Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

STAT

DDCI speech
pages 15-22
14 Feb 84
National Academy of
Science

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Hearings

Export Controls: Reconciling National Objectives

ADEMY INDUSTRY PROGRAM

National Academy of Sciences National Academy of Engineering

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

The Academy Industry Program (AIP), established in 1983, is a mechanism through which industry can support the independent work of the National Research Council (NRC), the operating arm of the National Academies of Sciences and Engineering, which provides authoritative advice to the government and private sector on scientific and technical matters and their policy implications. The AIP also provides a forum for the exchange of views among industry, government, and universities and provides opportunities for industry participation in a variety of NRC activities.

For further information, contact:

Director
Academy Industry Program
National Academy of Sciences
2101 Constitution Avenue, NW
Washington, D.C. 20418

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Briefings

Export Controls: Reconciling National Objectives

Selected presentations from an Academy Industry Program seminar held in Washington, D.C., on February 14, 1984.

National Academy of Sciences
National Academy of Engineering

Washington, D.C. 1984

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

PREFACE

The seminar "Export Control: Reconciling National Objectives" was held on February 14, 1984, under the sponsorship of the Academy Industry Program, as one of a series of programs designed to bring together representatives from industry, government, and universities to exchange views on major national issues. This volume includes four edited presentations given at the seminar as well as a summary of the day's discussions.

Anne Keatley
Director
Academy Industry Program

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

CONTENTS

OVERVIEW

Richard A. Meserve 1

THE JUSTIFICATION FOR AND CONSEQUENCES OF CONTROLS

John N. McMahon 15

TECHNOLOGY AND NATIONAL SECURITY

Roland W. Schmitt 23

CONTROLS ON TECHNICAL DATA

Paul E. Gray 35

SUMMARY

Richard A. Meserve 42

NOTES 50

APPENDIX

Session Chairmen and Speakers 52

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

OVERVIEW

Richard A. Meserve
Attorney
Covington & Burling

This presentation is intended to provide a factual foundation for the discussions that will occur throughout the day. Because the subject of today's forum embraces complex legal and technical issues, this tour through the export control system of necessity must be brief.

I shall divide my discussion into three parts. First, I shall provide a summary of some of the conflicting policy objectives that must be reconciled in establishing an export control system. I shall follow with an overview of the legal machinery by which exports are controlled and a summary of some of the current issues in implementation. Finally, I shall conclude by discussing the special problems associated with technical data controls.

Policy Objectives of Export Controls

The export control system is currently in great turmoil. The Congress is in the midst of revising the Export Administration Act. The House has reported a bill and a significantly different bill is working its way through the Senate. Many of the issues that we will discuss today may well be hammered out in the House-Senate Conference. The regulatory system is also in flux. There are many proposals under consideration to alter the regulations in far-reaching ways. Finally, there are struggles over policy between various government departments, reflecting the very significant differences of view within the federal government. Indeed, these interagency battles have become

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

sufficiently intense that reports of them appear in the popular press. The soothsayers here at the Academy should be congratulated for scheduling this forum at the exact time when public discussion might best illuminate and possibly affect the formulation of policy.

In my view, this turmoil in export controls is a manifestation of a fundamental and steadily intensifying conflict in policy objectives. On the one hand, the chief motivation for controls is national security, and several factors are converging that are seen as warranting the tightening of controls to serve national-security objectives. First, the United States is placing increasing emphasis on defense systems that apply high technology to counterbalance the Soviet quantitative advantage. Thus, it has become increasingly important to deny our potential adversaries access to the technology that gives us an edge. Second, we have moved into a period of heightened tension between the super powers. In such times, greater attention than usual is given to national security interests. Third, it appears that, at least in some important areas of military technology, the U.S. lead over the Soviet Union is diminishing. Finally, it is believed that these relative Soviet gains would not have been possible without the absorption of large amounts of Western technologies. A CIA report issued in mid-1982 asserts that the Soviets have saved hundreds of millions of dollars in research and development costs, have avoided years in research and development time, have significantly reduced their production costs, have enhanced weapons performance, and have enabled the incorporation of countermeasures to Western weapons early in the development of their own weapons programs. In sum, the increasing importance of protecting our technology, coupled with the intense Soviet efforts to obtain it, have enhanced the national security justification for strengthening the system of controls.

Simultaneously, however, there are other factors that press for a relaxation, or at least a refocusing, of controls. Perhaps chief among these factors is the impact of controls on international trade. Controls on direct trade with the Soviet bloc are not particularly significant in a macro-economic sense--in 1982, we exported only $3.5 billion in goods to the Soviet bloc, or about 1.7 percent of our total world trade of $207 billion. Thus, a tightening of controls on exports to

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

the Soviet bloc might not have a significant direct impact on the American economy, although, of course, it could be important to specific sectors of the economy, or to particular firms. But an effective system of controls cannot be limited to the Soviet bloc. It is necessary as well to impose restrictions on trade with other nations in order to prevent goods or data from being diverted. The friction induced by such West-West controls is said to have a significant and adverse impact on the capacity of American companies to compete in the international marketplace: the licensing process causes delay and creates uncertainty as to the reliability of American suppliers.

It appears, moreover, that a steadily increasing share of militarily significant technologies are dual-use in nature--that is, the technologies have both military and commercial applications. In fact, in some of these technologies, advances of significance to both types of applications are now likely to appear first in the commercial sector. Microelectronics is a prime example. The chip that provides the information-processing power for the video game that an American manufacturer wishes to export may be more sophisticated than the processor in a defense radar system. Moreover, the high technology areas that are of greatest significance for national security purposes are often the very ones that present the greatest trade opportunities for U.S. companies. For example, in the electronics area alone, it is estimated that American manufacturers will export nearly $26 billion of equipment in the next year, and over half of these exports will be subject to controls.

Finally, the adverse impacts of controls are not limited to the economic sphere. It is argued, for example, that restrictions have unintended and adverse national security impacts because they weaken the United States economically and they undercut the stability of relationships with friends and foes alike. Indeed, it is asserted that many of the controlled technologies are available abroad and thus the imposition of controls does not serve to deny technology to the Soviets; it merely harms U.S. interests.

It is probably impossible to reconcile the national-security and trade-promotion perspectives on export controls in a fashion that adequately satisfies both

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

goals at all times. I suspect only an uneasy and constantly changing compromise is attainable. My point here is to bring these perspectives to your attention at the outset, as they illuminate the many issues that arise in defining an appropriate control system.

The Legal Machinery of Export Control

Let me turn now to a discussion of the legal machinery by which exports are controlled and some of the current issues that surround the operation of that machinery.

The law with the broadest application is the Export Administration Act of 1979--the law which is currently subject to renewal by Congress. The law is administered by the International Trade Administration of the Department of Commerce through the Export Administration Regulations--also known by the acronym EAR. Exports subject to the EAR are controlled primarily in the interest of national security and foreign policy, and to a lesser degree to protect commodities in short supply. Technical data as well as commodities are controlled, and the controls cover reexports between foreign countries of products or data with U.S.-origin content, as well as exports from the United States.

Every item exported from the United States requires an export license. Two types of export licenses exist: general licenses and validated licenses. Most commercial transactions may be conducted under a general license without the necessity of submitting a formal application and obtaining an approval for the particular transaction. A general license is in some respects analogous to an exemption. The remainder of export transactions are subject to a rigorous application process that leads, if successful, to a validated license for the export. Under certain conditions, it is possible to obtain a multi-transaction license, usually in the form of a distribution license, to permit shipments over a period of one to four years to foreign consignees that have been established as reliable from the standpoint of U.S. national-security interests.

The determination of whether a validated license is required is guided by the nature of the item, the destination of the export, and, in some cases, the value of

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

the export. In processing an application, the end user and the end use of the export are significant factors in the Commerce Department's deliberations. For example, an end use that is connected with the production of military equipment in the Soviet Union may be more readily denied than an application for a more benign purpose. In a recent year, Commerce processed roughly 90,000 applications for validated licenses.

Sanctions for a violation of the Act can be severe. A single willful unlawful export can bring a corporation a fine of up to $1 million or an individual a fine of up to $250,000 or ten years in prison. Civil penalties may be imposed in an administrative proceedings for any violation, whether or not willful. These penalties may reach $100,000 if national security controls are violated. Goods may be seized and forfeited. And most serious of all, the right to engage in export trade may be suspended or revoked. Efforts to enforce the Act have recently increased; many of you have heard about the Custom Bureau's "Operation Exodus," which is designed to stop illegal outflow of high technology.

Although the Export Administration Act is by far the most significant of the statutory foundations for the control of exports, there are a number of other statutes that are important for particular types of products or technology, or for trade with particular countries. I mention them briefly in passing. Exports of defense articles and services--for example, military aircraft, tanks, artillery--are controlled under the Arms Export Control Act, which is administered by the State Department's Office of Munitions Control. The relevant regulations are the International Traffic in Arms Regulations--or ITAR. The scope of products and data controlled through the Arms Export Control Act is narrower than those subject to the Export Administration Act, but the controls are more far-reaching. In recent months, there have been efforts to extend the reach of the ITAR to cover technology that has non-military applications, such as in very high speed integrated circuits (VHSIC) and in cryptographic systems used in bank teller machines.

The Atomic Energy Act of 1954 regulates exports of special nuclear material, including enriched uranium, and facilities for their processing. The Trading with the

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Enemy Act of 1917 supports the Treasury Department's Foreign Assets Control Regulations, which govern trade with North Korea, Vietnam, and Kampuchea. This act also provides the foundation for regulations that control trade by foreign subsidiaries of U.S. firms with Cuba and trade by such subsidiaries in strategic products with the European Soviet bloc, even where the products have no U.S.-origin content. Finally, the International Emergency Economic Powers Act of 1976 permits the imposition of trade constraints in times of national emergency. This Act was invoked to freeze Iranian assets and later to embargo trade with Iran during the Iranian hostage crisis. It also was used recently by President Reagan to maintain export controls during a brief period in which the Export Administration Act had expired.

In addition to the exercise of the power authorized by this complex set of statutes, there are other means available to the executive branch to regulate the export of technology. These include the classification system, visa controls on international travel, the regulation of scientific exchanges with other nations, and perhaps most significant, contractual restrictions. As an example of the latter type of controls the Department of Defense (DoD) is currently considering a proposal to require recipients of DoD contracts or grants to transmit manuscripts for review by DoD either simultaneously with or before submission to a journal. The purpose of the review is to assure that militarily critical technology is not inadvertently revealed through publication.

Defining the Items Subject to Control

Let me now turn to a sampling of the issues that arise in the implementation of export control. The national-security perspective obviously justifies the adoption of expansive controls, whereas the trade-promotion perspective urges a narrow focus to the control system. An example of the debate over the scope of controls is reflected in the controls on embedded microprocessors. As you all know, microprocessors are now widely used in the control of machine tools and in a wide variety of other domestic and commercial devices. Although the end product itself may not be subject to stringent export control, the microprocessor may well be. If the controls on microelectronic devices were to apply, then the export

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

constraints would reach far beyond microelectronic exports to the wide variety of other goods that use microelectronics, including such mundane items as toys and sewing machines. The battle over what to control has been waged most fiercely in this area.

The debate on the scope of the controls is complicated by the fact that an entirely new method of identifying controlled items is slowly emerging. The EAR now includes a Commodity Control List that contains several hundred entries, many of which are generic in nature. The entries are grouped into ten categories, including metal-working machinery, chemical and petroleum equipment, electrical and power-generating equipment, and so on. Each entry contains a description of the item controlled and the countries for which validated licenses are required.

The origins of a new method of defining the items subject to control originated with a report of a task force of the Defense Science Board that was chaired by Fred Bucy of Texas Instruments.[1] The Bucy Report expressed the view that the control system was misfocused. It argued that rather than seeking to control Soviet acquisition of particular products, the proper objective should be to restrict Soviet access to the technology by which they themselves could produce militarily significant equipment. Our most important secrets are the know-how that enables the application of industrial processes. The Bucy Report therefore advocated that the government identify militarily critical technologies and regulate those tightly, while relaxing the controls on the exports of products.

Congress took cognizance of the Bucy Report in fashioning the Export Administration Act of 1979. That Act directed the Secretary of Defense to develop a militarily-critical technologies list--known by the acronym MCTL--and that the MCTL be incorporated in the Commodity Control List. Over the years since 1977, the Department of Defense has tried, with some industry participation, to perfect an MCTL. In fact, a list has been developed and is revised annually, but to date, portions of it are classified. The MCTL has not yet been folded into the Commodity Control List, although it is used informally as a guide in licensing decisions.

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

It is apparent that fundamental problems remain in implementing the MCTL approach. For example, it is impossible to regulate technology exports as such. Only exports of the embodiments of technology can be regulated--cross-border transmissions of particular commodities or particular data, such as blueprints or computer software. Someone in the executive branch must decide which specific products or information should be subjected to export licensing for particular destinations and which licensing standards should be applied in administering the controls. Although the Bucy philosophy may be sound, in practical application it is still necessary to convert the list of technologies into detailed instructions for industry and government administrators.

Perhaps in recognition that the physical manifestations of technology are the easiest way in which to identify or describe that technology, the MCTL reportedly includes an exhaustive list of equipment. It is said to be the size of a Manhattan phone book and to cover a broad spectrum of the products of U.S. industry, including many items that have substantial or even primarily non-military applications. At this stage, it is difficult to assess all the consequences of actually attempting to use the MCTL as a control list.

Unilateral or Multilateral Controls

Many militarily significant technologies are available in countries other than the United States and thus, the imposition of unilateral controls by the United States does not effectively preclude Soviet access. In recognition of this fact, the foreign availability of technology is a factor that, by statute, must be assessed in determining whether to apply controls. Nonetheless, there is room for disagreement as to whether identical technology is available abroad. Moreover, the exercise of unilateral controls by the United States on certain critical technologies is said to be justified by the need to maintain controls while we convince our allies that they should join us in multilateral controls of these technologies.

In fact, the United States has made vigorous efforts in recent years to convince our allies that they should

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

participate more effectively in establishing multilateral controls. The forum for these discussions is the so-called Coordinating Committee--known by the acronym COCOM--which consists of Japan and all NATO members (less Spain and Iceland). The organization is unchartered and voluntary, with headquarters in Paris. Although our COCOM partners take a somewhat more relaxed view of controls than does the United States, some tightening of the multilateral system is expected.

West-West Controls

Coupled to the issue of unilateral controls on exports is the issue of controls on technology that is exported to free-world countries, particularly Western Europe. In the current discussion in the Congress over the extension of the Export Act, this issue takes the form of a debate as to whether the Defense Department, which is the strongest advocate of the national-security perspective, should have a statutorily provided opportunity to review certain West-West license applications. The Department of Commerce is claimed to have a conflict of interest because of its trade-promotion obligations. The matter has some current intensity because of the controversy surrounding the recent seizure in West Germany of certain DEC computers that were in the final stages of shipment to the Soviet Union.

In the regulatory arena, the controversy over West-West controls currently manifests itself in certain proposed changes in the regulations governing distribution licenses, which are validated licenses authorizing multiple exports and which are particularly important to companies involved extensively in international trade. The changes revise the existing regulations so as to exclude certain electronic products and related equipment from eligibility for distribution outside the COCOM countries, Australia, and New Zealand. The changes also would tighten foreign consignee eligibility requirements, establish new audit procedures, and require no-reexport certification requirements from foreign customers outside the COCOM country group.

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Extraterritoriality of Controls

One feature of the U.S. export control system that has been particularly controversial surrounds our efforts to control the activities of persons and firms in other countries. The United States has exercised controls on foreign firms by reason of their ownership or control by U.S. interests, by virtue of the fact that the products or technical data that they export have U.S.-origin content and, in some cases, by reason of the fact that the products are made with U.S. technology. No other country attempts to regulate foreign export trade in this manner and the efforts of the United States to do so have lead to friction, diplomatic pressure, and occasionally even retaliatory action.

The most recent and controversial extraterritorial application of U.S. export controls occurred in connection with the Yamal Pipeline--the pipeline to transport natural gas from Siberia to Western Europe. Although the controls were officially cloaked with the justification of persuading the Soviet Union to modify its behavior toward Poland, the real motive is generally conceded to be our efforts to frustrate the installation of the pipeline. At first, the United States barred U.S. exports to the Soviet Union of oil and gas equipment and exports from third countries of equipment having U.S.-origin content or constituting the product of U.S.-origin technology where that content or technology had been exported to the foreign manufacturer while subject to a written assurance requirement barring reexport. Subsequently, the United States imposed a prohibition on exports to the Soviet Union of oil and gas equipment by any "person subject to the jurisdiction of the United States"--a restriction that was expressly defined to include all foreign firms owned or controlled by U.S. interests, regardless of whether those firms made use of U.S.-origin products or technology. The prohibitions were also expanded to forbid delivery by foreign firms of the products of U.S. technical data in certain circumstances, regardless of whether the data were subject to restrictions on reexport when the data were originally shipped from the United States.

Although the U.S. government ultimately relaxed these controls after intense pressure by several European governments, the episode has generated debate as to the

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

appropriate scope of controls on foreign persons. The result is that Congress may well impose some constraints on the power of the executive branch to exert extraterritorial controls to serve foreign policy objectives.

The Administration of Controls

As described earlier, the current control system is a maze of overlapping agency jurisdiction. For example, the Commerce Department is responsible for the administration of the EAR. The State Department is responsible for the administration of the ITAR. The Department of Defense has a critical role as an advisor to both these agencies. Enforcement power is exercised by officials of the Treasury Department, including the Customs Service, and the Department of Commerce. Not surprisingly, the efforts to correct this administrative morass are guided not only by the desire to streamline the system, but also by judgments as to how heavily to weigh the national-security and trade-promotion objectives. Those who favor greater emphasis on national security, for example, advocate a stronger role for the Department of Defense.

Controls on Technical Data

I will now turn to an important and difficult special facet of export controls--efforts to regulate the export of technical data.

The EAR controls exports of technical data from the United States and reexports of U.S.-origin technical data between foreign countries. Such data are defined to include "information of any kind that can be used, or adapted for use, in the design, production, manufacture, utilization, or reconstruction of articles and materials." The terms "export" and "reexport" are, in turn, defined to include not only a direct transmission across national boundaries, but any release of information in another country or release within the originating country with the knowledge or intent that the data will be transmitted abroad. A prohibited release may occur through visual observation of equipment and facilities, through oral exchanges, or even through the application of experience abroad. Thus, for example, a visit to a U.S. laboratory by a foreign national or even merely a

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

technical discussion with a foreign national within the United States may be deemed to constitute an export of technical data.

Obviously, these definitions are expansive and bring many ordinary communications formally within the export control system. The impact of these definitions is currently mitigated, however, by two significant limitations. First, data in the public domain are excepted. The regulations include a general license authorizing the export to all destinations of data that are generally available by publication or by release at open meetings. Second, the regulations include a general license permitting free-world transmissions of most non-public, non-military technical data. As you might imagine, vast quantities of technical information of a proprietary nature are constantly moving under the latter authorization without any government scrutiny. Some of these transmissions are subject to a requirement, however, that the exporter receive a prior written assurance that the data or its direct product will not be reexported to a prohibited destination.

Those who attach particular significance to the national-security objective believe that the controls on technical data are too lax. As a result, there has been considerable discussion of additional controls on scientific and technical communication. The possible changes include proposals to narrow the availability of the general license for public information and to require validated licenses for all exports of data relating to certain "critical" technologies. A critical technology might include, for example, information relating to the production of sophisticated semi-conductor devices. If the latter proposal were adopted, a communication involving a critical technology between an American company and a Western European customer might require a validated license--an express prior approval from the Commerce Department before the transmission could take place. Because of the severe inhibiting effect of such a scheme, it might be accompanied by regulatory changes to allow a comprehensive license for communication between, for example, a domestic company and its foreign subsidiary. Nonetheless, any such scheme would have a profound and far-reaching impact.

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Many serious policy questions are raised by such a tightening of controls on data transmissions in addition to the trade impacts. First, there is a question of effectiveness. The export system operates most understandably in the control of tangible objects because a discrete and observable physical event occurs when a commodity passes from one nation to another. The export of technical data--including, as it does, communication with foreign nationals in this country--is far more difficult to police.

Second, strong constitutional imperatives are involved. The Supreme Court has made clear that the First Amendment protects the right to communicate not only with other American citizens, but also with foreigners. These rights no doubt extend to technical communications, although in a commercial context, the protection may be limited. Before-the-fact restrictions on communications, such as those imposed by a licensing system, are the most serious and least tolerable limitations on First Amendment freedoms because of their chilling effect on speech. Thus, there are strong limitations on the government's authority to restrict communications. In fact, a United States Court of Appeals has sustained the application of the technical-data provisions of the current ITAR in the face of a constitutional challenge only by construing those regulations very narrowly.

Finally, constraints on technical data flows could have a profound impact on technical advance. It is asserted that restrictions on the free flow of information would serve to limit feedback, to delay the discovery of errors, to hinder the critical evaluation of technical information, and to undermine the pace of advance. Thus, it is argued that achievement of security by the restriction of technical communication may slow the pace and effectiveness of our overall technical effort. Even if viewed solely from a national-security perspective, there is a question as to whether the benefit of expansive controls on data is overwhelmed by the costs. As with controls on products, it is essential to focus the controls in a way that minimizes these costs.

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Conclusion

As demonstrated by even this simplified overview, the export control system is exceedingly complex. The creation of an appropriate control system requires a complicated and difficult balancing of competing objectives under circumstances of factual uncertainty. The development of common understanding among individuals with different perspectives on the issues can provide essential illumination of the murky policy terrain. Hopefully, today's discussion will serve to shed the necessary light.

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

THE JUSTIFICATION FOR AND CONSEQUENCES OF CONTROLS

John N. McMahon
Deputy Director
Central Intelligence Agency

As you can imagine, the Intelligence Community is somewhat uptight on technology transfer. We get a little demoralized when we spend a lot of effort to find out about Soviet weapons systems only to have them end up being ours. That's not an overstatement. The technology transfer on military-related hardware is enormous, and what I would like to do today is share with you a feeling that we are not really dealing with a bunch of spooks who get some information every now and then. We are dealing with a concerted effort by the Soviet Union, beginning in the Politburo, in a well organized structure that orchestrates the acquisition of hardware as well as technology.

At one time we were quite content to be the target of all of this because of the leading position the United States enjoyed in the technological world. That technology has been shared now, however, with Western Europe and Japan as they have expanded to match the United States technologically. They now afford the Soviet Union and their allies in the Warsaw Pact a happy hunting ground. If the Soviets can't get it here, they can get it someplace else.

With the Europeans very much involved in this now, we see strains developing. Our traditional European allies desire trade with the East and view the United States with a little bit of skepticism as we begin to put controls on that trade. We finally caught the attention of our allies about two years ago when we pointed out to them that it was not a question of trade, but of robbery. The Soviets were running clandestine operations against them and walking away with their technology free of

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

charge. That caught their attention and they now realize that it's for real. In the past year over 100 Soviets have been expelled from Europe because they were caught red-handed. I would like to share with you some insight on Soviet activities gleaned from a great many of our own clandestine operations as well as our experience with our Western allies. This is not a new issue between the Intelligence Community and the National Academy of Sciences. We had a very interesting dialogue with the Corson Panel[2] in which we studied the problems posed by our concern for U.S. national security needs as well as their impact on academic exchanges. It was not surprising that we didn't agree on all points, but there was a sufficient sharing of views that I think had a very valuable effect across the board. Insights were gained by the Academy as well as the public about a problem that until then had very much been overlooked. The Academy has played a very useful role in developing awareness throughout academia about this technology transfer problem.

Technology transfer, of course, has many facets, but in terms of national security, it can be distilled down to a simple, overriding problem, at least at the moment: the acquisition of military-related Western technologies by the Communist world, and here we focus principally on the Soviets and their Warsaw Pact allies.

The scope of the Soviet collection effort and the ability of the Soviet military industrial complex to assimilate Western technology is most impressive, and it really surprised us when we began to look into it. They can do it. There was a very glib line of thought for years that even if the Soviets got the technology, they couldn't put it to use because they couldn't reproduce it. All we had to do was make sure that they didn't get our production techniques, and they couldn't do much about it. Well, that has proven false; they can do much about it and are doing it today.

Just during the late 1970s, the Soviet collectors acquired some 30,000 pieces of Western controlled and uncontrolled equipment, weapons, military components, and manufacturing technology, and over 400,000 technical documents. Unfortunately, a good many of these documents were classified. We know that the KGB and their counterpart in the military, the GRU, as well as the

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Ministry of Trade, the Soviet Academy of Sciences, and the State Committee for Science and Technology are seeking and have already acquired and copied numerous items to help solve their problems in developing new weapons and military equipment.

They have hundreds of pieces of microelectronic fabrication and memory tester systems, hundreds of electronic test and metering systems for quality control of aviation, missile, and undersea systems. They have programmable oscilloscopes, scores of microwave and other advanced communications equipment, high quality large photographic systems for thin film production, multimillion dollar large machining centers for manufacturing tanks and military vehicles, industrial lasers and lasers for communications and weapons R&D, fiber optical production systems, space shuttle equipment and know-how, quality lubricants and rubber products for military vehicles, high density self-contained power supplies, and high modulus glass fibers.

That's just a sample of how they can reach into our technology and get it; and we know they have it. As a result of these acquisitions, the growth of Soviet military power has been greatly accelerated in all key areas. At the same time, there has been a steady erosion of technological superiority on which U.S. allied security increasingly depends. The narrowing of the technological gap in turn has compelled the United States and its allies to make even greater efforts to overcome the growing sophistication and lethality of the Soviet military focus.

Although there is growing public awareness of this problem, very few outside the Intelligence Community understand how the Soviet program for collecting and exploiting Western technology is organized and implemented.

Parenthetically, I would like to comment on an article that the French intelligence service kindly leaked through a French periodical in which they mused about the beauty of the United States and its ability to sustain two defense programs, one of their own and one of the Soviet Union, the problem being that we have to spend money just to stay even with ourselves because of this rush of technology to the Soviet Union.

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

The organization and structure of the Soviet S&T acquisition program is considerable. We have collected in the Intelligence Community a truly impressive amount of evidence about the Soviet Union's worldwide effort to acquire high technology, and it is no accident on the part of the Soviet Union. It is extraordinarily well organized, highly centralized, and under the direct supervision of the highest organs of the party and the state: the Politburo of the Communist Party Central Committee and the Council of Ministers. The primary control over technology acquisition and exploitation rests with the VPK, the Military Industrial Commission. Significantly, predecessors to the VPK have existed since the 1930s to ensure that the Soviet military gets the resources it needs from the planned economy. Sometime in the late 1960s, the VPK was directed to greatly expand its efforts in acquiring technology from the West as well.

The VPK directly oversees the participation of the twelve key Soviet industrial ministries that are involved in military production as well as in the assimilation of Western technology into that production. In addition to the VPK, there is a little-known organization inside the State Committee for Science and Technology called the Technical Center. It is a central clearinghouse for the program and is responsible for collecting the requirements and reports submitted by the defense industrial ministries to the VPK, and for the intelligence information and materials acquired by the collecting agencies.

The defense industrial ministries in turn are required to report regularly to the VPK on their progress in assimmilating the savings in this foreign technology into their weapons program. The collection requirements are gathered by the Technical Center, blessed by the VPK, and given to the collectors for action. The Soviets designate as the collectors the KGB and the GRU as well as the State Committee for Science and Technology, the Soviet Academy of Sciences, the Ministry of Foreign Trade, and the intelligence services and foreign trade missions of their Warsaw Pact allies.

From our knowledge, the KGB and the GRU account for about 70 percent of the most significant military-related items acquired from the West. This includes not only classified items, such as weapons systems components, but

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

also such key dual-use and export-controlled items as computers, microelectronics, fiber optics, powder metallurgy, composite materials, lasers, and associated production technology. In the recent French report that I spoke of, it was estimated that during the last three years the KGB alone acquired 30 percent of France's latest high technology achievements. It is interesting to note that 80 percent of this 30 percent was acquired on the open market.

The role of the State Committee for Science and Technology--the GKNT as we call it--and the Soviet Academy of Sciences in acquiring Western technology is of particular relevance to this gathering. The GKNT is responsible for coordinating all applied research in the Soviet Union. It also plays an important role in acquiring Western technology. GKNT's scientific and technical information gathering and processing activities are vital to the generation of Soviet requirements for foreign technological acquisitions. These activities are conducted through a nationwide, centrally-directed system that comprises some hundred thousand individuals and several thousand information departments affiliated with Soviet research institutes, design bureaus, and production facilities.

In addition, the GKNT manages efforts to acquire Western technology through the activities of Soviet scientists and engineers involved in academic, commercial, and scientific exchanges with the West, including those sponsored by the Soviet Academy of Sciences. This we know for a fact. In an era of quantum leaps in military technology, basic research has become increasingly important to a nation's long-term military potential. Most basic research in the Soviet Union is done under the auspices of the Soviet Academy of Sciences.

A fact difficult to accept in the United States is that the Soviets, with growing frequency, have used academic exchange programs with Western universities and research centers to acquire sensitive scientific information for use in their weapons programs. Western magnetic bubble memory technology, microelectronic and laser research, nuclear energy technology, and deep diving submersibles are but a few of the areas in which Soviet scientific exchanges have scored notable successes.

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

The Soviet Academy of Sciences, along with the GKNT, work closely with Soviet intelligence services. Soviet scientists traveling to the West are briefed by Soviet intelligence services on S&T intelligence requirements before they leave the country. They also are expected to assess their Western colleagues for their potential as intelligence agents. Moreover, an increasing number of intelligence officers are given S&T training to allow them to masquerade as scientists in part of these exchanges.

The Ministry of Foreign Trade (MFT) is responsible for the majority of the illegal trade conducted through normal trade channels. The MFT operates a large network of trade offices, joint companies, and purchasing missions whose staffs are quite adept at obtaining Western equipment. The KGB and the GRU regularly co-opt members of the MFT foreign trade organizations for special collection tasks abroad, and both intelligence services use the MFT trade missions abroad as cover for some of their personnel. Many of the 100-plus Soviets who have been expelled by Western countries for espionage within this past year were attached to these trade missions.

Finally, the Soviet Union has made increasing use of its East European surrogates to acquire Western technology, for two reasons. First, the East European countries generally have a better image in the West than the Soviet Union, and thus, their intelligence collectors are often able to blend and operate more freely. Second, the Soviets must have multiple channels for acquiring Western technology so that none of their defense industrial ministries become dependent on a single channel. The USSR Ministry of Radio Industry, for example, acquired embargoed items routinely through the Hungarian collectors. The most active East European countries in acquiring technology for the Soviets are East Germany, Hungary, Czechoslovakia, and Poland.

The Soviet Union and its East European allies use a vast array of methods to acquire U.S. and other Western technology. Let's discuss illegal trade through third countries, because this is the area where international export controls are the weakest. Unlike classic espionage operations, illegal trade, also known as diversions, rarely employs covert trade craft. Although intelligence officers are involved in arranging diversion operations,

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

the main mechanism for acquiring controlled items through this channel is a host of fraudulent trade schemes.

Computers and semiconductor production equipment are the main targets of diversion efforts. In this area, we have identified already some 300 firms operating from more than 30 countries, and there are probably many more that remain unidentified. We know of at least five major diversion networks operating in Western Europe. Two of these, Bruchhausen and Meuller Networks, are among the Soviet Union's largest suppliers of semiconductor production equipment, and they operate on a global scale. Both Meuller and Bruchhausen were indicted in 1977 in the United States Federal Court for illegal trade activities. However, because illegal trading is not an extraditable offense, they remain at large. Werner Bruchhausen, a West German, at one point in the 1970s had more than 50 front companies operating in Austria, France, the United Kingdom, Switzerland, West Germany, and the United States. From 1977 to 1981, millions of dollars of equipment used to make microprocessors, computers, and integrated circuits were transferred through Werner to the network to the Soviet Union.

Richard Meuller, also a West German, is a master at proliferating a maze of front companies with no ostensible connection to himself, and I must say that personally I stand in awe of his ability. We estimate that during the period 1977 to 1980, Meuller smuggled some $10 million worth of embargoed technology from the United States to the Soviet Union.

Just this past December, West German and Swedish customs seized two U.S. Vax 11/782 computers and related equipment that Meuller was attempting to smuggle to the Soviet Union. The diversion route followed a typically roundabout course, from the United States to a Meuller front company in South Africa, from there to another in West Germany, and then Sweden, finally, on their way to the Soviet Union. Fortunately, they were intercepted. Meuller's whereabouts at present are unknown. He may be residing in a Soviet bloc country.

None of our allies, of course, condone the use of their territory for illegal trade activities, but the penalties for engaging in diversions have little deterrent value. Fines rarely exceed a few thousand dollars,

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

while the profits for illegally selling controlled equipment to the Soviet bloc goes to the tens of millions of dollars. In 1982, Bruchhausen, for example, netted $18 million dollars. Prison terms are rarely imposed, and when they are the sentence is usually suspended.

The United States alone cannot respond adequately to the mounting threat posed by the Soviet technological acquisition program. Only a concerted, multifaceted approach, combining both effective export control policies and vigorous counterintelligence programs by the United States and its allies can thwart this highly organized Soviet acquisition effort. For many reasons, the United States must take the lead in making the case for stricter export controls and enforcement. Some of our allies still believe that trade is a way to persuade the Soviet Union to act more responsibly in the world, despite all the historical evidence to the contrary. Their economies are also far more dependent on exports than are ours, and they have traditionally viewed the Soviet bloc as a lucrative market.

Proposals to eliminate the requirement to obtain a validated license before exporting to COCOM countries goods that are subject to the multilateral COCOM controls could jeopardize our whole export control mechanism. It is the opinion of the Intelligence Community that removal of validated licenses for goods to be shipped to other COCOM countries would weaken substantially the ability of the United States to monitor the flow of its technology abroad and to prevent the unauthorized reexport of this technology to the Soviet bloc.

In conclusion, I can only impress upon you that it is a massive program on the part of the Soviet Union. It does work. When we see the Soviet weapons system that is actually ours or a derivative of ours, it convinces us of the enormity of this problem and the success that the Soviets enjoy. The insights that we have into the Soviet Union and what they are doing to us and the Western world convinces us that this merits the attention of the National Academy of Sciences as well as every American, including our industrial base.

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

TECHNOLOGY AND NATIONAL SECURITY

Roland W. Schmitt
Senior Vice President
General Electric Company

I totally support the objective of this Administration to assure that the United States is technologically superior to any adversary in weapons and defense. And I support this especially strongly now, at a critical time in our nation's defense. It is precisely my dedication to the objective--technological superiority in defense--that compels me to speak on this issue because I believe that some of the proposed policies and procedures will hamper, rather than improve, our ability to reach that objective. I am speaking from the perspective of concern with U.S. technology, not with international trade. The two are closely related, but my perspective is focused on technological strength.

We are waging a technological battle with the Soviet Union. And, too often, we find that we have superior technology, but they have equal or superior weapons. Why? Simply put, because they are good at extracting technology from us and at deploying it rapidly in weapons, while we are good at generating new technology but are often slow at deploying it in weapons.

To correct this imbalance, we must do two things: prevent the Soviets from getting our technology, and speed up our own deployment of it. But that is like saying that to win in sports you must score a lot of points and prevent your opponent from scoring. There is more to it.

It makes a big difference, for example, whether you are playing football or basketball. The balance between offense and defense is vastly different in the two. In basketball, unlike football, you cannot indefinitely

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

strengthen the defense without weakening the offense. So, too, in winning the technological battle with the Soviets, an obsession with a defensive strategy--with preventing leakage of our technology--will cripple our offense, our ability to remain the leader in generating new technology.

A question that must be asked over and over again is: why does the United States have so much that the Soviets want to acquire? This is a testimony of how well our technological system has worked. We should be very, very concerned about proposals to tamper with it. The balance between a leadership strategy and a protective strategy--between offense and defense, if you will--will determine the outcome of our contest with the Soviets.

A fundamental change in that balance is being proposed today. In the past, the essence of our strategy consisted of putting a fence of technology export restrictions around the Soviet Union and Eastern bloc countries to keep technology out. The proposed new strategy would put the fence around the United States and try to keep technology in. Such a change in strategy has vast implications for both our national security and our international economic competitiveness. We need to look very closely at the full effects of such a change--to identify the core issues relating technology and national security.

There are four core issues where differing views still exist:

- dual use--determining the extent and implications of the dual use of the same technology in both military and civilian applications;
- military criticality--determining just how critical a technology is to improving military capability;
- foreign availability--determining whether a technology is available from a foreign country and, if so, what we can do about the transfer of that technology to the Soviet Union;
- effective transfer--determining which technology transfer mechanisms are truly effective.

As I consider these issues, I'll often draw examples from the electronics technologies of very large scale (VLSI)

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

and very high speed (VHSIC) integrated circuits because they present these issues in their most dramatic form.

Dual-Use

If the dual-use issue didn't exist there would be no problem: you could separate the civilian from the military technology and classify the military technology.

Dual use is as old as technology itself--as old as the swords and spears that the prophet Isaiah proposed pounding into plowshares and pruning hooks; as old as the mirrors that Archimedes used to edify the people of Syracuse and then allegedly turned on the Roman fleet; as old as the telescope that a couple of lens grinders in Holland invented as a means to spy on their enemies, but that turned, in the hands of Galileo, into something very different.

But it wasn't so long after Galileo's day that a separation began to emerge between military telescopes and those used by the astronomers. Generally speaking, the breadth of dual use tends to diminish as you go from fundamental science toward final application. Consider VLSI, for example. At the fundamental science end, the things one has to learn--diffusion constants, carrier mobilities and lifetimes, and hot electron effects, for example--are clearly generic to all possible applications. Dual use is complete. The same goes for the next stage, engineering principles. The principles behind ion implantation or a new photolithography step are clearly common to military and civilian technologies. Dual use persists to a large extent in the fabrication processes for VLSI.

But by the time you reach the application stage, the chips used in military systems are likely to be distinct from the ones used in commercial products. Popular press reports to the contrary, it's unlikely that a chip taken from a video game would really serve as the critical part in a missile guidance system. In fact, as we move into the VLSI era, I believe that the technology tide is toward semi-custom chips, especially in applications where high performance is so important that additional cost is justified. Militarily specific chips are already protected by the International Traffic in Arms

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Regulations (ITAR), which forbid their export outside the United States or their exposure to foreign nationals. And if features or steps in the processes used to make the chips are uniquely important to military applications, they are covered by ITAR also.

In the final stages of military deployment of technology, the Soviets have in many cases been faster than we, as I suggested earlier. Recently they sometimes appear also to have been getting better further upstream--further in the direction of engineering principles and fundamental science. This has given rise to the demand for more controls upstream.

That in turn brought the response that upstream controls could damage our own ability to generate new technology to an even greater extent than they would hamper the Soviets' ability to acquire technology. These concerns led to the Corson Panel and to the recommendation of "tall fences around narrow areas."[3] For example, the Panel recommended that the control mechanism of restrictions written into government-funded contracts be used to take care of the so-called "gray areas"--areas that meet the following four criteria:

- the time from fundamental science to application is short;
- the technology is clearly military or dual use;
- the transfer of technology would give the Soviet Union a significant military advantage;
- the United States is the only source of the technology.

But, frankly, I believe that the Corson Panel recommendations, depending on how they are interpreted, still would allow too much control to be imposed on the initial, inherently dual-use stages of fundamental science and research leading to scientific and engineering principles. I believe these areas should be free of controls--outside the fence--except perhaps for a very few exceptions, such as cryptography, where the science is the technology. Restrictions on these fundamental areas would cost us more in leadership than it would gain us in protection. The work at the fundamental end of the process is what our universities and some of our industries do so well under the stimulus of an open, interactive system. That work provides leadership research,

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

educational experience for students, and an invaluable forum for access to world science and technology.

One particularly dangerous proposal for putting controls on research at the fundamental science and engineering end of the process concerns proposed restrictions on research by foreign nationals. A very high percentage of the doctoral degrees granted in U.S. schools are going to foreign nationals. The most recent study, conducted by the National Research Council in 1983, found that half of the U.S. engineering doctorates awarded in 1982 were received by foreign nationals, and that 39% went to foreign nationals on temporary visas.[4] They are studying at our best schools--for example, in 1982, 42% of the doctoral students in electrical engineering at the University of California, Berkeley, and 47% at Stanford were foreign nationals. And they are making important contributions: last year about half the technical articles in some major American journals in the areas of computer-aided design, information theory, and electron devices were written by foreign nationals.

In my view, restricting America's ability to use these people is one of the most threatening factors in winning the technological race, whether in military or commercial systems. Doctoral students are the seed corn of technological supremacy, and today a large, critical fraction of that seed corn is foreign born. Many of them will remain in the United States. The National Science Foundation has found that over half of the Ph.D. recipients have immediate plans for employment or postdoctoral work in this country. If we manage to keep them, that will go some distance--though only part of the way--toward solving the immense problem of research and development manpower facing us. With 1,400 engineering faculty positions vacant in our universities, and with a severe shortage of research-caliber people in electronics and computer science in industry, we need to make use of this important source of high caliber people.

As just one small personal example of the pervasiveness of this issue, I recently realized that five of the seven people who report directly to me at the General Electric Research and Development Center--as well as the one Nobel laureate in our laboratory--could not have been hired under the proposed technical data

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

export controls without prior licensing and many delays. I can think of nothing that might do more damage to U.S. leadership in science and technology in the next few years than to cut ourselves off from this source. Foreign nationals should be encouraged to participate in fundamental science and engineering in the United States. Even in some of the more applied fields, the need for people is so severe that I believe the State Department, the Department of Defense, and the Commerce Department should find some way to open the doors of applied research and engineering laboratories to foreign nationals who can be adequately screened. It is especially illogical to prevent U.S. industry from employing talented people who have been educated at the best American schools.

More generally, we should not fence ourselves off from the ideas and the talent of the rest of the world, especially at the fundamental science and engineering end of the technology development process. At this end of the spectrum, dual use is not a sufficient reason to encumber the processes of scientific and technological advancement.

It is in the areas from engineering prototypes downstream to specific applications that controls on the transfer of technology between the United States and other non-Communist countries should be considered. The specific steps to be taken will vary with individual technologies, depending on how fast the military and civilian technologies diverge as application is approached. If they diverge rapidly--in the engineering prototype or manufacturing stages, for example--the military part of the technology in those areas can be added to the ITAR list or even classified, and the civilian part does not need new controls. But if the divergence is less rapid, imposition of controls on the export of the technology, even to friendly countries, may be necessary.

Military Criticality

After deciding whether a technology is dual use, we next have to ask about its military criticality. The issue here centers on exactly what we mean by the term "military criticality." We especially must avoid con-

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

fusing it with "military utility." A militarily critical technology gives a nation's armed forces a new capability that they did not possess before--one that is capable of changing the military balance in some area of national defense. A militarily useful technology makes only an incremental improvement, either by providing incrementally better performance or by enabling a nation to make more of the weapons it already possesses for less money or in less time.

To give an example from VLSI, a militarily useful improvement might be the building of slightly more computational capability into a chip, to enable a missile guidance system to make more calculations and marginally improve its accuracy. A militarily critical improvement would be the implementation of an entirely new logic on a chip for the first time, making possible a method of missile guidance previously not possible--terrain following or terminal guidance, for example.

The name "Militarily Critical Technologies List" (MCTL) suggests that this distinction should be taken into account, just as the Bucy Report suggested.[5] But in fact, the MCTL list in its present form is a combination of militarily critical and militarily useful technologies. It runs to about 700 pages and contains a very large number of technologies. As I see it, that list should have two purposes. The first, which it fulfills admirably, is to alert the Department of Commerce to sensitive areas for the Department of Defense reviews of proposed licenses for export of technical data to Communist countries. Remember that all export of technical data to those countries is already controlled. The full list would make that control more effective by highlighting militarily-relevant technology.

But the list has another purpose--the monitoring and control of technology exports to non-Communist nations. For that purpose, the present list is far too inclusive. In its present form it would put severe restrictions on the transfer of many militarily useful but not militarily critical technologies to those nations. This has two potentially harmful impacts. First, fences blocking the exchange of technology prevent us from improving our own technology as fast as we otherwise might. Many important technologies are being and will be developed in friendly foreign countries. To cut ourselves off from interacting

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

with these advances will be harmful. Second, those fences have a very large adverse economic impact. The harm caused by these two impacts, in my view, outweighs the benefits to us of restricting the flow of militarily useful technology to non-Communist nations.

I am not disputing that such an outflow would make it easier for the Soviets to acquire the technology, or that, over time, incremental improvements can add up to a critical improvement. For example, the sum of incremental improvements to the accuracy of a missile eventually might convert it from a second strike to a first strike weapon. But the key words are "over time." Over that time, we can make our system move as fast or faster than the adversary's--provided we do not shackle the innovative power of our technical community. Even though our adversary may get better, we can retain our lead. But we can't retain a lead in critical technologies in the same way. With them either you've got it or you don't. Controls can be effective here in lengthening the time until the adversary has got it.

So we need a second version of the "Militarily Critical Technologies List," listing only truly militarily critical technologies and aimed at technical exchanges with non-Communist countries. The judgment should be made primarily by military experts in terms of the military impact of the technology, not merely in terms of the degree of technical change embodied in it. If a technology is found to be militarily useful only, then its export to non-Communist nations should not be subjected to the strictest controls and we should rely on our ability to attain leadership as the means of keeping our edge. This shorter list would also have another benefit. It would provide guidance to equipment designers and product planners as to the technology they could include in products aimed at international markets. Sometimes the use of a controlled technology can be avoided with little or no sacrifice in the performance of the product.

Foreign Availability

Suppose now that we have found a technology that is dual use, has reached the engineering prototype stage, and has been determined to be militarily critical--all

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

indicating that we should impose strong controls. The next issue is foreign availability--can it be obtained outside the United States.

There are really two questions here: what does foreign availability mean, and what impact does it have on controllability? It is possible to define foreign availability so narrowly that you find that nothing is available in foreign countries. But you have to go beyond carbon-copy availability and consider functional equivalence as well: can the technology available overseas do the same job as the domestically available one? To again use an example from VLSI, two computer memory chips might be deemed functionally equivalent if they both pack the same number of bits onto the same area of silicon with the same access time, even though they achieve this by totally different processes and design rules. The real question is whether the military function can be accomplished in an essentially equivalent way by a technology available from a non-U.S. source. This concept of functional equivalence has been written into recent proposals for updating the Export Administration Act. I believe it belongs in the act.

Like military criticality, foreign availability is a judgment call. But this judgment must be made by different people than those who judge military criticality. It must be made by qualified technical people from industry as well as government. The Commerce Department has established Technical Advisory Committees to do this job. The system has not worked well, partly because industry has not done its share to put enough people on these committees and to ensure that they participate adequately. But I believe this system can be made to work within the present framework through improved industry participation.

The other part of the foreign availability issue is, who has it? If another friendly nation already has a technology capability, we can gain more by including them within the fence than by shutting them out. Therefore, I recommend that we permit general licenses for the export to COCOM or other nations with whom we have a bilateral agreement of technology that is available to them anyway, and that we seek to use those agreements to strengthen controls--to keep that technology from going beyond those countries to the Communist bloc.

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Effectiveness of Technology Transfer

Suppose a technology meets the three criteria already discussed--it is dual use, it is militarily critical, and it is not available overseas. There is one more issue to be considered in applying controls: effectiveness of technology transfer.

So far we have been using the term "technology" as if it were a single entity. But, in fact, it is a whole collection of things--everything from underlying technical principles, to design, to specific embodiments, to methods of making, maintaining, and repairing those embodiments. To again give a specific example, a VLSI technology means much more than the chip itself. It means the function, the architecture, the computer-aided methods used to design and test the chip, the performance of the transistors used on the chip, the process steps used in making the chip, and the processing equipment that carries them out. These varied elements of one technology are transferred by different means. And those transfer methods vary widely in effectiveness.

The transfer of technology out of the laboratory into use is not an easy task. It is a critical part of the work of an industrial laboratory and I can assure you that it does not go very well if you rely on reports and documents alone. There is no reason to believe that such processes are very effective in any situation where the objective is to put the technology to work in a practical way. Transferring equipment and detailed know-how is much more effective. The Bucy panel came to exactly this conclusion.[6] It put together a list of technology transfer methods arranged in descending order of effectiveness. At the top of the list--highest in effectiveness--came such items as turnkey factories, licenses with extensive teaching, joint ventures, and technical exchange with ongoing contact. At the bottom of the list--lowest in effectiveness--were undocumented proposals, commercial literature, and trade exhibits.

In the case of VLSI design and process technology, we should be highly concerned with the Soviets' acquisition of items at the top of the list--for example, photolithography systems, steppers, ion implanters, and computer-aided design terminals and computers. We also should put strict controls on such things as equipment design

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

drawings. Once again, the fence protecting these controls must surround COCOM and other friendly nations, not the United States alone, because many of those nations are producing equipment as sophisticated as our own.

In considering the effectiveness of transfer methods, VLSI presents a special problem. Chips are so small that we must assume that even classified chips will be stolen, so we can't rely primarily on protection of the chip itself--that's too likely to fail. Instead, we should protect the know-how--usually embodied in the circuit design and process equipment--that would enable an adversary to reproduce in quantity or even improve on the stolen chips. Another line of defense is to make the chip immune to reverse engineering, i.e. immune to the practice of taking it apart layer-by-layer to find out how it was designed and made. I believe that there will be a technological solution to this problem and that VLSI and VHSIC chips can be made immune to reverse engineering, even if they are stolen.

Having put these lines of defense into place, we will do ourselves no good, and may do ourselves some harm, by further attempting to restrict the flow of basic scientific and engineering information on VLSI. Such a restriction would buy us negligible protection in exchange for considerable sacrifice to our capability for extending leadership. The issue of access to scientific literature, academic exchange, and open discussion of scientific development was considered by the Corson Panel. After extensive briefing by the intelligence community, some at high levels of classification, the panel concluded, "...in comparison with other channels of technology transfer, open scientific communication... does not present a material danger from near-term military implications."[7] But as stimulants to the creative process by which Western industrial nations have attained and maintained technological leadership, these channels are absolutely vital. Here we have a mechanism that helps us much more than it helps our adversaries. Recognition of the value of scientific interchange as a key part of a leadership strategy should be at the heart of our policy. The Bucy and Corson reports essentially tell us that we can separate the transfer methods most important for protection from the ones most important for leadership. We can control the first of those classes, while leaving the second free.

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Summary

First, the areas of fundamental scientific and engineering research should remain unfettered by additional controls, even in dual-use areas. The harm we would do to our leadership by such controls would outweigh any additional protective benefits that would accrue. This holds especially strongly for work in those fundamental areas that have become highly populated by foreign nationals in American laboratories.

Second, we should distinguish clearly between military criticality and military utility. This distinction might take the form of two militarily relevant technology lists. A long list of all militarily useful technologies--much like the present MCTL--would help deal with the problem of technology transfer to Communist bloc countries. A shorter one, containing only truly militarily critical technologies, would help deal with the problem of controlling technology exports to non-Communist nations.

Third, foreign availability should be defined in terms of functional equivalence. And we should permit general licenses for the export of critical technology to COCOM nations or other nations with which we have bilateral agreements.

And, finally, our export control regulations regarding non-Communist countries should focus on controlling the highly effective technology transfer mechanisms, such as the transfer of turnkey factories, process equipment, and extensive transfer of manufacturing techniques or teaching of those techniques.

By such means as these, I believe we can achieve the combination of leadership and protection that enables us to achieve the objective we all share--assuring that the United States is technologically superior to any adversary in weapons and defense, and remains that way.

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

CONTROLS ON TECHNICAL DATA

Paul E. Gray
President
Massachusetts Institute of Technology

I would like to discuss here the impact of export controls as they apply to technical data or information, the impact on the research enterprise generally, and specifically on research as it is conducted in universities.

I take as my lesson for the day two comments drawn from Dick Meserve's earlier comments. In speaking about the regulation of technical data, he pointed out that efforts to regulate such data could have a profound effect on technical advance. He also said that we are dealing in this arena with conflicting forces, that reconcilement is impossible, and that the best one can hope for is an uneasy and changing compromise. If I can contribute in some way to defining some of the dimensions of that uneasy and changing compromise, I would regard this as a happy occasion.

I would like to organize these remarks around three propositions: First, we should avoid strengthening the Soviet military posture through the careless or unintended transfer of significant technology. Second, we should recognize that most mechanisms intended to limit technology transfer will have some effect on the system that produces innovation and technical advance. Third, we should develop and apply controls in a way that achieves some appropriate balance between these conflicting objectives. Such balance is crucially important to the national interest. Indeed, the national interest may be defined, I suggest, in terms of our success in working out such a balance.

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

I would like to begin with some comments about technology generation and technology transfer. There are, of course, many sources of technology generation: universities, federal and industrial research laboratories, corporate research and development activities, and those myriad activities that are involved with the manufacture, production, distribution, and service of technical systems.

Within these different kinds of organizations there is an equally broad range of activities, starting with basic research at one end, continuing through engineering science and applied research, through research and development as it is commonly construed in the industrial setting, through prototype and product development and manufacture, on through sales and distribution and service. There is, of course, some segregation of activities by sources. For example, much of the basic research in this country is performed in the research universities. In the other areas of research and development, however, the segregation by source is less clear, and there is very broad overlap.

We heard earlier from Mr. McMahon about technology transfer mechanisms--ranging from espionage and other covert activities, to the diversion of legally exported technology, often involving third nations, to the participation of foreign nationals in technological activity, and also to access to the open literature.

Any efforts to control technology transfer will have some impact on the research enterprise, and it is that question that I would like to address. The quality and integrity of research are anchored in its nature as a dispersed, interdependent, and cumulative enterprise. Research is dispersed in that work at the frontier, in most fields, is carried on simultaneously in several locations. It is interdependent in that different investigators or groups of investigators rely on work done elsewhere to validate and extend their own work. The closer work is to the frontier of knowledge and the more swiftly a field is developing, the more researchers depend on open and rapid communication with colleagues working on similar problems elsewhere. This dependence leads to the development of informal networks of communication that rely on working papers, on preprints, and especially on personal communication.

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

In a rapidly developing field, these informal mechanisms of communication assume the principal burden of communication among colleagues. The refereed journals of science become the publications of record, but they are not the primary means for communicating innovation.

Research is cumulative in the sense that many small steps taken by individuals working in different places and under different auspices contribute to new knowledge. Indeed, I would suggest that the leadership of the United States in fields as diverse as commercial cryptography and recombinant DNA has come about precisely because of the open, interdependent nature of research in American universities. In such endeavors, limitations on the communication of results obviously impede progress. I might also say that such secrecy is exceedingly difficult to achieve simply because so much of the communication that occurs is informal in character.

I suggest, therefore, that the quality of research is crucially dependent on good communication. It is an essential element of the system.

Publication is important for the role that it plays in feedback and, through feedback, for the role it plays in assuring the effectiveness of the research enterprise. Two years ago Sissela Bok at the Harvard Medical School wrote on the subject of secrecy in research, and I would like to quote from her paper:

> The felt need to take a stand against secrecy also springs from concern for what is most central to the scientific enterprise itself, from a recognition of the damage that secrecy can do to thinking, to creativity, and, thus, to every form of scientific inquiry. Because secrecy limits feedback and restricts the flow of knowledge, it hampers the scientist's capacity to correct estimates according to new information, to seek connections, to take unexpected leaps of thought, and secrecy is expensive in that it fosters needless duplication of effort, postpones the discovery of errors, and leaves the mediocre without criticism and peer review. Secrecy, therefore, can cut into the quality of research and slow scientific momentum.[8]

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Beyond the impact that secrecy and constraints on information flow have on the effectiveness of research, there is another issue that is related to the character of research as it is carried out in universities. The United States comes close to being unique in the world in the degree to which it combines, in one set of institutions, the functions of education, particularly graduate education, and basic research, and I suggest that this coupling produces enormous benefits to the country. There are great consequences to involving experienced researchers and younger colleagues, graduate students and undergraduates, together in the research enterprise. The benefits run both ways. Young people bring to research a kind of freshness and enthusiasm and vigor with which we are all familiar. They often don't know that "it can't be done that way," and in the process of working side by side with more experienced people, they learn in the most effective way how to become capable, independent professionals in the research context.

The coupling of education and research is fundamental to the research enterprise as it exists in universities and needs to be considered when one looks at the impact of controls. Beyond this question, there is the issue of having access in the university research community to the ablest individuals. Universities are typically cosmopolitan communities. That is not by accident. Talent does not come with a particular passport, and it is important that the university community have access to the ablest individuals, whatever their nationality. In this regard, I would like to underscore the importance of what Dr. Schmitt said this morning about arbitrary constraints on the ability of foreign nationals to work in research programs.

Thus, it seems to me that if one limits either access to research or communication of research results, there are several immediate consequences. There is the loss of the corrective sort of feedback that normally arises when there is open communication. In that respect, I would like to share with you a paragraph from a speech that was delivered in this building two and a half years ago by my colleague, Jacob Den Hartog, who was being honored as the recipient of the Founders Award of the National Academy of Engineering. Let me just read one paragraph from his acceptance speech:

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

> All my life I have tried to explain engineering matters by the "case" method. I can do no better now and I propose to discuss briefly two engineering cases, in a "philosophical" manner, because I really know practically nothing of either case. The reason for such crass ignorance is secrecy, of the legal-commercial variety in one case and of the governmental patriotic type in the second case. Both kinds of secrecy I find deplorable; like "sin," I am against it, but also, like sin, I can do nothing useful about it. The job of writing a law which would prohibit these objectionable secrecies but would not interfere with the common daily intercourse of parties and persons is so formidable that I do not believe that there exists a lawyer in this world who can do it, even if he were a Jefferson, a Lincoln, or a Franklin.[9]

Dr. Den Hartog then goes on to talk about his two cases: first, plate glass failures in Boston's John Hancock Tower, and, second, the very high speed gas centrifuge for separation of uranium isotopes. The point he makes in each case is that secrecy--in one case, secrecy brought about by an agreement between the parties in an out-of-court settlement, and in the other case, secrecy brought about by the penchant of first the Atomic Energy Commission and then the Department of Energy for classifying all work related to nuclear energy--that such secrecy inhibits enormously the role of feedback as a self-correcting mechanism in the engineering world and in the areas of scientific progress. I think he is exactly on target in that respect.

I suggest also, that if there are limitations on access or on communication of results in university research, universities will be less able to attract the most competent people. Some people simply will choose not to work in such areas if the results are restricted.

Most importantly, there will be a loss in coupling of research with education, as I suggested earlier. And I suspect that in some cases there will be an unwillingness to undertake certain classes of work because of the restrictions that apply. These consequences do not occur from simple adherence to a principle. They reflect the practical difficulty which we in universities have in trying to limit anybody's access to what goes on in any

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

particular corner of the place. It is very hard to do. In the end, there will be diminished quality of process and diminished quality of results.

When Admiral Inman spoke two years ago about these matters, he suggested that the problem as it existed in universities could be resolved if universities were simply willing to recognize the prior loss of innocence and agree to have the same kind of relationship with the federal government in certain research areas that they have recently undertaken with industry in the industrial sponsorship of research at universities. I would like to suggest here, as I did then, that such a perspective is simply wrong. It does not correspond to the reality of relationships which exist between universities and industrial sponsors of research. About as far as any university has gone to restrict results that come from industry-sponsored research is to agree to a certain period of time, typically 60 days, in which papers can be reviewed for inadvertent disclosure of patentable intellectual property. Incidentally this experience with industry is not novel, since universities are in a similar situation with certain federal sponsors.

As we think about the development of controls, particularly as they bear on technical data, it is crucially important that there be sensitivity to the subtleties that are involved. I have tried to suggest here some of those subtleties. There is a need for balance, a need for tailoring solutions which fit the problem. It is not a question of balancing off the national interests against academic freedom. As Dr. Schmitt said earlier, the national interest is served neither by excessive openness in terms of transferring information to the Soviets, nor by excessive controls that would have an untoward effect on the production of new ideas, on innovation.

The Corson Panel put it very well, I think, in speaking about achieving national security by accomplishment--security by accomplishment rather than security through secrecy.[10]

What are the considerations that ought to enter into that formulation of controls? It seems to me that one needs to consider the practical utility of information. One needs to recognize that technology transfer is a

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

difficult and tortuous process and that know-how is much more important than technical reports. One needs to recognize as well that information is perishable; it has a finite lifetime. Its value decreases with time, and the generators of knowledge, if they are reasonably expeditious in putting it to use, ought to have some innate advantage because of that perishable quality.

I would suggest that, in the application of controls, it is necessary to distinguish among the various intellectual activities. Basic research needs to be treated in one way. Products, devices, prototypes--things--need to be treated in another way. In addition, not all activities are amenable to such easy classification--particularly in those areas where the research frontier is very close to the applications frontier. The Corson report spoke about the gray areas.[11] (I do wish they had chosen a different adjective, but those areas do exist!) They are sensitive, and they will not easily yield to resolution of these questions.

To summarize, I would simply say that it is important for us as a nation to try and strike a balance between objectives that are in conflict. The national interest lies not in either extreme but in setting goals and policies that serve both the cause of national security and the larger progress of science and technology on which so much of this nation's strength depends.

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

SUMMARY

Richard A. Meserve
Attorney
Covington & Burling

In light of the limited time available to me, I shall not attempt to summarize the wealth of information presented today, but rather will focus on a few items of particular significance. I should say at the outset that I do not mean to slight anyone's comments; there are many important points that I will not attempt to cover.

Controls on University Research

Let me focus first on some of the issues concerning controls on university research activities. Paul Gray, the President of MIT, gave an eloquent summary of the important societal values that derive from openness in scientific research. He described science as a cumulative enterprise in which each participant builds on the work of others. Openness prevents duplication of effort, enables the critical analysis of new work by others, and allows cross fertilization whereby scientists learn of others' work and apply that work in their own activities. President Gray emphasized the costs associated with data controls and the need to assure that any restrictions are not excessive.

Edith Martin of the Department of Defense (DoD) responded by describing the DoD's plans to deal with the variety of issues that arise from university research supported by that agency. The policy is not yet final but is sufficiently mature that she felt comfortable to tell us about it. Dr. Martin asserted that DoD does not plan to place any restrictions on its grantees with regard to attendance at conferences. With regard to publications--a particularly sensitive area from the

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

university viewpoint--Dr. Martin described the DoD's policy in terms of a decision matrix. One axis of the matrix is defined by the nature of research (e.g., basic research) and the other axis by the sensitivity of the specific research area. I won't go through the matrix in detail, but for what DoD calls 6.2 research--the applied research end of the spectrum--and for work in the sensitive technologies that the DoD most wants to protect, DoD plans to impose a contractual constraint that would require a researcher to submit a paper for DoD review 90 days before publication and to receive approval before that paper could be published. For 6.1 research--the basic-research category which encompasses most of the DoD-funded work in universities--and for research in even sensitive technology, the DoD plans to impose an obligation only for simultaneous submission to DoD and to the journal. DoD will have the opportunity for comment, but not approval. Thus, in the areas of research that comprise, perhaps, the great preponderance of DoD-sponsored work by universities, it appears that many of the concerns about constraints on free flow of information may be somewhat alleviated.

Nonetheless, the suggestion that some university researchers must seek approval before publishing will not sit well with the university community. Indeed, President Gray stated that he suspects that MIT would not undertake research subject to this restriction. Thus, paradoxically, DoD may lose the participation of our premier research universities in those very areas that it has deemed most critical. Moreover, as this publication policy moves into implementation, questions may arise with regard to the boundary between sensitive and non-sensitive research. It thus does not appear that the controversy over DoD policy has as yet been resolved to the satisfaction of all the affected parties.

Several government representatives stated that the government does not intend to require universities to police the activities of foreigners on campus. They recognize that such surveillance is an activity that universities are unaccustomed and unwilling to perform. There is also government recognition of the fact that a large number of graduate students in our universities are foreign nationals and that we as a nation benefit from their presence and their work. The government now intends to regulate the admission of foreign graduate

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

students to the United States and the universities will have no obligation to restrict the areas in which they study.

Controls on Trade

Having put the university issues to one side, let me turn to a variety of issues that arise in the trade area. I won't attempt to summarize the large amount of factual information presented, but rather will try to focus on a few areas in which there seemed to be a conflict between industry and government viewpoints. Let me say, however, that today's participants were remarkably congenial in their interaction with each other for the most part, and there were not, in many cases, sharp disagreements between speakers from industry and government. Thus, I will try to draw distinctions in some cases from the subtle differences in emphasis. This may result in the mischaracterization of the view of one side or another, and for that I apologize.

Let me first turn to the very important question of what to control. Several government representatives discussed the importance of the control scheme. Mr. McMahon from the CIA began with an extended discussion of the nature of the losses that have occurred. He described a very aggressive Soviet acquisition effort involving hundreds, if not thousands, of agents that has been remarkably successful in taking American technology and applying it in the Soviet Union. Indeed, he commented that the United States is building two defense programs--our own and the Soviets'. We heard from William Schneider of the Department of State that, among the items, the Soviet Union has obtained an improved targeting system for ICBMs and other dramatic acquisitions of a similar nature.

The complexity of the issue was revealed in the comments of Stephen Bryen from the Department of Defense. He asserted that up to 90 percent of the militarily significant technologies arise from the commercial sector. This fact, coupled with the aggressiveness of the Soviet acquisition effort, provides a foundation for the government view that controls on dual-use items must be tightened so that we can more adequately protect our national security. But, the consequence of tighter

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

controls is that American firms selling controlled items may be at a disadvantage in the international marketplace in sales to our allies.

As a result, several government and industry representatives spoke of the need to define more clearly what is controlled. The militarily critical technologies list (MCTL)--a document of some 700 pages--is very hard to apply because of its length and breadth. All agreed that the MCTL should be streamlined. Nonetheless, the Export Administration Act requires that the MCTL be folded into the commodity control list, which is the basic list of products that are subject to licensing. So although there was a concession on the government side that we need to focus our efforts and to clarify what needs to be controlled, it isn't clear in what order events will happen. If the inclusion of the MCTL in the control scheme occurs before the list is pruned, both government and industry will have increased difficulty with the system.

One speaker from industry--Roland Schmitt--suggested a helpful structure for viewing the problem of defining what to control. Dr. Schmitt described a series of hurdles that a policymaker should go through in determining whether a technology should be controlled. The first hurdle related to the maturity of the technology. Dr. Schmitt stated that the front end--the research end--of the technology-development process is characteristically dual use; knowledge at this stage is in such an inchoate form that its application, or its ultimate application as it moves toward the development end of the spectrum, will usually be in both military and civilian systems. But, he argued that such knowledge is so important for our overall technical advance that it ought not to be controlled. He asserted that as you move towards the application of technology, to the actual chips, a divergence occurs. A chip, for example, that is used in a commercial application is typically quite different in its characteristics from one that is used in military systems. And this differentiation will become increasingly clear in the future as we move towards the custom design of chips. A product with solely civilian applications should be free of controls.

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Dr. Schmitt's second criterion related to military criticality, as distinct from military utility. In his view, the existing MCTL is, in fact, a list of technologies that have some utility in military systems, but are not necessarily critical for such systems. He asserted that for control purposes there should really be two lists: a list of equipment with military utility, which ought not to be controlled in transactions with Western allies or the Third World, but which might be controlled in our trade with the Soviet bloc if other hurdles are overcome; and a list of equipment that is militarily critical--and this should be a very narrow category of technology--for which West-West control might be appropriate.

The third hurdle was foreign availability, and Dr. Schmitt stressed here that the important fact is not that identical technology be available, so much as that the technology available abroad be functionally equivalent in meeting the military purpose to that which is available in the United States. If the technology is available abroad, there is no point in unilateral controls.

Finally, Dr. Schmitt emphasized that the means of transfer should be considered. The industrial community is very much aware that it is difficult to transfer research or technology from the laboratory into the marketplace, and we ought to recognize this fact to some extent in our control system. Documents, for example, are relatively ineffective in actually transferring the capacity to produce a given technology. What really needs to be controlled are turnkey operations or the intimate educational interactions that go into learning how to apply a technology. The export system should be geared to recognize the differing effectiveness of various methods of transfer. A turnkey transfer of technology might be very closely regulated, whereas a publication should not be.

A second industry perspective on determining what to control was presented, and I will just mention it quickly in passing. It's an obvious point, but one that many in industry feel is overlooked: the government should not attempt to control things that cannot be controlled. There are some technologies--certain personal computers, for example--that are available from Japan or elsewhere.

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

In light of this fact, we are not achieving a national-security objective by tightening controls on such computers; we are merely hurting American industry.

A final element that emerged from the discussion of the focus of controls concerned the delay between advances in technology and the applications of those advances. We heard many times that there is a long and perhaps lengthening procurement cycle--the time required to move a technology into application in military systems. It was asserted that the procurement cycle requires up to 15 years in defense systems in the United States. It was also claimed that the Soviets are able to shorten that time and are more efficient at taking new ideas, perhaps even new ideas they obtain here, and embodying those ideas in their own military systems. This leads to the view, expressed by some from industry, that by emphasizing the control of technology we may be focusing in part on the wrong end of the problem. Rather, our effort should be directed towards speeding up the process by which new ideas are folded into military systems.

Let me now turn to a major industry concern--West-West controls. It was pointed out by one of the questioners that our export system requires validated licenses for trade even with our allies in certain products. But, of the 24,000 license applications that were filed for exports to COCOM countries in a recent year, only 50 or so were denied. The question was raised as to whether it is an efficient allocation of the government's resources to stop 50 exports out of 24,000.

Mr. Olmer from the Department of Commerce responded that we need to continue to control such West-West transfers by way of validated licenses because the Justice Department requires a paper trail in order to convict those who are violating the system, and because there is a benefit in stopping those 50 cases even though the search is, admittedly, like the hunt for a needle in a haystack.

There was universal agreement on the importance of COCOM controls and the need to strengthen the multilateral control system. We heard from the government people, however, that despite efforts to improve the COCOM mechanism and to develop a compatible scheme with

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

that of our Western allies, progress has been slow. COCOM operates with a very small staff on a budget of about $500,000 a year. Moreover, there are questions about the overall quality of COCOM. Thus, the government has made efforts to upgrade the COCOM system.

The point was made from the floor that it is really not COCOM, but rather each of the governments that we need to influence. The problem is not just one of getting agreement at a COCOM bureaucratic level, but of penetrating each member's legal system. Perhaps I am straining here to pull the parties apart a bit, but the general thrust of the comment was that upgrading COCOM will not achieve compatibility in the control systems among the allies.

Process

The last issue that I would mention is one of process. Everyone who spoke supported the principle that if the system is to work, it must depend on cooperation between government and the private sector. Many of the government people agreed that industry and the university community have much to offer in terms of explaining the costs of controls and providing information on foreign availability and the like. Again, however, this is an area where government practice may depart somewhat from the ideal. We saw today that two of the principal government officials involved in the area had yet to meet each other, so cooperation within the government might be a good place to start. Moreover, it appears that with regard to the proposed new requirements for the distribution licenses, advance cooperation or even communication with industry did not, in fact, occur. Clearly a greater convergence of practice and principle would seem desirable.

I would like to close with the following observation. Many of us have read newspaper articles concerning export controls with increasing frequency in the last year or so. The articles typically are about the seizure of goods that were en route to the Soviet Union or some other prohibited destination. Unfortunately, the central policy issues involving export controls are not well illuminated by such stories. Everyone in this room

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

wants to prevent such diversions, and there is agreement on all sides that the export system should be enforced strongly. Export issues, therefore, are quite unlike problems concerning the Middle East or arms control, where the press reports help to develop informed policy by revealing all sides of the issue. Export controls present a very complicated problem and fora like the one we have had today are essential in developing the necessary understanding that will enable the solution of very difficult problems.

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

NOTES

1. U.S. Department of Defense, Office of the Director of Defense Research and Engineering. Report of the Defense Science Board Task Force of U.S. Technology, An Analysis of Export Control of U.S. Technology--A DoD Perspective (Washington, D.C.: GPO, 1976), pp. 1-3.
2. National Research Council, Panel on Scientific Communication and National Security, Scientific Communication and National Security (Washington, D.C.: National Academy Press, 1982), pp. 13-26.
3. Ibid., pp. 4-6, 48-51.
4. National Research Council, Office of Scientific and Engineering Personnel, Summary Report: 1982 Doctoral Recipients from United States Universities (Washington, D.C.: National Academy Press, 1983), p. 31.
5. An Analysis of Export Control of U.S. Technology--A DoD Perspective, pp. 15-18.
6. Ibid., pp. 4-8.
7. Scientific Communication and National Security, p. 41.
8. Sissela Bok, "Secrecy and Openness in Science," The Journal of Science, Technology and Human Values, 7, Winter 1982, p. 32.
9. Jacob P. Den Hartog, Founders Award Lecture, November 4, 1981 (Washington, D.C.: National Academy of Engineering, 1981), p. 7. Dr. Den Hartog declined to give a title to his speech; however, at the end of his talk, he offered as a title the following poem:

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

On Philosophy;
On Secrets, Legal or Patriotic;
On Broken Glass & Three Mile Island;
On Boston's proud, heroic Glass Tower & on the still continuing World Leadership of this country in Science and Engineering in this our Glorious Twentieth Century;
On Pride of Profession &

Glory Hallelujah!

10. Scientific Communication and National Security, p. 45.

11. Ibid, pp. 4-6, 48-51.

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

APPENDIX

Session Chairmen and Speakers

Stephen Bryen
Deputy Assistant Secretary for
International Economics,
Trade and Security Policy
Department of Defense

Thomas Christiansen
Manager, International Trade
Relations
Hewlett-Packard Company

John Copeland
Director, International Projects
Motorola Inc.

Dale R. Corson
President Emeritus
Cornell University

Hugh Donaghue
Vice President, Government Programs
and International Trade Relations
Control Data Corporation

Paul E. Gray
President
Massachusetts Institute of Technology

Robert E. Herzstein
Senior Partner
Arnold & Porter

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4

William Howard
Vice President, Research and Development
Motorola Inc.

Edith Martin
Deputy Undersecretary for Research
and Advanced Technology
Department of Defense

John N. McMahon
Deputy Director
Central Intelligence Agency

Richard A. Meserve
Attorney
Covington & Burling

Lionel Olmer
Undersecretary for International Trade
Department of Commerce

Frank Press
President
National Academy of Sciences

Robert M. Rosenzweig
President
Association of American Universities

Roland W. Schmitt
Sr. Vice President, Corporate Research
and Development
General Electric Company

William Schneider, Jr.
Undersecretary for Security Assistance,
Science and Technology
Department of State

Peter D. Trooboff
Partner
Covington & Burling

Robert M. White
President
National Academy of Engineering

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600170003-4