CHAPTER V

The Military Implications of East-West Technology Transfer

CONTENTS

CHAPTER V

The Military Implications of East-West Technology Transfer

INTRODUCTION: THE CONCEPT OF MILITARY RISK

All trade, and trade in technology in particular, necessarily carries with it a risk that the trade will enhance the military capability or at least the military potential of the trading partner. In the case of U.S. trade with the Soviet Union, it can be argued that any accretion in Soviet military capacity weighs against the United States in an overall worldwide balance of power. Whether the political or economic benefits of trade with the U.S.S.R. offset the military costs is a matter of judgment. In order to consider such potential tradeoff's carefully, it is useful to distinguish among five categories of possible military risk:

1. Technologies which not only have a clear and direct military application that could have a substantial effect on relative force capabilities, but which also make possible the construction of weapons or the development of skills currently outside the realm of the recipient technical competence;
2. Technologies whose immediate application would advance civilian industry, but which might also be applied to military purposes in a way that would give the recipient access to weapons or military skills that it does not now possess, including:

   A. Technologies that lend themselves to direct diversion, with or without modification. An example of the former might be the precision-grinding machines sold in 1972 to the Soviet Union. It has been alleged that these machines were instrumental in allowing the Soviets to produce precision ball-bearings needed for the guidance system in multiple independently targetable reentry vehicles (MIRVS), thereby providing them with a capability they would not otherwise have possessed at the time. A hypothetical case of diversion with modification would arise if a large computer, sold to TASS or Aeroflot for a specific civilian end use, were reprogramed to perform military functions and/or actually moved from one site to another; and

   B. Technologies that lend themselves to indirect diversion, either by providing hands-on training that would be otherwise unavailable (again, the example of large computers applies), or by providing the opportunity for reverse engineering;
3. Technologies with clear and direct military application that could improve, simplify, or render cheaper or more efficient a military industrial activity already within the recipient's technical competence, or that would help to move

[1] See "Export licensing of Advanced Technology: A Review," Hearing before the Subcommittee on International Trade and Commerce of the Committee on International Relations, U.S. House of Representatives, Apr. 12, 1976.

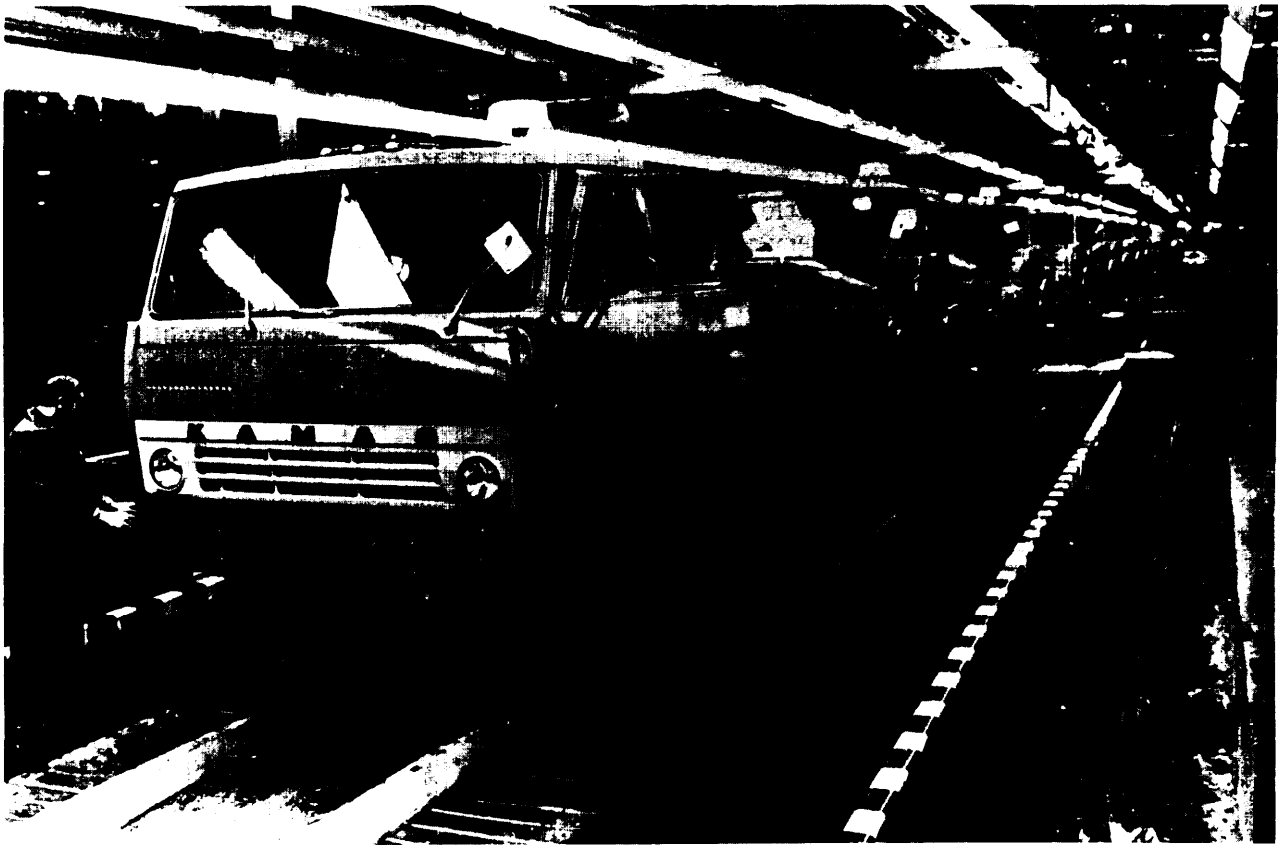
Photo credit. U.S. Department of the Air Force

Left: model of the MIRV warhead that is positioned in the nose cone (circled on right) of the U.S. Minuteman Missile

existing military development activities ahead on promising paths;

4. Technologies whose immediate application would advance a civilian industry, but which might be applied to military purposes in a military industrial activity already within the recipient's technical competence, or which would help to move existing military development activities ahead on promising paths. The same subgroups in #2 above apply here. An example of a civilian technology capable of direct diversion is semiconductor production technology; direct diversion after modification occurred when the equipment of the Kama River truck plant was altered to produce military vehicles. All computer sales carry with them the danger of indirect diversion, as all provide important training opportunities for programmers who may later be employed in the military sector; and finally
5. Technologies that would be applied to civilian industry, thereby releasing resources that might be used in the military sector. Any consumer good technology is an example, as are turnkey plants for the production of fertilizer. The latter not only make a significant contribution to agricultural productivity, but if the products of these plants are exported, also may generate the hard currency necessary for further purchases of other technologies, including those with direct military application.

These categories and the examples that illustrate them are summarized in table 13.



m h S K m R p

Table 13.—Categories of Military Risk

Nature of equipment	Direct military application	Diversion from civilian use	
		Direct	With modification
Permits capabilities that would not otherwise exist i n this time frame	'1'Nuc-lear-w;apons design information in mid-1 940's	2A. Precision machines	2B. Advanced computer hardware or software
Improves or makes-more efficient-an existing capability	3. Naval nuclear reactor production techniques	4A. Semiconductor production technology	4B. Turnkey truck plant
Frees resources for military use	N/A	5A. Fertilizer production technology, or technology expanding production of manu - facturing goods for export, thereby con tributing to hard-currency earnings	N/A

SOURCE: Office of Technology Assessment

The likelihood that a given technology will markedly improve the recipient's military capacities decreases as one moves from category one to five. There is unanimity among the United States and its allies that technologies in the first category should be stringently protected, and there is little argument that the third category deserves protection as well. Similarly, most would oppose the blockage of items falling in the low-risk fifth category, and the remainder would agree that it is impracticable. Given the wide availability of acceptable alternatives to most U.S. technology, only a coordinated policy of economic warfare both within and outside CoCom(Coordinating Committee for Multilateral Export Controls) could impose such a blockage. There is clearly little hope for support of such a policy in Western Europe and Japan. Thus, the most difficult risk assessment lies with the dual-use technologies in categories two and four.

ASSESSING MILITARY RISK

Two fundamentally different techniques can be used to restrict trade involving technologies with potential military significance. In the first system, decisions are made case-by-case. Each proposed technology sale is subjected to careful analysis to determine the possible military uses to which it might be put, and to decide the significance and likelihood of these military applications occurring. Decisions are made on the merits after detailed consideration of the individual case, using some standard of acceptable risk. The second basic approach proceeds deductively. It first establishes lists of specific and generic capabilities that are deemed militarily significant and of the technologies that are instrumental to these capabilities. The sale of any item on this list becomes, by definition, detrimental to the security interests of the United States, and is therefore prohibited. The difference between these approaches is largely one of basic orientation; actual licensing systems combine elements of both. Nevertheless, the fundamental orientation of a licensing system towards either a case method or a list strategy shapes its possibilities and its weaknesses. The following pages consider these alternative approaches in more detail.

THE CASE METHOD APPROACH

Ideally, a case method or ad hoc system of export control includes a comprehensive system of risk assessment in which a number of characteristics of the technology in question and of the circumstances of its sales are ascertained, the importance and implications of each piece of information are weighed, and a decision is made on the basis of a complete understanding of both the technology and its probable end use. At least seven different considerations may enter into this kind of assessment:

1. The capabilities of the technology must be thoroughly understood; its various uses must be identified; and the ease or difficulty with which it might be modified and diverted must be assessed. The task can be performed only by experts thoroughly conversant with the technology and its range of applications.
2. For each application of the technology, the comparative capabilities of the United States and the recipient nation must be assessed. This assessment involves determining technical leads and lags and estimating the rate of change in the differentials. In this connection, the possibility cannot be dismissed that a technology which is obsolete in the West may still have a significant impact on the military capacity of, for instance, the Soviet Union or the People's Republic of China (PRC).
3. The mechanisms of transfer must be considered. In 1976, the Defense Sci-

ence Board produced an analysis of the transfer of technology and U.S. national security.[2] The resulting document, commonly known as the Bucy report, assessed selected areas of high technology, their impact on U.S. strategic requirements, the full range of mechanisms through which they may be transferred (see chapter VI), and the effectiveness of current export control restrictions. One principal finding of the Bucy report (others are summarized below) is that the effectiveness of a technology sale varies according to the relationship between seller and buyer; the more active and continuing the relationship, the better the chance that the technology will be assimilated. The report ranks transfer mechanisms according to this criterion and concludes that the most effective—and therefore the most risky— transactions are the sale of turnkey plants, licenses with extensive teaching efforts, joint ventures, and training and exchanges that involve prolonged contact between buyer and seller and the provision of technical information. As a rule, these should be subject to closer scrutiny and tighter controls than less active mechanisms, like product sales, which do not usually transfer current design and manufacturing technology.

4. Knowledge of the recipient environment is required. There is a common misconception that technology transfer is "something like a pass from a thrower to a receiver. In fact, it has more of the characteristics of an organ transplant, with all the attendant requirements of compatibility with the environment, plus the surgical (i.e., managerial) skills necessary to establish all the intimate working relationships between the transplant and the connecting parts of the system."[3] The Soviet system, for instance, is often characterized as inefficient and inflexible, and therefore unable to make optimum use of imported technologies. Chapter X discusses the fact that the ability of the U.S.S.R. to absorb, diffuse, and duplicate Western technology has been hampered by a system in which enterprise managers, who are responsible for introducing new technology, often have no incentive to do so. Such impediments make it less likely that the technology will be used in a manner that produces results similar to those achieved in the country of origin. Even more importantly, the U.S.S.R.'s ability to improve imported technologies through domestic R&D and innovation is constrained by the difficulties of translating new concepts into serial production. For instance, according to recent testimony by Rauer Meyer, former Director of the Office of Export Administration (OEA), the Western-built Volga automobile plant has not revolutionized the Soviet motor vehicle industry; instead, the Soviets are currently conducting negotiations with Western firms to modernize other car plants. Meanwhile equipment similar to that used at Volga is currently being supplied to a tractor plant at Cheboksary. Despite the restructuring of civilian R&D activities in the Soviet Union during the late-1960's, the link remains weak between the economic incentives and material rewards of research institutions and the economic contributions of the new technologies developed by them. It would be a mistake, however, to extrapolate too easily from the civilian to the military sector. In the Soviet Union, the military takes priority; resource allocations are made first to the military, regardless of short-

[2] *An Analysis of Export Control of U.S. Technology–a DOD Perspective* (Washington, D. C.: Defense Science Board Task Force on Export of U.S. Technology, Feb. 4, 1976).

[3] Herbert Fusfeld, Director of Research, Kennecott Copper, quoted in National Academy of Sciences, *Review of the U.S./U.S.S.R. Agreement on Cooperation in the Fields of Science and Technology*, National Research Council, May 1977.

54-2020-79--

ages elsewhere in the economy, and the military sector receives the best manpower and equipment. The consequences of the inefficiencies that permeate other parts of the society, therefore, are not necessarily as serious in that sector.

5. The risk of diversion of a dual-use technology is substantially affected by the requirements, priorities, and intentions of the recipient. If, for instance, the technology is essential to meeting a need that has a very high civilian priority, the chances diminish that it will be diverted for direct military use. Large computers that direct oilfield operations are low-risk items from this perspective, not simply because they would be cumbersome and difficult to move and reprogram without detection, but because oil and gas production is extremely important to the Soviets. Similarly, it is unlikely that equipment installed in plants to manufacture drill bits will be put to any other use; the bits are sorely needed in the Soviet oil industry. There is always a chance, however, that priorities may change. Risk of diversion will therefore fluctuate over time, and for reasons not always apparent to Western observers.
6. The existence and effectiveness of techniques to prevent conversion of civilian technologies to military use must be considered. In some cases the technique is one of deterrence; while diversion to military use remains possible, the likelihood that the United States would learn of such diversion and react by cutting off future technology transfers diminishes Soviet incentives to divert a given technology. The ability to conduct on-site inspections, to monitor plant output, or to incorporate in the technology devices designed to prevent reverse engineering or alteration all have this effect. It must be recognized, however, that no deterrent is infallible. The large computer installed in the Kama River truck factory, for instance, is monitored by the American firm that supplied it as part of its contractual agreement with the U.S.S.R. Periodic reports showing the allocation of computer time are made to the Department of Commerce, but there is good reason to believe that, if it is analyzed at all, this data (which arrives in the form of voluminous computer printouts) is subject only to spot checks. Another approach is to render diversion physically difficult or impossible; e.g., to seal electronic components in a medium that will destroy the component if any attempt is made to disassemble it. Such attempts are expensive and according to technical experts are rarely, if ever, infallible.
7. Finally, individual sales of technology cannot always be evaluated in isolation. Sometimes the impact of a technology transfer can only be appreciated in the context of a number of related sales that may have preceded it; the importance of a single item may derive from its position as one of a series of items that, taken together, enhance an existing capacity or provide a new one. There is, for instance, a qualitative as well as a quantitative difference between providing 5 computers and 5,000; similarly, a relatively small piece of machinery may only assume its proper importance after it is perceived as a link in the chain of an entire process that has been acquired piecemeal.

If all the preceding factors could be weighed, knowledge of the chances of a technology's enhancing the military capabilities of an adversary would be substantial. But the effectiveness of this kind of risk assessment, and the case-by-case decisions that it entails, is vitiated by two problems. The first is the absence of clear policy guidelines. The Export Administration Act of 1969 (see chapter VII) declares that it is the policy of the United States "to restrict the export of goods and technology which would make a significant contribution to the military po-

tential of any other nation or nations which would prove detrimental to the national security of the United States. " The law does not define "significance;" presumably this is left to the officials who administer the licensing process. The Department of Defense (DOD) maintains a list of criteria to be applied to the potential sale of any dual-use technology. These criteria form the basis of judgments about the probability of diversion taking place and being detected, and the consequences of such a diversion:

1. Is the item appropriate in quantity, quality, demonstrable need, design, etc., to the stated civilian end use?
2. Is there any evidence that the stated end user is engaged in military or military support activities to which this item could be applied?
3. How difficult would it be to divert this item to military purposes?
4. Could such diversion be carried out without detection?
5. Is there evidence of a serious deficiency in the military sector which this item, if diverted, would fill?
6. Is technology of military significance, which is not 'already available, extractable from this item?[4]

The answers to these questions would provide much of the information needed to make an accurate judgment of the probability of military diversion and impact of this diversion on the adversary's military capacities. This information does not, however, help those making the decisions on export licensing to evaluate the "significance" of such impacts against the objectives of U.S. strategic policy. But a yardstick against which "significance" may be measured will probably never be forthcoming.

The significance of any given improvement in Soviet or Chinese military capability and potential is almost impossible to define in the abstract. An improvement in the capacity to acquire a new military capability may not matter unless the country concerned makes the effort to translate potential into real capabilities. The significance of actual military hardware depends on whether a situation arises in which it can be put to use. How useful a given military capability may be—whether in battle or for political intimidation—may depend on the way in which the United States structures its own foreign policy or military objectives and the capabilities demanded of U.S. forces. Even if the United States were to articulate a detailed array of political/military objectives, and the force characteristics necessary to achieve these objectives, doubt would remain about the significance of incremental improvements in the military forces of potential opponents. In the absence of such a clear and explicit set of objectives, the officials who administer an export-control system must to some extent rely on commonsense and conventional wisdom.

A second problem lies in the actual administration of the case-by-case approach. Limitations on the resources available to administer export controls and the complexity of the procedures may make the system so inefficient as to be counterproductive. As chapters III and VII document, industry criticism has centered on the delays in the processing of export license applications by OEA. The volume of cases that must be handled, the volume of information that must be assembled on controversial cases, and the diversity of interests represented in the process have resulted not only in delays, but in decisions which have been subject to intense retrospective criticism on the grounds that military risk or foreign availability were improperly assessed or that foreign policy interests improperly outweighed serious military implications. Examples of such criticism may be found in the Kama River truck plant, the Bryant grinder case, and the controversy surrounding the Dresser drill-bit plant.

[4]See Jonathan B. Bingham and Victor C. Johnson, "A Rational Approach to Export Controls, " *Foreign Affairs,* April 1979, p. 889.

THE CRITICAL TECHNOLOGY APPROACH

The recognized need both to clarify policy and to simplify and sharpen the licensing procedure has caused Congress to endorse the DOD investigation of the critical technology approach to export control. This exercise, which represents a systematic effort to confront the problem of military risk through a comprehensive reappraisal of the Commodity Control List (CCL) could potentially shift the weight of present U.S. export-licensing policy from the case method to the "list approach." The critical technology approach grows directly from the findings and recommendations of the Bucy report, which may be summarized as follows:

- Design and manufacturing know-how are the most important elements in strategic technology control. Therefore, the categories of export that should receive primary emphasis are arrays of design and manufacturing know-how; keystone manufacturing, inspection and test equipment; and products accompanied by sophisticated operation, application, or maintenance know-how.
- The more active the participation of the transmitter, the more effective the technology transfer mechanism. Therefore, more active mechanisms of transfer must be tightly controlled, but product sales may be largely decontrolled since these usually do not transfer current design and manufacturing technology. Control of product sales should stress their intrinsic utility.
- The United States should preserve its strategic leadtime by denying all exports of technology that represent revolutionary advances to the receiving country. Transfers may be approved if the technology represents only an evolutionary advance, unless both nations are on the same evolutionary track. In this case, the receiving country's immediate gain from the acquisition of the technology should be assessed.
- Current U.S. export control laws should employ simplified criteria in order to expedite the majority of license requests. Currently, the absence of established criteria for evaluating technology transfers requires a cumbersome case-by-case analysis of all export applications. DOD should, therefore, develop policy objectives and strategies for the control of key high-technology fields that specifically identify the key elements of technology, including critical processes and key manufacturing equipment.
- These key elements of technology should be released only to other CoCom nations. Any CoCom nation that allows this technology to pass to any Communist country should be prohibited from receiving any further strategic know-how.
- Techniques meant to discourage diversion of products to military applications are not a meaningful control mechanism when applied to key design and manufacturing know-how, and should not be relied on to prevent diversion to military use.

The critical technology approach is predicated on the assumption implicit in the Bucy report that "one can select the subset of technologies of significant military value on which our national military technology superiority can be presumed to be most dependent."[5] It goes on to assume that this set of critical technologies will be small in number and relatively stable over time; that they can be subjected to stringent export controls that deny them automatically to any Communist country; and that the development of a Military Critical Technology Product and Information List, which will replace the present Controlled Commodity and CoCom lists, will allow the decontrol of many products

[5]Testimony of Dr. Ruth M. Davis, former Deputy Under Secretary of Defense for Research and Advanced Technology, before the Subcommittee on International Economic Policy and Trade, Committee on Foreign Affairs, U.S. House of Representatives, Mar. 22, 1979.

and processes which currently appear on the latter, but which are not in fact "critical." The approach is intended both to enhance the protection of U.S. technological leadtime and to make the export control process simpler, quicker, and more predictable by eliminating most of the present need for case-by-case review; the goal is to protect the military leadtime of the United States with minimal interference with trade.

As originally conceived, the methodology employed by DOD in the critical technology exercise may be summarized as follows:

1. Determinations of critical technology areas. The first list of military critical technologies was completed in January 1979. It identifies 15 broad areas of applied science or engineering that will serve as indicators of the fields in which the specific critical technologies to be controlled will be found. The 15 areas are:
   —computer network technology;
   –large computer system technology;
   — software technology;
   —automated real-time control technology;
   — composite and defense materials processing and manufacturing technology;
   –directed energy technology;
   —LSI-VLSI design and manufacturing technology (LSI refers to large-scale integration and VLSI to very large-scale integration in microelectronics);
   — military instrumentation technology;
   — telecommunications technology;
   –guidance and control technology;
   — microwave componentry technology;
   — military vehicular engine technology;
   —advanced optics technology (including fiber optics);
   — sensor technology; and
   —underseas system technology.
2. Determination of specific component technologies within each of these 15 areas of applied science and engineering. Various degrees of progress have apparently been made in 9 of the 15 areas listed above. This work has been accomplished by Critical Technology Expert Groups (CTEG) composed of volunteers from industry working with DOD and other Government officials. CTEGS are examining such areas as computer networks, LSI manufacturing design technology, ray processors, acoustical rays, lasers, wide-body aircraft, etc., but not all of the groups have reported their findings. DOD has testified that the date of completion of this step will be determined by the budgetary allocation, and has made no prediction of when activities in all 15 areas might be completed.
3. After completion of step 2 for each of the 15 broad areas, analysis of the military critical technologies to determine the elements of design, manufacture, utilization, testing, and maintenance functions that can be subjected to export controls. This step recognizes the fact that it may be impossible to fully control all critical technologies because some mechanisms of technology transfer may be difficult or impossible to contain; e.g., information in the public domain.
4. Recommendations as to which products, technical information, or other controllable features of each military critical technology should be placed on a list of embargoed items. This step will utilize criteria that correspond to those employed by DOD and listed above. They include the determination of foreign availability; the technological capability in and military reliance on the critical technology by the potential recipient; and the comparison of these capabilities and dependencies with those in the United States, including the rate of change of this comparative differential.
5. Formulation of a Military Critical Technology Product and Information List of items not to be exported, accompanied by a list of technology transfer mecha-

nisms effective for each of the critical items which should be subject to Government control.

At the end of this process, DOD will presumably have arrived at a list of critical products and information that should be barred from export and a list of technology transfer mechanisms that should be subject to Government control. Some assume that the United States will propose CoCom's adoption of this list in place of its present one and that it will also replace the existing CCL with the list of critical technologies. These changes may or may not be accompanied by a transfer of the main responsibility for export control from the Secretary of Commerce to the Secretary of Defense.

It is by no means clear, however, that this will be the outcome. Since its inception in the summer of 1976, progress on the critical technology approach has been slow. High DOD officials have, in the past, attributed this to inadequate resources, asserting that there have been "no technological or institutional hurdles which would prevent the implementation of the Critical Technology Approach."[6] This assertion is somewhat controversial. Discussions within DOD have indicated a lack of consensus on the aims and probable results of the critical technologies exercise. This uncertainty, as well as the conceptual difficulties inherent in the enterprise, has almost certainly contributed to the delay.

Some in DOD regard the critical technologies approach primarily as an in-house exercise. They expect that the product will not be a new form of CCL, but rather an enhanced internal capability for assessing the military impact of dual-use technologies. A variety of offices within DOD perform technical assessments for license applications. In the past, these offices have not always applied uniform criteria to the cases under their consideration.

In August 1979, those offices in DOD responsible for export licensing and those engaged in the critical technology exercise were reorganized (see chapter VII) and their activities centralized. This should provide an excellent opportunity, not only for strengthening and rationalizing the Department's role in the export-licensing process, but for defining with more precision the Department's practical expectations for a critical technologies list. At the least, an important product of the critical technologies approach should be refined and internally consistent guidelines for assessing the strategic capabilities of technologies.

It would be premature at this stage in the development of the critical technology approach to speculate on the difficulties that may arise in attempts to implement it, or on the possible consequences of its implementation. Several observations are in order, however. First, whatever the procedural outcome of the current exercise, DOD will profit from the detailed information it has gathered and the insights it has gained on the military capabilities of many technologies. On the other hand, it would be both misleading and unwise to regard the development of a critical technology list as a panacea to the difficult problem of protecting U.S. military technology leads. Skepticism already exists, both in Government circles and within the business community, as to whether the revised lists will indeed be shorter than present ones; there is fear, in other words, that reluctance to decontrol items or a broad definition of criticality will result in similar or longer lists. This might further inhibit East-West trade and could also provoke objections among some members of CoCom. From the other side, there are fears that a critical technology list will be too short, i.e., that items of marginal, but potentially important, military utility will be decontrolled to the ultimate detriment of the United States.

It is highly likely that, whatever the outcome, the list will be criticized, either for the items it includes or excludes. The belief that a critical technology list can ever be entirely noncontroversial rests on the assumption that definitive, highly refined, empirical judgments can be made regarding the mili-

[6] Ibid.

tary utility of a myriad of products and processes. This is unlikely. In the final analysis, inclusion on such a list requires judgments on the part of policy makers; the issues are not purely matters of technical or scientific "fact." Moreover, it is dangerous to assume that the existence of a critical technologies list can in itself obviate the case-by-case review. Considerations of both foreign availability and end use can never be entirely eliminated; simply because an item appears on a U.S. list of embargoed technologies does not prevent its export from abroad; and simply because an item does not appear on this list does not mean that under certain circumstances it could not constitute a significant improvement in the strategic position of an adversary. Finally, because the cutting edge of technology moves so rapidly, any list must be subject to constant review and update.

Those involved in the critical technology effort recognize these problems. One important aim of their activities is to substantially decrease the volume of cases that are presently subjected to detailed case analysis so that resources may be concentrated on those cases involving difficult judgments. In order for this to occur, however, methods must be devised to screen export applications to the Communist world–not necessarily in the exhaustive manner that pertains now, but in some way that will "catch" potentially troublesome cases involving technologies that do not appear on the critical technologies list, assuming that this list is generally viewed as comprehensive without being overly inclusive. One might imagine a system that proceeded roughly in the following manner:

1. All requests for export licenses to the Communist world would be subjected to an initial screening process. The criteria applied here would reflect the concerns of all the executive departments involved in licensing and might ask such questions as:
   – Is the item on the critical technologies control list? If so, presumably no further inquiry is necessary. If not,
   – Is the stated end use plausible?
   — Are large amounts of training entailed in the sale?
   – Is there any obvious military relevance, even if this is not "critical"?
   – Have inordinately large quantities of this equipment been exported?

   The object is to raise a "red flag;" to catch-out potentially troublesome cases. In this way, the volume of cases that require further review should be greatly reduced and the serious "log-jam" which presently plagues the licensing procedure substantially eliminated.
2. Any case in which a red flag appears would then be subject to a moderate degree of examination specifically targeted to answer the particular objection raised in the first cursory screening.
3. Should this moderate examination not resolve the problem, an analysis similar to the intensive case-by- case review presently conducted by OEA should be conducted.
4. In addition, random checks should be made to ensure that the procedure is producing the desired results. These might take the form of periodically selecting isolated applications that otherwise would have been granted after step 1 and subjecting them to the deeper consideration of steps 2 or 3.
5. In cases where threat of reverse engineering or diversion appears to be a major problem, an analysis should be conducted of the procedural or technical mechanisms that could minimize the dangers.

SUMMARY

The process outlined above is intended as nothing more than a suggestion for a way of thinking of export control in a manner that combines the case study and list approaches discussed here. It should be apparent that unless both are utilized, no one formula can resolve the immensely complex issue of determining which technologies make "significant contributions" to the military capacities of our adversaries, and no simple procedure is likely to soon be instituted to protect such technologies. The protraction of the critical technology exercise itself indicates the extreme difficulty which confronts even the Nation's foremost technical experts in making recommendations in these areas, and should caution all observers of the folly of expecting magical automatic solutions to such complex problems. Western technology has undoubtedly contributed to Soviet military capabilities in the past and it will continue to do so in the future, regardless of any unilateral efforts the United States could undertake. There is no reason to believe that drastic changes in DOD's efforts in the area of export control will materially alter this situation. In the final analysis, the national security of the United States is most surely protected by its maintenance of technological leads in those areas that have been deemed militarily critical.