CORRECT KNOWLEDGE is the result of a complex process in which ideas and information can be checked, tested, and challenged continuously and without restraint by all interested parties. Many who adhere to this view also believe that scientific discovery and technological innovation become difficult or impossible in the absence of open communication within the research community. These assertions are widely held to be true among scientists and engineers. In modern history, however, military competition between adversaries has fueled pragmatic efforts to limit or discourage open communication of ideas and information in many fields of research.

Scientific and technical information is a major product of federally sponsored research. National scientific and technical information policy, like many broad areas of government concern, is not anywhere articulated in a comprehensive form. Agencies that sponsor basic and applied research in support of broad mission needs—such as the Departments of Defense and Energy and the National Aeronautics and Space Administration (NASA)—each have their own policies and practices for dissemination and access to information produced. Those seeking to understand scientific and technical information policy must derive it from numerous statutes, legislative histories, regulations, and executive branch directives. Policies for restricting the availability or communication of scientific and technical information are similarly mandated by a

Stephen B. Gould is Director, Project on Scientific Communication and National Security, Committee on Scientific Freedom and Responsibility, American Association for the Advancement of Science, Washington, D.C.

variety of government edicts. One purpose that many of the edicts have in common is to restrict or prevent the transfer of militarily useful technology to other nations.

An unclassified report released in September 1985 by Secretary of Defense Caspar W. Weinberger states the current case for caution in determining the availability of scientific and technological information with military applications.[1] The report, prepared by the U.S. intelligence community, argues that Western technology is being systematically acquired legally and illegally by "intricately organized, highly effective collection programs specifically targeted to improve Soviet military weapon systems." Although the value of these programs for Soviet technological development and advancement cannot be measured, acquisition of Western equipment and technical documents are estimated to benefit all Soviet military research projects. In the view of the Department of Defense (DOD), assimilation of Western technology by the Soviet Union is so broad that the United States and other Western nations are thus subsidizing the Soviet military buildup.

While undesired technology transfer to the Soviet Union is not the only impetus for regulating the flow of scientific and technical information, such transfer is currently the driving force cited by federal officials in support of a vigorous technology security campaign. Secrecy (here associated with information security classification procedures) is not the only tool being used by federal agencies to inhibit acquisition of scientific and technical information by U.S. adversaries. Within the past few years the government has sought to develop and implement procedures intended to keep certain categories of unclassified information out of the public domain, yet widely accessible by the research community and industry of the United States and its allies. Since mid-1984, the government has also sought to clarify what types of scientific and technical information will remain available for unrestricted circulation within the United States and international research communities.

This commentary will review and discuss restrictions imposed by the federal government on dissemination of scientific and technical information. The primary statutory and administrative mechanisms for controlling scientific and technical information will be explained. Commentary concerning the wisdom of controls on such information will be reviewed. Finally, the implications of the current system of restrictions will be examined.

How Restrictions are Imposed

The strongest statutory bases for restrictions on scientific and technical information are found in the Invention Secrecy Act and the Atomic Energy Act. Executive branch discretion and interpretation have played a major role in imposing restrictions based on the Export Administration Act and the Arms Export Control Act. A series of executive orders have established and maintained the security classification program without any statutory basis.

Before discussing these mechanisms for restricting dissemination of scientific and technical information, it is useful to examine National Security Decision Directive (NSDD) 189, signed by President Reagan on 21 September 1985. This directive is intended to set forth current administration policy on the dissemination of information resulting from basic and applied research sponsored by the federal government. According to the directive:

> It is the policy of this Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted. It is also the policy of this Administration that, where the national security requires control, the mechanism for control of information generated during federally-funded fundamental research in science, technology and engineering at colleges, universities and laboratories is classification. Each federal government agency is responsible for: a) determining whether classification is appropriate prior to the award of a research grant, contract, or cooperative agreement and, if so, controlling the research results through standard classification. No restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification, except as provided in applicable U.S. Statutes.[2]

The label *fundamental research* was not commonly used as a descriptive term within the scientific and engineering research community prior to release of the directive in draft form in May 1984. According to Department of Defense officials, the term was deliberately chosen both to convey the nature of research which would likely fall within the scope of the policy, and to allow each relevant individual federal agency to formulate an operational definition of the term best suited to its particular security needs.[3] NSDD 189 itself provides only a general definition:

> "Fundamental research" means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.[4]

In a memorandum conveying NSDD 189 to the heads of executive branch departments and agencies, the White House stressed the policy "preserves the ability of the agencies to control unclassified information using legislated authority provided expressly for that purpose in applicable U.S. statutes."

Proposed revisions to the Department of Commerce regulations which implement the Export Administration Act also employ the concept of fundamental research and contain the same definition used in NSDD 189.[5] According to the proposed regulations, information arising during or resulting from fundamental research qualifies for unrestricted export to any destination under a General License for Technical Data Available to All Destinations (General License GTDA). A General License GTDA is roughly equivalent to a regulatory exemption requiring no prior notification to the Department of Commerce for the export of qualifying categories of technical data. Scientific or technical information that is already publicly available or is made public by the transaction in question, educational information, and information in certain patent applications also qualify for this license.

The regulations further spell out explicit rules-of-thumb that will be used to identify research qualifying as "fundamental research." Research conducted by scientists or engineers working for a university will normally be considered fundamental research, unless the university or the researchers accept any restrictions on free and immediate publication of scientific and technical information resulting from the research project.[6] Research conducted by scientists or engineers working for a federal agency or a federally funded research and development center (FFRDC) may be designated as fundamental research under any appropriate system devised by the agency or center. Research conducted for a business corporation will be considered fundamental research only if the researchers are free to make scientific and technical information resulting from the research publicly available without restriction or delay based on proprietary considerations.

Almost one year prior to the issuance of NSDD 189, the Department of Defense made known its operational criteria for determining whether research is fundamental. According to a memorandum issued by the under secretary of defense for research and engineering, all unclassified

contract research supported by funds allocated from Department of Defense budget category 6.1 is considered to be fundamental.[7] Unclassified research performed on a university campus and supported by 6.2 funding is "with rare exceptions" also considered fundamental. University researchers are to be informed in advance of any Department of Defense grant or contract whether the proposed research will be considered fundamental, and, if not, what contract controls are proposed by the department to restrict dissemination of research data.[8] Contract research projects performed in off-campus university facilities that are not supported with 6.1 funds generally are not considered fundamental. Some discretion in assigning the fundamental label is allowed for research performed for the Department of Defense in federal laboratories under both budget categories 6.1 and 6.2.

Department of Defense officials have indicated that research sponsored by the federal government that is not considered fundamental may still be free of restrictions.[9] However, scientific and technical information that remains unclassified can be considered by the government to be restricted under the Export Administration Act or the Arms Export Control Act if a researcher is obligated to a contractual agreement with the sponsoring agency that restricts dissemination of information arising during or resulting from a research project. As indicated earlier, neither statute offers a well-defined basis for restricting the flow of unclassified information. Since the constitutionality of direct application of the statutes to scientific and technical information has been questioned, the government has sought to rely primarily on contractual agreements to bring such information under the control of the implementing export regulations. By deciding what research projects should be subject to contractual restrictions, the sponsoring agency essentially determines what information will be subject to export controls.[10] The Department of Defense in 1983 secured an exemption to the Freedom of Information Act that permits the department to withhold from public disclosure information it determines to be subject to export restrictions.[11]

The Export Administration Act of 1979, as amended by Congress in 1985, mandates the use of export controls to the extent necessary "to restrict the export of goods and technology which would make a significant contribution to the military potential of countries which would prove detrimental to the national security of the United States."[12] The act defines *technology* to mean:

> The information and knowhow (whether in tangible form, such as models, prototypes, drawings, sketches, diagrams, blueprints, or

> manuals, or in intangible form, such as training or technical services) that can be used to design, produce, manufacture, utilize, or reconstruct goods, including computer software and technical data, but not the goods themselves.[13]

The act requires that a list of militarily critical technologies, to be developed by the Department of Defense, be added to the control list of goods and technology subject to national security export controls.[14] While the Department of Defense has developed its list of critical technologies, it has not yet been added to the control list. The department's list is widely regarded as a list of all advanced technologies that can be applied to the development and manufacture of military systems.

In the 1985 amendments, the following declaration of policy was added to the act:

> It is the policy of the United States to sustain vigorous scientific enterprise. To do so involves sustaining the ability of scientists and other scholars freely to communicate research findings, in accordance with applicable provisions of law, by means of publication, teaching, conferences, and other forms of scholarly exchange.[15]

The House Committee on Foreign Affairs, which originally proposed the amendment, has indicated that the phrase "in accordance with applicable provisions of law" is intended to encompass constraints imposed by executive classification authority and contractual agreements between researchers and their sponsors based on national security, proprietary or trade secret considerations. The committee added the policy statement to the amendments because of concern that an overly broad interpretation of the act could seriously limit "the legitimate scientific communication process on which scientific productivity in the United States depends." In the view of the committee, existing government authority to declare material classified, to control work performed under contracts, and to limit the entry to and movement within the United States of foreign nationals is adequate to meet U.S. security needs.[16]

The Arms Export Control Act provides authority for restrictions on the export of technical data related to defense articles.[17] The International Traffic in Arms Regulations (ITAR) in implementing this statute define *technical data* to include:

> Information which is not classified pursuant to U.S. laws and regulations and which is directly related to the design, engineering, development, production, processing, manufacture, operation, overhaul, repair, maintenance, or reconstruction of defense articles. This includes blueprints, drawings, photographs, plans, instructions, computer software and documentation. This also includes informa-

> tion which advances the state of the art of articles on the U.S. Munitions List.[18]

Information in the public domain, and general mathematical and engineering information only indirectly useful in the defense field are not considered to constitute technical data. The ITAR does not yet explicitly employ the concept of fundamental research, and thus the Arms Export Control Act could be considered one of the "applicable U.S. statutes" available to restrict unclassified technical data arising from such research.

The dissemination controls on federally sponsored research imposed by a combination of contractual agreements and the export control statutes are generally not restrictive enough to enshroud scientific and technical information in secrecy. Unclassified documents containing scientific and technical information developed under the sponsorship of the National Aeronautics and Space Administration fall into six categories: (1) ITAR documents; (2) Expert Administration Regulations (EAR) documents; (3) "For Early Domestic Dissemination" documents; (4) "Limited Distribution" documents; (5) documents disclosing an invention; or (6) publicly available documents.[19]

ITAR documents bear a notice stating that the information falls under the purview of the U.S. munitions list and thus should not be transferred to foreign nationals in the United States or abroad without specific approval. A notice on EAR documents states that the document "may not be transferred to foreign nationals of proscribed destinations without specific approval." Both types of documents are available to U.S. citizens and may be available without an export license to scientists and engineers in other countries under the terms of specific government-to-government technical cooperation agreements.

Documents not otherwise restricted under the provisions of ITAR or EAR that contain the results of NASA research and development that have significant potential for domestic, commercial, or governmental benefit are designated as restricted distribution documents. "For Early Domestic Distribution" documents are those containing technical data determined to be applicable to commercial products or processes which could be brought to market within a reasonable time period and which would contribute to a recipient's share of the market because the resulting product or process will reach the market sooner or will be superior to those of competitors. Such documents bear the following notice:

> Because of its significant early commercial potential, this information, which has been developed under a U.S. Government program, is being disseminated within the United States in advance of general

> publication. This information may be duplicated and used by the recipient with the express limitation that it not be published. Release of this information to other domestic parties by the recipient shall be made subject to these limitations. Foreign release may be made only with prior NASA approval and appropriate export licenses.[20]

This designation has been used by NASA since 1973. Starting in 1985, documents can also be designated by NASA as "Limited Distribution" documents. Such documents contain technical data determined to relate to a proof-of-concept or a major breakthrough that would allow a major technological improvement that could be applied in a commercial or governmental aerospace system or subsystem within five years. Copies of these documents bear the following notice: "Because of its significant technological potential, this information, which has been developed under a U.S. Government program, is being given a limited distribution whereby advanced access is provided for use by domestic interests."[21]

The centerpiece of Department of Defense dissemination policy is also a procedure for marking all newly created technical documents with distribution statements. The statements are for purposes of defining availability of technical documents within the defense community and indicating how requests for documents from outside the department should be handled. The procedures apply to all technical documents generated by research, development, test, and evaluation programs funded by the Department of Defense.[22]

Seven distribution statements can be used by Department of Defense components that generate or are responsible for technical documents. Documents with distribution statement *A* are approved for public release and unlimited distribution. Documents with statements *B*, *C*, *D*, or *E* are automatically available to defined entities. Requests from other parties must be specifically approved by the controlling office within the Department of Defense. These four statements may be applied to classified, declassified, and unclassified documents.

B documents are available to U.S. government agencies. Justifications for assigning this availability include protection in accordance with the desires of a foreign government furnishing the information; protection of information not owned by the U.S. government that is received from a contractor with the understanding that it may not be transmitted outside the U.S. government; protection of the results of test and evaluation of commercial products or military hardware when disclosure may cause unfair advantage or disadvantage to the manufacturer; and protection of technical or operational data from automatic dissemination under the International Exchange Program. *C* documents are available to U.S. government agencies and their contractors,

and require protection for information and technical data that advance current technology or describe new technology in an area of potentially significant military application. *D* documents are available to the Department of Defense and its contractors, and may concern a system or hardware in the development or concept stage. *E* documents are available only within the Department of Defense. *F* documents are available only as directed by the controlling office and are generally technical documents that are classified.

For documents marked with distribution statement *X*, distribution is authorized to government agencies and private individuals or enterprises eligible to obtain export-controlled technical data. The Department of Defense Authorization Act of 1984 contained a provision exempting technical data deemed subject to the export control laws from disclosure by the Department of Defense under the Freedom of Information Act.[23] The Department of Defense has broadly interpreted this authority to permit the withholding of subject technical data from any type of public disclosure. The implementing regulations set forth requirements for eligibility to obtain such data from the Department of Defense.[24] Private firms and individuals must sign a contractual agreement which certifies compliance with U.S. export control regulations; that recipients of the data are U.S. citizens or persons admitted to the United States for permanent residence; that data are needed to bid or perform on a contract with the U.S. government or for other approved purposes; and that access to the data will not be provided to persons other than employees or persons acting on the recipient's behalf without the permission of the Department of Defense. The department reserves the right to deny requests for subject technical data if the data are judged to be unrelated to the purpose for which the requestor is certified; if the significance of the data for military purposes is such that release for purposes other than direct support of approved activities may jeopardize an important technological or operational military advantage of the United States; or if credible and sufficient information is known that the requestor has violated U.S. export control law, violated its certification, made a certification in bad faith, or made an omission or misstatement of material fact.

The Atomic Energy Act, first passed by Congress in 1946, requires that most information relating to nuclear weapons and nuclear energy be designated as Restricted Data.[25] Restricted Data is defined in the act as "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy."[26] Information within this definition is "born classified" as a government secret unless

and until it has been declassified by the government. A significant amount of information falling within the definition of *Restricted Data* has been declassified. Although the designation has generally been applied to data generated by government employees or with government sponsorship, the information control provisions of the act have been applied to any information falling within the definition of Restricted Data regardless of where the information originated.[27] The law requires any person making any invention or discovery generally useful in the field of atomic energy to file a report with the Department of Energy within six months giving a complete description of it, unless a patent application has been filed.

At the request of the Department of Energy, the Atomic Energy Act was amended in 1981 to authorize withholding of unclassified information from release if disclosure could result in a significant adverse effect on the health and safety of the public or the common defense. Justification is required that release of the information would significantly increase the likelihood of illegal production of nuclear weapons; or theft, diversion, or sabotage of nuclear materials, equipment, or facilities.[28]

The Invention Secrecy Act permits the government to block the granting of a patent and prohibit an inventor from disclosing the invention to anyone else when, in the view of a defense agency, publication or disclosure of an invention would be detrimental to the national security.[29] A secrecy order issued by the patent commissioner is effective for not more than one year, subject to a possible renewal. Two alternatives are currently being worked out by the Patent and Trademark Office in cooperation with the Department of Defense. The first option would allow the issuance of a patent along with an order which limits use or disclosure of the invention to classified projects of the government. A second option would allow the issuance of an order which limits disclosure to persons employed by the originating company. Publication of such a patent would require an export license, as would the export of a product or process making use of the invention. Under both options the patent would be withheld until the order was rescinded.[30]

Information can be classified for national security purposes pursuant to a program that is currently defined by Executive Order 12356.[31] Classification at one of three levels—top secret, secret, and confidential—can be applied to information if it concerns "scientific, technological, or economic matters relating to the national security," or "capabilities of systems, installations, projects, or plans relating to the national security." Basic scientific research information not clearly related to the national security cannot be classified. Access to classified

information is provided only upon a determination both of an individual's trustworthiness, by way of a background investigation, and that such access is essential to the accomplishment of authorized government activities.

Review of Commentary

Application of all types of restrictions to scientific and technical information has long been a controversial matter within government and the research community. Discussion and debate on the wisdom of imposing controls on information resulting from research supported by the federal government has occurred throughout the past four decades. In 1948, Vannevar Bush addressed the issue in a manner not antagonistic to the current multilayered system of controls:

> We can compete in the open with any totalitarian power and give them cards and spades as far as fundamental science—the foundation on which development rests—is concerned....But in the applications which grow through development out of fundamental science, it is a different matter. The critical point may well be reached far earlier in the process than we are accustomed to think, and ...we must be alert to it and ready at once to erect the defenses of protection and security which it demands.[32]

Congressional hearings held during the 1950s first brought attention to complaints by leading scientists that technological secrecy practiced by the federal government was more damaging than beneficial to U.S. national security.[33] The issues aired then are still being debated today—Defense and Commerce Department directives and regulations designed to cut down on the flow of technical information, how the flow of militarily valuable technological know-how to potential enemies can be confined without unduly harming U.S. interests, and whether there is too much uncertainty about what information should be classified or restricted.

During the hearings, scientists testified that the United States since World War II has "steadily lost ground relative to our competitors until now there is serious question whether the U.S. actually retains leadership in certain critically important areas of military technology." They insisted that trying to keep secret broad areas of knowledge was futile. Determined foreign data collection activities were seen to be seldom blocked while internal information flows were obstructed.[34] Lloyd Berkner delivered the strongest indictment of U.S. secrecy and characterized the then prevailing attitudes as follows:

> As a nation we have become neurotic, so preoccupied by imagined aches and pains that we have lost sight of our great strength. We allow ourselves to believe that the system of Soviet communism has elements of strength superior to our own when we could readily reason that a totalitarian socialism can only follow—never lead—our true system of free enterprise that exploits diversity. We have been misled to adopt some of the Soviet methods with consequent suspicion, mistrust, divisiveness and loss of leadership that always follow such methods. We see spies under every chair and from the consequent fear, prescribe remedies that sap our strength. In rooting them out, let's keep our sense of proportion. Our strength should come from our leadership and unity, a superiority which no espionage can conquer.[35]

In 1970, a Defense Science Board task force headed by Frederick Seitz focused on secrecy in military research and development. In addressing specific questions posed by the director of defense research and engineering, the task force considered security classification from the national long range and short range viewpoints. The task force generally concluded that the Department of Defense security classification system required major surgery if it was to function properly in the defense, national, and international environment. The information most deserving of classification was deemed to be that which industry often treats as proprietary. The task force argued that security classification was "most profitably applied in areas close to design and production, having to do with detailed drawings and special techniques of manufacture rather than research and most exploratory development." The task force concluded that the amount of scientific and technical information which was held to be classified could advantageously be decreased as much as 90 percent by limiting the amount of information classified and the duration of its classification. The task force recommended that as a general rule, research and early development should be unclassified. Classification was recommended only when development of military systems approaches the "blueprint" stage. In particular, the "confidential" category was considered to be inappropriate for research and development programs, and "special access" limitations were judged to be more likely to seriously impede difficult technical programs than not.[36]

Restrictions on scientific and technical information based on export control laws received heightened attention subsequent to a study by the Defense Science Board in 1976. A panel chaired by Fred Bucy argued that design and manufacturing know-how are the principal elements of strategic technology control. Technology contained in applied research or development was deemed to be of possible significance

in selected areas. The categories of export that were seen as deserving primary emphasis were: (1) arrays of design and manufacturing know-how; (2) keystone manufacturing, inspection, and test equipment; and (3) products accompanied by sophisticated operation, application, or maintenance know-how.[37] This premise helped set in motion more vigorous efforts to apply export control regulations to transfer and dissemination of technical knowledge related to militarily useful advanced technology.

In 1982, a Defense Science Board task force study on university responsiveness to national security requirements found that the shift in emphasis of export controls from product control to control of technology—including products, equipment, and arrays of know-how—complicated relations between the Department of Defense and the university research community. The task force noted that researchers in universities are driven by goals and motivations quite different than those found in industry, where proprietary restraints act to inhibit the flow of important know-how. Since prestige and recognition are attained in academia by being the first to publish a new idea or concept, the task force saw it as crucial that the Department of Defense be sensitive to differences between industry and universities in its pursuit of the control of technologies that are critical in a military sense. Stating that control of technical information generated by research could be a major obstacle to restoring a healthy relationship between universities and the Department of Defense, the task force recommended that clear guidelines be established for dissemination of technical information in Defense-funded university research. The task force urged that the guidelines not be overly restrictive and not inhibit the legitimate flow of scientific information. A dialogue between the government and the university community since the issuance of this task force report has led to the policies on fundamental research articulated in NSDD 189 and the general license provisions of the Export Administration Regulations.[38]

A study on scientific communication and national security by a panel chaired by Dale Corson recommended that no restriction of any kind limiting access or communication should be applied to any area of university basic or applied research, unless it involves a technology meeting all of the following criteria: the technology is developing rapidly, and the time from basic science to application is short; the technology has identifiable direct military applications or is dual-use and involves process or production-related techniques; transfer of the technology would give the Soviet Union a significant near-term military benefit; 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 panel recommended classification for university research meeting these criteria. Noting that most universities will not undertake classified work, the panel recommended as an alternative written agreements no more restrictive than a prohibition of direct participation in research projects by nationals of designated foreign countries, and a requirement for simultaneous submission of manuscripts to a publisher and the contract officer with a sixty-day period for the sponsoring federal agency to seek modifications.[39]

Although concluding that the criteria suggested by the Corson panel are unworkable, Department of Defense officials have opted for use of contractual controls on university research not considered fundamental. The potential use of classification to restrict fundamental research is sanctioned by NSDD 189.

Analyses from a variety of perspectives of the tension between controls on the export of technology and the environment required for the advancement of science and technology in the United States indicate areas of agreement and disagreement as to the widsom of controlling unclassified scientific and technical information arising from federally sponsored research. Roland Schmitt sees a "Catch-22" dilemma in seeking to protect the products of an asset that can be destroyed by the act of protection—a system of research and development that is highly interactive and largely open.

Schmitt agrees with what has become a consensus view that all areas of fundamental scientific and engineering research should remain unfettered by controls including research of military interest. With respect to unclassified technical data that is not deemed fundamental, Schmitt tacitly accepts some level of control by urging that procedures be developed "for screening foreign nationals who come to the United States for research training or technical employment so that they can have the same freedom of access to unclassified technical information as U.S. citizens."[40] Other observers and institutions regard any attempt to control technical information as counterproductive for national security. Stephen Unger argues that openness supports national security:

> The free exchange of knowledge among scientists and engineers is a key factor in promoting progress. An integral part of the scientific process is the publication and wide dissemination of new ideas, discoveries, and experimental results. By this means, critics may detect errors or faulty reasoning, point out possible improvements, or confirm the validity of what was done. Colleagues (often complete strangers) may suggest solutions or alternative approaches to problems raised. They may find applications other than those that the

> author had in mind—sometimes in entirely different fields. Mention in a technical paper of unsuccessful approaches to a problem helps others avoid wasting effort in exploring blind alleys. Publication of successful solutions to problems makes it unnecessary for others to expend time and energy in solving them again, although it is common for a solution to inspire others to find better, often simpler, solutions to the same problems. They may also generalize published solutions to cover broader classes of problems.[41]

Resistance to controls on communication of unclassified technical information is centered in the scientific and engineering professional societies. These societies seek to advance fields of knowledge by promoting open presentation, discussion, peer review, publication, and dissemination of technical information to all who want it, regardless of nationality. Through publication of journals and the sponsorship of meetings, societies seek to create a permanent record of knowledge generated in scientific and engineering fields. By one self-evaluation:

> From a neo-protectionist perspective the Institute for Electrical and Electronics Engineers must rank as a significant threat to Western and U.S. national security. As publisher of over fifty state-of-the-art technical journals the IEEE provides a direct conduit for critical information transfer across national boundaries, although in view of the international authorship this is not unidirectional.[42]

In a September 1985 letter to the secretary of defense, the elected presidents of twelve scientific and engineering societies emphasized that the broad range of unclassified information subject to Department of Defense controls places limits on the exchange of scientific and technical information that, in turn, are detrimental to the national security interests of the nation. In the view of the societies:

> In science and engineering research, the open exchange of information ensures that critical peer review is applied to new advances, provides valuable cross-fertilization of ideas and helps avoid duplication of effort. One of the principal missions of our organizations is to encourage and provide opportunities for such exchange and thereby to promote advances in the fields of knowledge which we represent. Since such advances are also important to national security, we feel impelled to advise you of the counterproductive consequences of the current DoD policies and of the limitations in our ability to respond to them.[43]

Of particular concern to the signatories is a directive, first proposed by the Department of Defense earlier in the year, setting policy for the presentation of scientific and technical papers based on research sponsored by the department.[44] The guidance bars approval of unclassified papers judged to contain export-controlled information unless physical

access to the presentation will be limited to government employees and individuals certified by the department as eligible to receive export-controlled technical data. Such "unclassified/limited access" presentations were first required on an ad hoc basis by the Department of Defense during a meeting of the Society for Photo-Optical Instrumentation Engineers in April 1985.

Where are We Headed?

Dissemination restrictions on a significant body of unclassified information arising from government-sponsored research appear now to play a substantial role in national scientific and technical information policy. What is unclear is whether the availability and use of restrictions on unclassified technical data will lead to a decrease in the use of classification authority. According to Sumner Benson, the Reagan administration considered establishing a fourth category of classification, below the existing three categories of confidential, secret, and top secret. This approach was rejected as too expensive and cumbersome since classification controls require specified physical facilities to house the documents, detailed procedures for controlling the documents, and costly and time-consuming security clearances for personnel who will have access to the documents. As an alternative, the application of procedures based in export regulations rather than classification is seen by proponents as allowing much greater flexibility in disseminating technical information while still inhibiting Soviet access to information subject to the controls.[45]

In the absence of substantially decreased use of the current classification system, it is clear that export controls will lessen the availability of U.S. government-sponsored technical information within the international research community. Technical documents arising from many categories of unclassified research, which in the past were likely to be made publicly available, will now only be accessible to defined sectors in the research community.

Reliance by the government on contractual agreements between researchers and their sponsors to bring scientific and technical information within the purview of export control statutes from the start of a research project may make the controls legally defensible. No consensus has been reached on whether use of contractual agreements to keep information out of the public domain makes sense from a public policy perspective. Recognizing that export controls are unlikely to completely halt the undesired transfer of militarily useful knowledge to our military adversaries, defense officials argue that making the acquisition

activities of our adversaries more difficult and expensive will hinder the advance of their military technologies and bolster U.S. national security. Critics question whether the increased transaction costs associated with acquisition of export-controlled information by scientists and engineers in the United States and friendly nations may similarly hinder the advance of Western military and civilian technology. Since a significant portion of the controls on unclassified information now in place are new, their impact, both on Soviet and friendly acquisition of export-controlled knowledge, cannot yet be measured.

The "red-tape" burden associated with the new controls could, at least in theory, be substantially less than would have been the case if such controls had been expanded a decade ago. For example, partial automation of the certification, access approval, and document handling systems associated with implementation by the Department of Defense of its policy of selective dissemination of certain categories of unclassified technical data could make access by eligible individuals and enterprises only marginally different than obtaining publicly available documents from the department. Actual experience with access has yet to be assessed.

The physical safeguards expected by the government for export-controlled information have not been made clear. Such information cannot be kept in publicly accessible library collections, and this alone may hinder productive access. Industrial users may experience little difficulty in handling controlled documents since existing procedures for managing proprietary information may be common and familiar.

Export-controlled knowledge poses particular problems for many academic research institutions. The large population of foreign nationals on most university campuses makes even minimal safeguards awkward. Faculty may utilize government documents much less extensively than in the past if they cannot freely share the information with their students regardless of nationality. Over the long term, this may reduce the value of academic teaching and research in fields substantially supported by government research and development funding.

Export-controlled knowledge also poses difficult choices for some professional societies. Between restrictions that may discriminate against members who are citizens of nations with less than complete official access to U.S. technology and the difficulties associated with access by academic researchers, society effectiveness and the value of membership may be reduced whether a society accepts "unclassified/restricted access" sessions or not. Some societies could be faced with a choice of facilitating the sharing of all unclassified ideas among

fewer individuals or facilitating the sharing of a smaller body of information among all members. The creation of barriers to participation in U.S. professional society meetings by foreign scientists and engineers may also contribute to decreased society effectiveness and sharing of information. This is a matter of great concern to the scientific and engineering societies since leadership in some areas of technology resides within other nations.

Complaints from within the military research establishment point to further possible effects of procedures designed to prevent public dissemination of unclassified information with military applications. It has been argued that such restrictions are making it difficult for the national laboratories to recruit and retain the best researchers. One laboratory official analyzed the situation as follows:

> How can [researchers] grow professionally if their work cannot be widely discussed or presented for peer review? How can they be rewarded without the opportunity to publish in the open archival literature? What this means is that we have a great deal of difficulty acquiring experienced people. We have to grow them ourselves.[46]

Conclusions

It is not difficult to accept the fact that the Soviet Union has a vigorous program for legally and illegally obtaining scientific and technical information relating to Western technology that is valuable for the development of military systems. The legal collection efforts are certainly duplicated to a greater or lesser degree by both public and private sector entities in most technologically active nations for both civilian and military purposes. The use of espionage in conjunction with comprehensive monitoring of publicly available information is a logical and cost-effective tactic for enhancing the rate of advancement of Soviet military technology. The reality of an arms race and multilateral technology embargoes make such acquisition efforts a rational course of action. Solely within the context of military competition, efforts to hinder the Soviet acquisition of Western technology serve an important policy role.

The costs and benefits to national security of restrictions on the dissemination of scientific and techincal information with military application have clearly not been definitively assessed and may not be measurable. Consequently, there is no consensus within the research community that is broadly supportive of dissemination restrictions as a component of national security policy. On paper, the current array of controls on scientific and technical information appears logical from a

military perspective. In theory, the restrictions may permit researchers to continue to have access to state-of-the-art government-sponsored research without significant transaction costs. Yet the history of government is rife with examples of well-intentioned policies that respond to particular problems and, when implemented, prove to have unintended counterproductive effects. Simply because there has been so little agreement about the efficacy of dissemination restrictions on scientific and technical information, these policies may be at risk of having unfortunate implications for the advancement of both military and civilian research in the United States.

Much recent attention has been devoted to the unwieldy aspects of the classification system—the volume of information that is classified by the government, the number of people that consequently must hold clearances, and the difficulties of adequately screening and policing cleared personnel. The recommendations of the Defense Science Board task force on secrecy, in combination with the system now in place to control unclassified technical information, offer one alternative that could be usefully considered by the government to ease the strains on the information security system. Declassification of most technical information now currently classified, along with continued control of such information using the new procedures for limiting dissemination of unclassified information, may yield broad benefits to military and civilian research and development.

Despite general talk of "regulatory impact assessments" to be conducted prior to new government regulations, the federal government does not systematically weigh the broad implications of its controls on scientific and technical information. It is the unwanted responsibility of the research community to document the costs of regulation and seek relief if serious disruptions in the advancement of science and technology can be proven. The government and the research community have struggled with defining the tradeoffs between national security and openness in science and technology for much of the post-World War II era. The process of determining an optimal balance between openness and secrecy promises to continue.

References

1. Technology Transfer Intelligence Committee. *Soviet Acquisition of Militarily Significant Western Technology*. Washington, D.C.: USGPO, 1985.

2. United States, National Security Decision Directive. "National Policy on the Transfer of Scientific, Technical and Engineering Information" (NSDD No. 189). Washington, D.C.: White House, 21 Sept. 1985.

3. Leo Young to the Working Group on Export Controls of the Department of Defense/University Forum, informal discussion, 14 Sept. 1984.

4. United States, National Security Decision Directive. "National Policy on the Transfer of Scientific, Technical and Engineering Information" (NSDD No. 189).

5. See *Federal Register* 51(16 May 1986):17986-89.

6. Arrangements providing for a prepublication review by a sponsor of university research solely to ensure that the publication would neither compromise patent rights nor inadvertently divulge the sponsor's trade secrets are not considered restrictions under this provision.

7. U.S. Department of Defense. Office of the Under Secretary of Defense for Research and Engineering. Memorandum on "Publication of the Results of DoD Sponsored Fundamental Research." Washington, D.C.: U.S. DOD, 1 Oct. 1984.

8. Examples of specific contract controls include requirements for prepublication review by the government, with or without right to withhold permission for publication; restrictions on prepublication dissemination of information to noncitizens or other categories of persons; or restrictions on participation of noncitizens or other categories of persons in the research.

9. Leo Young to the Working Group on Export Controls of the Department of Defense/University Forum, informal discussion, 14 Sept. 1984.

10. U.S. Department of Defense Directive 5230.25, dated 6 Nov. 1984, specifies that judgment on whether technical data under consideration discloses critical technology with military or space application will be generally guided by the Militarily Critical Technologies List.

11. 10 U.S.C. Section 140c, as added by Public Law 98-94, "Department of Defense Authorization Act, 1984," Section 1217, 24 Sept. 1983.

12. 50 U.S.C. 2402 (2) (A) App.

13. 50 U.S.C. 2415 App.

14. 50 U.S.C. 2402 (d) App.

15. 50 U.S.C. 2402 (12) App.

16. See *Congressional Record* 131(16 April 1985):H 2006.

17. 22 U.S.C. 2751

18. 22 C.F.R. 125.01.

19. See NASA Management Instruction 2230.1B.

20. Ibid., 2230.1D.

21. Ibid., 2230.1E.

22. See U.S. Department of Defense Directive 5230.24, "Distribution Statements on Technical Documents."

23. 10 U.S.C. 140c.

24. See U.S. Department of Defense Directive 5230.25, "Withholding of Unclassified Technical Data From Public Disclosure."

25. 42 U.S.C. 2011-2296.

26. 42 U.S.C. 2014(y).

27. See Cheh, Mary M. "Government Control of Private Ideas." In *Striking a Balance: National Security and Scientific Freedom,* edited by Harold C. Relyea, p. 8. Washington, D.C.: American Association for the Advancement of Science, 1985.

28. 95 Stat. 1163 at 1170.

29. 35 U.S.C. 181-88.

30. See Committee on Scientific Freedom and Responsibility. "Scientific Freedom and National Security." *AAS Bulletin* 8(Winter 1986):1-2, 7.

31. See *Federal Register* 47(25 June 1982):27836-42.

32. U.S. Congress, House, Committee on Government Operations. *Availability of Information From Federal Departments and Agencies* (Part 8). Hearings, 85th Cong., 1st sess. Washington, D.C.: USGPO, 1957, pp. 2159-60.

33. U.S. Congress, House, Committee on Government Operations. *Availability of Information From Federal Executive Agencies* (Part 4). Hearings, 84th Cong., 2d sess. Washington, D.C.: USGPO, 1956, p. 725.

34. Ibid., p. 751.

35. Ibid., p. 754.

36. U.S. Department of Defense, Office of the Director of Defense Research and Engineering. *Report of the Defense Science Board Task Force on Secrecy.* Washington, D.C.: DOD, 1 July 1970.

37. U.S. Department of Defense, Office of the Director of Defense Research and Engineering. *Report of the Defense Science Board Task Force on Export of U.S. Technology.* Washington, D.C.: DOD, 4 Feb. 1976.

38. U.S. Department of Defense, Office of the Under Secretary of Defense for Research and Engineering. *Report of the Defense Science Board Task Force on University Responsiveness to National Security Requirements.* Washington, D.C.: DOD, 1982.

39. Panel on Scientific Communication and National Security, Committee on Science, Engineering, and Public Policy, National Academy of Sciences, National Academy of Engineering, Institute of Medicine. *Scientific Communication and National Security.* Washington, D.C.: National Academy Press, 1982.

40. Schmitt, Roland W. "Export Controls: Balancing Technological Innovation and National Security." *Issues in Science and Technology* 1(Fall 1984):126.

41. Unger, Stephen H. "A Proposal to Limit Government Imposed Secrecy." *Technology and Society* 2(Dec. 1983):3-6.

42. Bogumil, R.J. "Society and Technological Secrets." *Technology and Society* 2(March 1983):2.

43. James Y. Oldshue, Gerard Piel, Charles A. Eldon, Paul E. Pritzker, Robert R. Wilson, Lewis Larmore, Marvin F. De Vris, Robert R. Shannon, Ellis K. Fields, Richard W. Karn, Wilbur L. Meier, Jr., and T.K. Pethe to Caspar W. Weinberger, joint communication, 17 Sept. 1985.

44. U.S. Department of Defense, Office of the Under Secretary of Defense for Research and Engineering. "Policy and Guidelines for the Presentation of DoD-Sponsored Scientific and Technical Papers" (Draft Proposal), 24 Oct. 1985.

45. Benson, Sumner. (Discussion during a symposium, "Scientific Freedom and National Security: Is There a Conflict?" at the 1985 Annual Meeting of the American Association for the Advancement of Science.) In *Transaction/Social Science and Modern Society* (forthcoming).

46 Smith, R. Jeffrey. "Scientific Secrecy: An Unhealthy Trend." *Science* 228(14 June 1985):1293 (quote is from Arthur H. Guenther, chief scientist at the Air Force Weapons Laboratory).

This Page Intentionally Left Blank