How Technology Security Supports Security Assistance

By

Dr. Stephen D. Bryen
Deputy Under Secretary of Defense for Trade Security Policy, and Director, Defense Technology Security Administration

President Reagan already has alerted the American people to the critical importance of technology security. The President's statement on "Strategic Technology Export Controls," which was published in the Winter, 1988 issue of *The DISAM Journal*, noted the costly Toshiba-Kongsberg diversions of submarine technology to the Soviet Union.[1] The statement pointed out the subsequent improvements in export controls that have been instituted by the governments of Japan and Norway, and also called on all U.S. allies to strengthen their strategic trade control systems. Let me give you some background on the President's statement, explain more recent developments, and make clear why our technology security program is vital to the success of your efforts in security assistance management.

ROLE OF TECHNOLOGY IN NATIONAL DEFENSE

Secretary Carlucci's annual report to Congress lists four programs under "Collective Security." These are: regional security, security assistance, international armaments cooperation, and technology security. This juxtaposition shows that both of our programs--security assistance and technology security--are integral parts of the overall effort at collective security that stands at the base of our national security policy. Organizationally, the Defense Security Assistance Agency (DSAA) and the Defense Technology Security Administration (DTSA) play mutually reinforcing roles.

National security export controls have had strong support in the United States for nearly 40 years. The reason is that protection of advanced technology is central to our entire postwar strategy for defense and foreign policy.

Since the founding of NATO, the United States and its allies have counted on superior economic productivity and technological innovation to offset Soviet military and political pressures. Because we are democracies and consumer-oriented societies, we have not matched our Soviet adversaries in numbers--soldier for soldier, tank for tank, aircraft for aircraft.

For the past 20 years the Warsaw Pact has maintained a lead of more than 2-to-1 over NATO in main battle tanks and about 2-to-1 in combat aircraft. In the same period it has increased its advantage in artillery from less than 2-to-1 to over 3-to-1. Since 1965, NATO has lost its advantage in surface-to-air missiles and combat helicopters, with the Eastern Bloc now holding a lead of more than 2-to-1 in surface-to-air missiles and a smaller lead (1.3-1) in helicopters. The Warsaw Pact now also has an advantage of about 3-to-1 in infantry fighting vehicles.

In the past 10 years the Soviet Union has built 3,000 land- and sea-based ballistic missiles, the United States 700; the Soviet Union 25,300 tanks, the United States 7,600; the Soviet Union 27,300 artillery pieces, the United States 3,200.

To offset these large numbers, the Western allies rely on the technological edge provided by the brains and organizing abilities of our scientists, engineers, and businessmen. This requires that

the United States continually seek improvement in our defense-related science and technology. We do this through the support of basic research at laboratories and universities and through reliance on the competitive forces at work in private enterprise. For example, the semiconductor industry finances most of its research and development (R&D) from commercial sales. Yet, it has provided much of our lead over the Soviet Bloc in military systems that depend on computers and microelectronics.

As you in the security assistance field are well aware, the United States also strengthens its defense through the selected sharing of technologies with our allies. Under the NATO aegis, we join our European allies in cooperative projects to capitalize on the combined technological and industrial capabilities of the Western alliance. We work together to establish the requirements for many weapon systems. The United States also is trying to achieve greater cooperation in military technology with Japan.

Such cooperation in defense-related technology is heavily influenced by the overall economic climate. Cooperation among the United States, Europe, and Japan has increased in the 1980s as the world's market economies have been revitalized.

THE SOVIET THREAT TO WESTERN TECHNOLOGY

To be effective, technology development and technology cooperation must be reinforced by technology security. It does us little good to outpace the Soviet Union in R&D and production capabilities if the Soviets are able to acquire the fruits of our efforts and use them to improve their weapons.

Here we face a serious and continuing problem. The Soviet Union is pursuing a two-track effort to overtake the West in military technology. First, the Soviets are working hard to improve their own national capabilities in order to surpass the West in basic weapons technology. They invest heavily in their own R&D base, and have outspent the United States in military research, development, test, and evaluation every year since 1972. They also free their defense-industrial ministries from bottlenecks that throttle production in other ministries. In the 1980s the Soviet defense-oriented ministries have served as models of efficiency for their civilian ministries.

The second Soviet track is one that concerns us here. This is a well planned and wide-ranging campaign to obtain by legal and illegal means Western technology that has military uses. We have only begun to realize the full scope of that effort in the last two or three years.

The USSR acquires from the West about 6,000 to 10,000 pieces of hardware and more than 100,000 technical documents. These acquisitions pay off. According to Soviet estimates, an average of more than 5,000 military projects benefit each year from Western hardware and documents. [2] For example, Western technology has enhanced the T-72 and T-80 tanks, new fighter and ground attack aircraft, artillery fuzes and shells, and submarines and surface warships. Western technology also has contributed significantly to electronics and microelectronics systems and to radars and computers that support ground, naval, air, and space operations.

TOSHIBA-KONGSBERG SALES

The most dramatic recent example is the sale by European and Japanese companies of propeller manufacturing technology to the Soviet Navy. This technology has helped make Soviet submarines substantially quieter and hence allow them better to avoid detection by U.S. and allied anti-submarine forces. The new technology gives the Soviets a windfall of historic proportions in anti-submarine warfare, which Admiral Crowe, Chairman of the Joint Chiefs of Staff, calls "one of the great technological fights going on in the world right now."[3] Thus, the Soviet Navy will overcome with Western assistance many of the vulnerabilities about which it learned from the

Walker spy ring and which it could not have overcome alone. The United States will have to spend several billion dollars to compensate for these losses.

This quantum jump in undersea capability reinforces the long-term Soviet drive for a blue water navy that can harass and hobble NATO at sea. Quieter and less vulnerable attack submarines would be better able to disrupt the trans-Atlantic sea lines of communication during a war in Europe. These lines would be critical for resupply of weapons and equipment from North America to Europe, just as they were in the two world wars.

Quieter Soviet attack submarines also are more dangerous for Western ballistic missile submarines. This is disturbing for the United States, but even more so for our entire collective security system and the security assistance program. Two of our major allies, the United Kingdom and France, depend on a handful of missile-launching submarines for much of their strategic nuclear force. These national deterrents are now at greater risk, because of the actions of a few executives and engineers from allied nations.

POLICY IMPLICATIONS

The Toshiba-Kongsberg case drives home the growing importance of foreign technology for United States security. The Soviet Navy gained Japanese and Norwegian technology, not American technology. Advanced technology with critical military uses is becoming sufficiently widespread that our security can be put at risk through the loss of technology by our allies and friends. This fact has major implications for our security assistance programs.

Toshiba-Kongsberg sales indicate that the Soviets can obtain high technology illegally even from well-known corporations. The firms involved were not back-room operations or mail fronts for technobandits, but the type of solid, established companies that always were assumed to obey the law and to maintain tight internal security. Toshiba Machine is a subsidiary of one of the largest, most technologically advanced, and most commercially reputable Japanese corporations. Kongsberg Trading Company was (before its dissolution) a division of Kongsberg Vaapenfabrikk, which is owned by the Norwegian Government. Moreover, one Member of Congress has noted that this was not a "rogue operation" but a "conscious corporate decision made at the highest levels of these companies."[4]

Recent investigations indicate that more than these two firms have diverted machine tool technology to the USSR through falsified papers. The Norwegian police report on the Kongsberg case, which was issued in October 1987, stated that machine tool builders in France, West Germany, and Italy also had shipped goods to the Soviet Union in violation of their export control regulations. In April 1988, the Government of France announced the arrest of several executives of a French company, Forest Line, for selling the USSR the equipment to produce turbine blades used in advanced jet engines.

The Toshiba-Kongsberg sales have shaken the Western alliance more than any strategic trade case in recent memory. All Americans must be disturbed that the Soviet Union easily penetrated to the inner core of the Western high tech and defense establishment. There is a particularly sobering lesson here for those of us concerned with security assistance. We must ensure that the United States is sufficiently careful in approving transfers of military technology that this technology will not get to the Soviet Bloc and be turned against us.

U.S. POLICIES TO PROTECT ADVANCED TECHNOLOGY

The United States has followed consistent policies to meet this Soviet threat. The legislative basis for protecting the U.S. technological lead was established soon after World War II. The Export Control Act 1949 stated that the United States could prohibit any exports of "potential

military significance." This language was slightly modified in the Export Administration Acts of 1969, 1979, and 1985 to refer to exports that would make a "significant contribution to the military potential" of any country or combination of countries which would "prove detrimental to the national security" of the United States.[5]

Such export controls were soon made part of the broader Western policy of collective security. The multinational organization that was established to enforce these controls--the Coordinating Committee for Multilateral Export Controls, or COCOM--has been a near replica of NATO in terms of membership. NATO began functioning in late 1949 in Paris, COCOM in early 1950 and also in Paris. COCOM soon included all original members of NATO except Iceland, plus West Germany, which joined NATO in 1955. Greece and Turkey joined NATO in 1952, COCOM in 1953. Japan joined COCOM 1952, the year that the peace treaty, which included a security assistance pact with the United States, came in effect. Some three decades later, Spain joined NATO in 1982 and COCOM in 1985.

COCOM recently has expanded its controls over equipment and technologies that form the strategic infrastructure of the 1980s. In particular, computers and microelectronics have revolutionized such critical military functions as command and communications, missiles, and air defense. In 1976 the influential Bucy report of the Defense Science Board noted that the "mere presence" of large computer installations "transfers know-how in software" and "develops trained programmers" and other personnel. All of this could be "redirected to strategic applications."[6] After a two-year list review ending in July 1984, COCOM agreed to control industrial robots, electronic grade silicon, printed circuit boards, high-speed super mini-computers, and small computers with battlefield applications. It also established its first comprehensive controls on computer software and sophisticated telecommunications switching equipment. Simultaneously, COCOM recognized legitimate East-West trade objectives by raising the ceiling on mainframe computers by 50 percent capacity and by decontrolling many personal computers. Since 1984, COCOM has been involved in a continuing review of the control list.

Efforts are now underway to strengthen the existing controls on items such as superconducting materials and metals, computer software, superprecision measuring equipment, photosensitive devices, acoustic wave devices, electronic materials, lasers, recording equipment, power sources, and microwave components. The United States also wishes to add to the control list sensitive technologies such as coating processes, substrates, and coating materials of a strategic nature.

STRENGTHENING ENFORCEMENT OF EXPORT CONTROLS

Most recently, COCOM governments have moved to tighten the enforcement of export controls and to establish greater uniformity in the enforcement of controls and in the prosecution of violations. This is the area to which President Reagan referred in the statement printed in the Winter issue of *The DISAM Journal.*

COCOM members have differed very widely in these areas. For example, the United States assigns several hundred officials to review license applications and to enforce export control regulations. The U.S. Export Administration Act of 1985 punishes violations of these regulations with prison terms of up to ten years.[7] The Department of Defense, which has the strongest stake in the success of export controls, plays a vigorous role in U.S. Government policymaking.

By contrast, prior to the Toshiba-Kongsberg case, Japan apparently assigned only 40 full-time officials to export licensing. There was no role for the Japan Defense Agency. Some COCOM governments still have no criminal sanctions for violations of national security that often do more damage than traditional espionage. In the wake of Toshiba-Kongsberg, Japan and Norway have strengthened their licensing and enforcement systems. But some other governments

have moved very slowly to investigate the problems revealed by these sales and by the Norwegian police report.

We need real reciprocity in COCOM. A technobandit indicted in one Western country should be treated as an outlaw in all. I believe that each COCOM nation should agree to take effective action against any firm--whether foreign or domestic--that illegally exports goods on the control list. This approach will require a faster and more systematic sharing of information on potential diversions among customs and law enforcement agencies. It also will require criminal penalties severe enough to deter potential violators. The United States has made clear that as COCOM governments take such steps, we can begin to remove the remaining restrictions on the transfer of technology within COCOM.

The Reagan Administration has moved forcefully to encourage our allies to take the necessary steps. We successfully pressed for a special COCOM meeting last July, at which member countries agreed to give greater attention to licensing and enforcement. We took the lead in preparing a Special Political Meeting of COCOM governments held in Versailles in January 1988. The United States delegation was headed by Deputy Secretary of State Whitehad, an indication of the importance the Administration attaches to COCOM improvement. That meeting focused on enforcement as the key means to prevent any future Toshiba-Kongsberg cases. All governments agreed to share information on potential diversions, to cooperate more effectively to stop such diversions, and to work closely with non-COCOM countries to strengthen the protection of Western high technology.

PROTECTING HIGH TECHNOLOGY IN NEUTRAL COUNTRIES

As you in the security assistance field know, high technology--including military high technology--has been spreading beyond the United States, Europe, and Japan to neutral and nonaligned nations. This complicates technology security even further. In the early 1980s the Defense Department and the intelligence agencies discovered that the Soviet Union was penetrating--at times almost plundering--many of these countries. The USSR was turning to these nations, which usually had weak or nonexistent export control and industrial security systems, to get the Western technology it could no longer acquire readily from COCOM countries.

In January 1985, President Reagan directed DOD to review proposed exports to 15 countries in eight strategically important fields of high technology. These included neutral European nations, rapidly industrializing nations in East and South Asia, and Middle Eastern countries with close ties to the Soviet Union. This DOD review has ensured that high tech exports would have to meet the criteria of U.S. national security interests, bolstered by the most current information from our intelligence agencies. We immediately began to spot, and stop, proposed exports that posed a clear risk of being diverted from the recipient country to the Soviet military. These actions alone made the program a success from the standpoint of national defense and savings for the taxpayer on future defense budgets.

But the Administration had a positive rather than a negative goal in mind. We wanted to encourage legitimate trade in high technology. Therefore, the United States began negotiations with several neutral and nonaligned nations to improve their export control systems as a means of receiving higher levels of American technology. We have been backed by allied governments through the COCOM "third country initiative." Congress has given formal legislative sanction to this element of U.S. policy. Section 5.(k) of the Export Administration Act of 1985 states that whenever negotiations with non-COCOM countries produce "agreements on export restrictions comparable in practice" to those maintained by COCOM, the United States shall treat exports to those countries "in the same manner" as exports to members of COCOM.[8] Many representatives of neutral nations have stated candidly that they planned to tighten their procedures for technology security in the expectation of gaining "5k treatment" with regard to U.S. high tech exports.

The results of this program have been impressive. Since the Defense Department began reviewing these license applications:

- Nearly 50 percent of the 15 countries DOD reviewed have been dropped from the list because they have adopted COCOM-like programs to protect our technology.
- All the neutral countries in Western Europe have adopted COCOM-like controls and backed them with national laws.
- DOD review has prevented sensitive goods from going to Iran, Libya, and Syria.
- Soviet and East Bloc operatives gathering technology for the Soviet armed forces have found many of their contracts divided up and their diversion networks shut down.

Most importantly, this success has made COCOM credible again. It has shown that the United States and its allies can protect their militarily-applicable technology despite the internationalization of high technology. COCOM governments recognized this fact when for the first time they endorsed the third country initiative publicly at the Versailles political meeting.

Let me add that this DOD effort has had important technical spin-offs for American exporters and American national security. The Defense Department has reviewed over 38,000 license applications, all within strict time constraints. The Administration has proved the effectiveness of automated case processing and of an electronic data link between the Departments of Defense and Commerce. Other COCOM governments, notably France, are now setting up computerized systems. It is hard to remember that, prior to the Reagan Administration, export controls proceeded ponderously by means of hand-carried documents and antiquated filing and retrieval systems.

IMPLICATIONS FOR SECURITY ASSISTANCE

These broad national security policy considerations have direct implications for the management of security assistance and arms cooperation. We know that there are major benefits to sharing the development and production of military systems with allied and friendly governments. These benefits range from improved standardization and interoperability to reduced costs resulting from shared development efforts, the elimination of duplication of efforts, and potential economies of scale in production. An increasingly important benefit of co-development is the synergistic effect achieved when U.S. and European industries combine their technical expertise to achieve weapon advances which meet the common threat from the Warsaw Pact. The growing sophistication of European armament industries is a resource which can benefit the entire alliance.

Nevertheless, our description of Soviet efforts to gain Western technology show that decisions to share advanced technology in key areas can have serious risks. Co-development involves the application of emerging technology years before a weapon system is to be fielded. Therefore, any compromise could permit the enemy to exploit the technology for his own weapons, or to develop countermeasures even before the United States and our allies could produce the new weapon. Compromises of technology could have devastating results on future battlefields.

I have explained that U.S. allies in COCOM share our commitment to technology security and are working to tighten up their own control systems. Nevertheless, Eastern bloc intelligence services are making major efforts to penetrate Western defense industries, as we saw in the Toshiba-Kongsberg case. Obviously, the greater the number of persons who know a secret, and the greater the Soviet effort to learn that secret, the greater the possibility of a compromise. The Department of Defense must define carefully the risk inherent in any decision to transfer advanced technology abroad, and must weigh this risk to our collective security against the benefits to collective security.

The underlying national and DOD policy that guides technology transfer at any level is that classified and export-controlled military information is a national security asset which must be conserved and protected. It may be shared with foreign governments only when there is a clearly defined advantage to the United States. Preservation of the U.S. defense industrial base is also a key consideration.

CASE STUDY IN TECHNOLOGY SECURITY

The Multiple Launch Rocket System (MLRS) co-development effort is an excellent example of how this policy objective is served.[9]

The MLRS is an all-weather, rapid-fire, non-nuclear system designed to supplement other weapons available to a division or corps commander for the delivery of a large volume of fire in a very short time against critical, time-sensitive targets. A basic memorandum of understanding (MOU) on a cooperative program for a medium multiple launch rocket system was signed by the United States, United Kingdom, Germany and France in July 1979. The MOU encompasses the development of a multiple launch, free flight rocket system that will satisfy the agreed tactical requirements of all four participating countries.

The MLRS program calls for a three phase cooperative effort. In Phase I, the United States developed the system to include the rocket and an improved conventional submunition warhead. Concurrently in Phase II, Germany developed a scatterable antitank mine warhead. Italy joined Phase I and Phase II of the program in fiscal year 1982. Phase III involved the cooperative development of a terminal guided warhead (TGW) for the attack of enemy armor vehicles. In December 1983 the participants signed an MOU Supplement initiating the TGW Cooperative Development Program. The program has been carried out by an international consortium composed of five major defense firms.

Technology transfer and security issues concerning the MLRG-TGW program are addressed by a Security and Technology Transfer Working Group (STTWG) composed of government representatives from the partner nations and chaired by the U.S. representative. Classified information relating to critical military technologies has been shared among the governments of the participating nations. This "background" information set a baseline for the development effort. Technological advances made during development have been appropriately classified and identified as "foreground" information. This foreground information has been shared among the partners but cannot be released outside the program without the unanimous consent of all the participating governments.

The STTWG also has addressed such other problems as the international transfer of classified hardware, the expedited handling of classified visits, the provision of secure communications among the contractors, and the certification of secure facilities for foreign-owned concerns. Many of these problems were faced for the first time in the MLRS-TGW program. It took firm insistence by the Defense Technology Security Administration to ensure that this cooperative program took full account of U.S. and allied security considerations.

HOW YOU CAN HELP

Each of the military services maintains technology security offices that contribute to the overall DOD effort to protect our technological edge over our adversaries. Moreover, the Defense Technology Security Administration works closely with the military services and Defense Security Assistance Agency in developing security procedures for cases like that of the MLRS-TGW.

Officers who attend the Defense Institute of Security Assistance Management can help strengthen our technology security on their next tours of duty by helping achieve a balanced approach to technology transfer in the arms sale cases they work. They can play a particular role abroad in explaining to allied and friendly military officers and government officials why it is that the United States insists on stringent security measures and why such measures contribute to the collective security of both nations. Often, foreign officials do not know of U.S. requirements and must be informed on why the United States insists on them.

U.S. officers working on security assistance can also help the technology security program by informing DOD of problems they foresee in the security program by advising DOD of problems they foresee in the security procedures of foreign governments. If we can jointly tackle these problems before they become serious and lead to a loss of technology, we are much more likely to preserve a permanent relationship in sharing weapons systems and technologies with the foreign government.

We must all keep in mind that the United States and our allies depend on our technological edge to offset the numerical advantage of the massive Soviet military machine. From this perspective, we can see that technology security is critical to our collective security policies and that technology security and security assistance must be mutually reinforcing.

NOTES:

1. President Ronald Reagan, "Strategic Technology Export Controls, *The DISAM Journal of International Security Assistance Management* (Vol. 10, No. 2; Winter 1988), p. 57.
2. U. S. Government, *Soviet Acquisition of Militarily Significant Western Technology: An Update* (Washington, September 1985), p. 6.
3. Quoted in Tim Carrington, "The Silent War: Undersea Arms Race Is Preoccupying Navies of U.S., Soviet Union," *The Wall Street Journal*, June 24, 1987, p. 1.
4. Congressman Charles Wilson (Democrat, Texas). Statement made at U.S. Congress, House of Representatives, Subcommittee on International Economic Policy and Trade, of the Committee on Foreign Affairs, *Hearing on Policy Implications and Proposed Legislation Concerning the Toshiba-Kongsberg Diversion Case*, June 30, 1987 (draft transcript, p.12).
5. The Export Control Act of 1949, section 1(b). The Export Administration Act of 1969, Public Law 91-184, 83 Stat. 841, section 3(1)(B); see also section 2(2). The Export Administration Act of 1979, Public Law 96-72, 93 Stat. 503, section 3 (2) (A); see also section 2 (5). The Export Administration Amendments Act of 1985, Public Law 99-64, Public Law 99-64, retains these sections of the 1979 act.
6. *An Analysis of Export Control of U.S. Technology--A DOD Perspective. A Report of the Defense Science Board Task Force on Export of U.S.Technology*, February 4, 1976 (Washington: Office of the Director of Research and Engineering, 1976), p. 25. This is often called the "Bucy Report," named for the task force chairman, J. Fred Bucy, Executive Vice President of Texas Instruments.
7. The Export Administration Amendments Act of 1985, Public Law 99-64, sections 11 (a) and (b).
8. The Export Administration Amendments Act of 1985, section 5.(k) Negotiations, With Other Countries.
9. I am relying primarily on the narrative of the MLRS-TGW case prepared by Lieutenant Colonel Bradley W. Smith, Office of the Deputy Chief of Staff for Intelligence, Department of the Army.