

AD-A208 010

# STUDY PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

## INTERNATIONAL TECHNOLOGY TRANSFER AS PRACTICED BY THE U.S.S.R: IMPLICATIONS FOR U.S. NATIONAL SECURITY

BY

MARVIN D. REDD, SR.

DTIC  
ELECTE  
MAY 23 1989  
S D

**DISTRIBUTION STATEMENT A: Approved for public  
release; distribution is unlimited.**

12 FEBRUARY 1989



U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

| REPORT DOCUMENTATION PAGE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                       | READ INSTRUCTIONS<br>BEFORE COMPLETING FORM                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|----------------------------------------------------------------|
| 1. REPORT NUMBER                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2. GOVT ACCESSION NO. | 3. RECIPIENT'S CATALOG NUMBER                                  |
| 4. TITLE (and Subtitle)<br>International Technology Transfer as Practiced by<br>the USSR: Implications for U.S. National Security                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                       | 5. TYPE OF REPORT & PERIOD COVERED<br>Individual Study         |
| 7. AUTHOR(s)<br>Marvin D. Redd, Sr.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                       | 6. PERFORMING ORG. REPORT NUMBER                               |
| 9. PERFORMING ORGANIZATION NAME AND ADDRESS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                       | 8. CONTRACT OR GRANT NUMBER(s)                                 |
| 11. CONTROLLING OFFICE NAME AND ADDRESS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                       | 10. PROGRAM ELEMENT, PROJECT, TASK<br>AREA & WORK UNIT NUMBERS |
| 14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                       | 12. REPORT DATE<br>12 Feb 89                                   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                       | 13. NUMBER OF PAGES<br>27                                      |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                       | 15. SECURITY CLASS. (of this report)<br>Unclassified           |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                       | 15a. DECLASSIFICATION/DOWNGRADING<br>SCHEDULE                  |
| 16. DISTRIBUTION STATEMENT (of this Report)<br>Approved for public release; distribution is unlimited.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                       |                                                                |
| 17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                       |                                                                |
| 18. SUPPLEMENTARY NOTES                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                       |                                                                |
| 19. KEY WORDS (Continue on reverse side if necessary and identify by block number)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                       |                                                                |
| 20. ABSTRACT (Continue on reverse side if necessary and identify by block number)<br>In its broadest sense, technology transfer encompasses the collection, documentation and dissemination of scientific and technical information, including data on the performance and costs of using the technology; the transformation of research and technology into processes, products, and services that can be applied to public or private needs; and the secondary application of research or technology developed for a particular mission that fills a need in another environment. <sup>1</sup> The above perspective of technology transfer is a benign one; one which takes place among and between amicable |                       |                                                                |

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE(When Data Entered) 4

and cooperating sociopolitical, cultural and/or national friends. The following paper examines the more notorious side of the technology transfer issue, with especial emphasis on its practice by the Soviet Union, who, through copying, espionage, and blatant thievery, sooner or later acquire western technology for themselves and Warsaw Pact nations. Forms of technology transfer are scrutinized through the use of several case studies and finally the efforts used by the U.S. at deterring this leaching away of one of the bulwarks of western-nation national security are surveyed.

---

1            A. B. Linhares, Introduction, Directory of Federal Technology Transfer. Executive Office of the President, Federal Coordinating Council for Science, Engineering and Technology, p.v.

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE(When Data Entered)

USAWC MILITARY STUDIES PROGRAM PAPER

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.



INTERNATIONAL TECHNOLOGY TRANSFER AS PRACTICED BY THE U.S.S.R:  
IMPLICATIONS FOR U.S. NATIONAL SECURITY

AN INDIVIDUAL STUDY PROJECT

by

Marvin D. Redd, Sr.

Major Samuel J. Newland  
Project Adviser

**DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.**

U.S. ARMY WAR COLLEGE  
Carlisle Barracks, Pennsylvania 17013  
12 February 1989

|                                      |                                           |
|--------------------------------------|-------------------------------------------|
| Accession For                        |                                           |
| NTIS                                 | CRA&I <input checked="" type="checkbox"/> |
| DTIC                                 | TAB <input type="checkbox"/>              |
| Unannounced <input type="checkbox"/> |                                           |
| Justification                        |                                           |
| 3y                                   |                                           |
| Distribution/                        |                                           |
| Availability Codes                   |                                           |
| Dist                                 | Availability for Special                  |
| A-1                                  |                                           |

## ABSTRACT

AUTHOR: Marvin D. Redd, Sr.

TITLE: International Technology Transfer as Practiced by the  
U.S.S.R.: Implications for U.S. National Security

FORMAT: Individual Study Project

DATE: 12 February 1989 PAGES: 23 CLASSIFICATION: Unclassified

In its broadest sense, technology transfer encompasses the collection, documentation and dissemination of scientific and technical information, including data on the performance and costs of using the technology; the transformation of research and technology into processes, products, and services that can be applied to public or private needs; and the secondary application of research or technology developed for a particular mission that fills a need in another environment.<sup>1</sup> The above perspective of technology transfer is a benign one; one which takes place among and between amicable and cooperating sociopolitical, cultural and/or national friends. The following paper examines the more notorious side of the technology transfer issue, with especial emphasis on its practice by the Soviet Union, who, through copying, espionage, and blatant thievery, sooner or later acquire western technology for themselves and Warsaw Pact nations. Forms of technology transfer are scrutinized through the use of several case studies and finally the efforts used by the U.S. at deterring this leaching away of one of the bulwarks of western-nation national security are surveyed.

---

<sup>1</sup> A. B. Linhares, Introduction, Directory of Federal Technology Transfer. Executive Office of the President, Federal Coordinating Council for Science, Engineering and Technology, p. v.

## TABLE OF CONTENTS

|                                                                    | Page |
|--------------------------------------------------------------------|------|
| ABSTRACT.....                                                      | ii   |
| CHAPTER I. OVERVIEW.....                                           | 1    |
| II. TECHNOLOGY TRANSFER: HOW IT HAPPENS.....                       | 3    |
| III. AT STAKE: ECONOMIC SOLVENCY AND MILITARY<br>BALANCE.....      | 7    |
| IV. NATIONAL SECURITY CONCERNS: MILITARY<br>STRATEGIC ASPECTS..... | 12   |
| V. SELECTED CASE STUDIES ON TECH TRANSFER.....                     | 15   |
| VI. EFFORTS AT DETERRENCE.....                                     | 19   |
| VII. CONCLUSIONS.....                                              | 22   |
| BIBLIOGRAPHY.....                                                  | 24   |

INTERNATIONAL TECHNOLOGY TRANSFER AS PRACTICED BY THE U.S.S.R:  
IMPLICATIONS FOR U.S. NATIONAL SECURITY

CHAPTER I

OVERVIEW

In the Annual Report to the Congress submitted by Secretary of Defense Frank C. Carlucci for fiscal year 1989, one of the cornerstone national security objectives was posited as follows: *To prevent the transfer of militarily critical technology and knowledge to the Soviet bloc, and to other potential adversaries.* Obviously, the protection of U.S. technological advances that may be directly or indirectly relatable to military application by the U.S.S.R. is vital to our national interests.

The use of another country's technology to further the scientific, but more often militarily-related objectives is certainly not a recent phenomenon. Rather, this practice has been an ongoing one even before man concentrated his interests between geopolitical/social/cultural boundaries. The invention of what we know to be the wheel by prehistorics and the introduction of gunpowder by the Chinese and its refinements and evolution by subsequent cultures are well-known examples of mankind's emulation, expansion and use of a knowledge base begun by a "genesis" entity.

Perhaps the most extreme, well-documented and provocative example of technology transfer was in the case of the U.S.S.R's acquisition of the technology required to fashion their own atomic device. As this technology transfer was by means centered in espionage against the United States, it did not follow the more traditional form of transfer which is in vogue today.

"For nearly two decades, the Soviet Union has maintained a massive, national program to acquire critical military-related Western technology. Soviet military decision makers acquire such technology through legal and illegal channels. Their acquisition strategy is, in fact, coordinated at the highest levels of their government. Such a well-defined effort poses a direct military threat to the security of the United States and its allies."<sup>1</sup>

In the future, the stakes involved in the denial of U.S. technology transfer to the Soviet and bloc nations may be appreciably higher, with potentially more expensive and more lethal consequences for failure.

1. Office of the Undersecretary of Defense for Policy, Assessing the Effect of Technology Transfer on U.S./Western Security - A Defense Perspective-, February 1985, p. E-1.

## CHAPTER II

### TECHNOLOGY TRANSFER: HOW IT HAPPENS

Technology transfer occurs in one of four possible ways:

- Legal transfer
- Espionage and other illegal activities
- Battlefield exploitation
- Parallel development

Of the four, the legal transfer of technology is the most common. The U. S. Department of Commerce is responsible for overseeing the sale of advanced technology to foreign countries and has the difficult task of balancing the needs of a free enterprise economy with the requirements of national security. The Department of Defense has criticized the Commerce Department recently for lax oversight, pointing to the easy access the Soviets have to vast unclassified U. S. computer data bases.

Each year, the Soviets obtain nearly half a million unclassified U. S. documents on technical subjects.<sup>1</sup> This has enabled them in recent years to narrow the U. S. lead in nearly all key technological areas, particularly microelectronics, and to overtake the West in some other key areas.<sup>2</sup> The enormous strides the Soviet have made in recent years in the area of semiconductors had its basis in the legal sales of Western equipment to third-party countries, which in turn made the technology available to the Soviet Union.<sup>3</sup>

In Proceedings, the U.S. Naval Institute magazine, advertisements routinely describe the latest innovations in military hardware. In a recent edition, the reader was invited to "eavesdrop on the unseen. [The] Compact Towed Array Sonar System gives ultra-sensitive performance...is totally passive and operates at an extremely low frequency, so the target is never alerted. It weighs only 8 tons...." While advertisements like these in many score other periodicals do not provide specific technical information, they nevertheless do give the Soviets and other countries with inimicable attitudes towards the west a fairly accurate idea of the kinds of systems being developed by western industries. When the Soviets wed that information to what they gather through espionage and other transfers of Western technology, they have what they need to mimic and frustrate U. S. weapons- and[in this case] perhaps to defeat the U. S. Navy in some future battle.<sup>4</sup>

Battlefield exploitation provides another penetration point for the Soviets to gain insight to Western advanced technology. The methodology of reverse engineering is employed, wherein only a component part of an entire system is necessary for Soviet scientists to imaginatively fabricate and mimic the operation of the entire system.

This problem amplifies in peacetime when actual ordnance expenditures are relatively rare but the enemy has plenty of time to exploit his finds.<sup>5</sup> In the 1986 raid on Libya, the Navy could have used submarine-launched conventional Tomahawk land-attack cruise missiles(TLAM-C). If it had, and Libyan coastal air defenses had shot down a TLAM-C or one had failed to function properly, this front-line weapon could have been compromised. The Libyans would have reaped a political and financial bonus by selling the missile to the Soviets, who then could have dissected the missile's logic and guidance systems and improved their own systems or developed a counter to those of the United States.<sup>6</sup>

Parallel development provides the final method of technology transfer. They find ideas for new technology in open-source Western literature-such as advertisements in defense industry journals [as already mentioned] and exhibits at open symposia-and in their observations of operational Western systems.<sup>7</sup> The Soviets mimic technological concepts from many different sources and apply them to military applications. The uncanny similarity between the U. S. space shuttle and the one the Soviets recently launched is but one example.

1. Kathryn Jones, "CIA Official Expects Soviets to Step up Industrial Spying", Dallas Morning News, 17 February 1988.
2. *Soviet Acquisition of Military Significant Western Technology, An Update*, September 1985, p. 1. Report on hearings before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, U. S. Senate, 97th Congress.
3. CDR Marc D. Goldberg, "Rapping Ivan's Sticky Fingers", Proceedings, October 1988, p. 74.
4. Ibid., p. 69.
5. Ibid., p. 75.
6. Ibid., p. 76.
7. Ibid., p. 76.

## CHAPTER III

### AT STAKE: MILITARY BALANCE AND ECONOMIC SOLVENCY

#### U.S.DEFENSE COSTS=POTENTIAL SOVIET SAVINGS

It has been repeatedly demonstrated that the military requirements of the Soviets are preeminent in their pursuit of Western technology. Their persistent targeting of principal technologies give hope to Soviet objectives of appreciably enhancing their force structure capabilities, while concurrently securing for them major defense costs and time savings. As noted by the Office of the Undersecretary of Defense for Policy, "acquiring U.S. weapon secrets can assist Soviet military designers in countering U.S. weapons, or developing systems with similar technology."<sup>1</sup> Some of the more highly publicized cases of espionage and illegal equipment sales-such as the Walker-Whitworth sale of cryptologic material to the Soviets and the Toshiba-Kongsberg sale of advanced milling machines for making marine propellers-highlight the problems at hand. They are part of a massive industrial espionage scheme: The Soviets spend \$1.4 billion annually on a worldwide effort involving KGB intelligence officers and other espionage agents to obtain military hardware, blueprints, product samples and test equipment.<sup>2</sup> More alarming, is that both American and Western-ally corporations located in "friendly" countries are making microelectronic and other sophisticated hardware available to the Soviets at distressing rates.

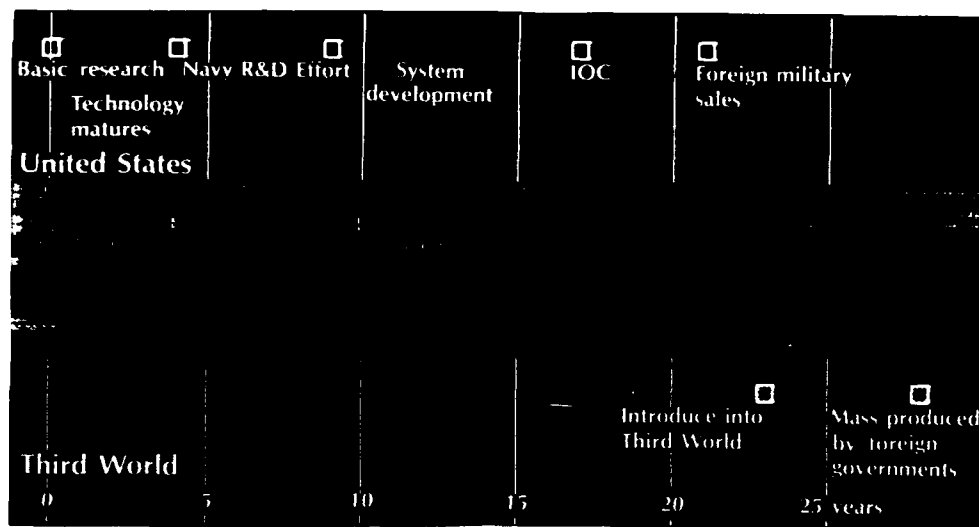
Reciprocally, this leaching of U.S./Western technologies has a triple consequence:

•First, by its very nature it reduces and in some instances, eliminates any advantage the U.S. may have enjoyed by way of technology supremacy. Since the United States is technologically superior to the U. S. S. R. yet outclassed in terms of force structure, it is essential to the West that this technology advantage be maintained and even increased.

•Secondly, it produces a vulnerability to operating systems we have on line which may go undetected for an appreciable period of time, perhaps to the point of never being discovered.

•Thirdly, this pirating of technology, once it is discovered, results in very costly efforts in many instances to nullify the impact of the Soviet adaptation. This translates to increased expenditures of money and human resources which may have been used in pursuit of new horizons. The Soviets, like our Japanese and Korean allies, have mastered the art of technological mimicry and adaptation.

"Tis faster to Copy than to Create: The time it takes for the Soviets to acquire a specific new Western technology varies with the complexity of the application."<sup>3</sup>



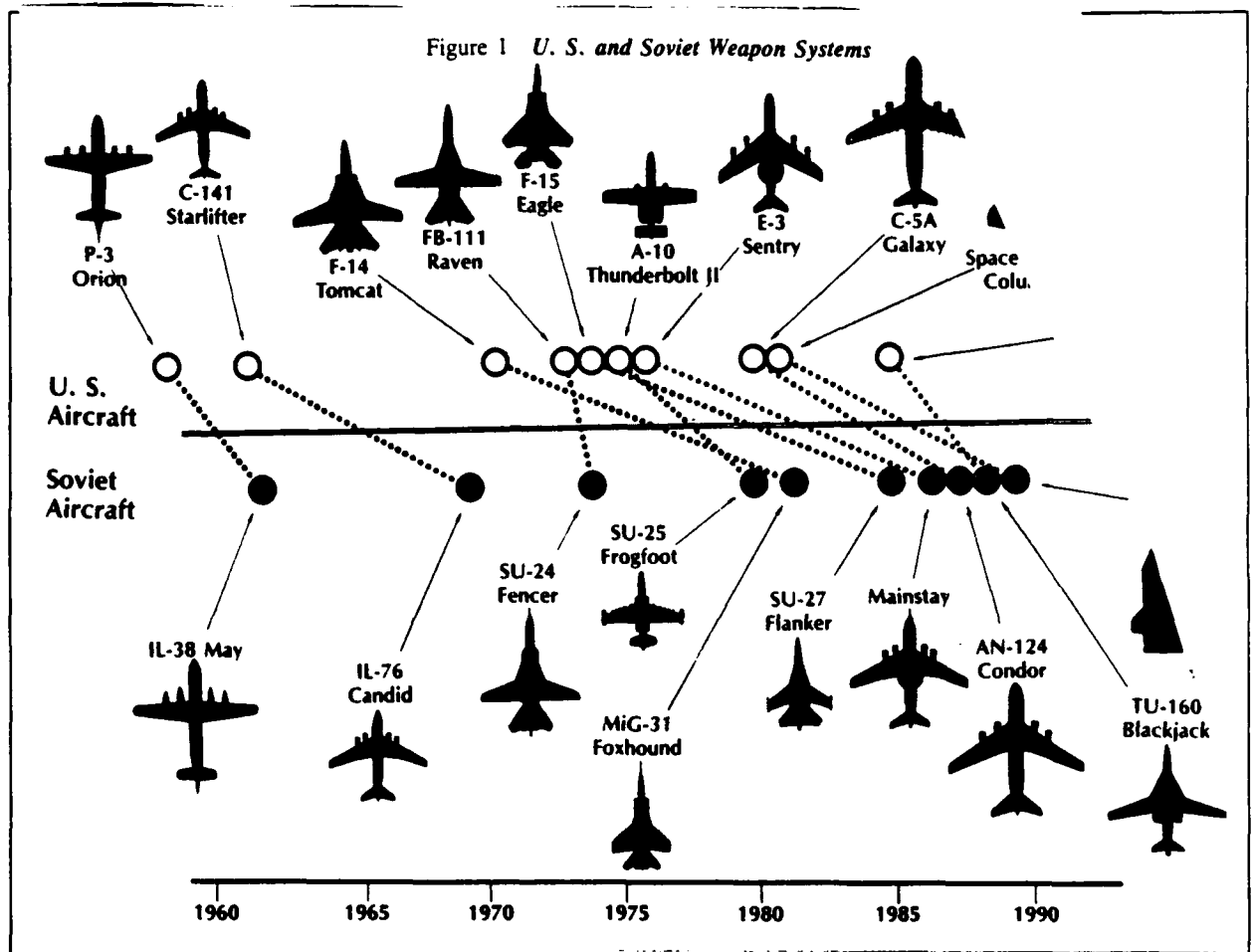
**Figure 1**Technology Transfer Time Line

Source: CDR Marc D. Goldberg, "Rapping Ivan's Fingers", Proceedings, October 1988, p. 78.

The above figure illustrates a 25-year time line, which is said to be typical, over which technology transfer occurs. You will note how quickly the Soviets enter into development once the U. S. achieves Initial Operating Capability (IOC).

The Soviets continue to flatter us with their imitations of our most advanced military systems. We have only to note the strong similarity between our C5A and their Condor heavy airlift aircraft, between our C-141 and their IL-76....But even more serious has been the Soviet testing of their SS-X-24 and SS-X-25 missiles during the early 1980s. These system developments are clear indications that the Soviets no longer wait for the United States to prove a concept before they feel compelled to build and test it themselves. The technology transfer gap has been significantly reduced and the United States' lead in both electronic and military hardware has been significantly eroded.<sup>4</sup>

The illustration at Figure 2 depicts the fielding of U. S. weapons/space systems and the parallel parodying of these systems by the Soviets.



**Figure 2 U. S. and Soviet Weapon and Space Systems**

Source: Proceedings, October 1988, p. 75.

The Soviets estimated that by using documentation acquired on the U. S. F-18 fighter, their aviation and radar industries saved five years in developing the next generation of fire-control radars for Soviet fighter aircraft. The manpower savings on this project

alone translate into over 1,000 man-years of scientific research.<sup>5</sup> Since the Soviets are capable of taking their illicitly obtained technologies from development to IOC more rapidly than the United States, this factor more than any of the others presented here should serve as a compelling reason for the U. S. and its allies to maintain their vigilance against the well-orchestrated transfer of militarily useful technology from the U. S. to the U. S. S. R.

1. Office of the Undersecretary of Defense for Policy, Assessing the Effect of Technology Transfer on U. S./Western Security- A Defense Perspective- February 1985, p. 5-4.

2. Goldberg, p. 74.

3. Ibid., p. 76.

4. John E. Holland, Jr., LTC, Transfer of High-Technology To the Soviet Union-A Predicament for the United States, p. 10.

5. Caspar W. Weinberger, Report of Secretary of Defense to 99th Congress on the Technology Security Program, p. 10.

## CHAPTER IV

### NATIONAL SECURITY CONCERNS: MILITARY STRATEGIC ASPECTS

Richard Pipes, in his article, "How to Cope With the Soviet Threat", states:

The industrial assistance given to the Soviet Union helps its military effort directly and indirectly--directly by providing so-called 'dual-use' technology which can be applied to the production of both military and non-wartime equipment; and indirectly by strengthening the Soviet military mobilization base.<sup>1</sup>

The previously described leaching of U. S. technological advances is a national security issue. The acquisition by the Soviets of our technology is demonstrably detrimental to the Western ability either to maintain the existing military balance or to advance appreciably its ascendancy.

In Department of Defense (DoD) Directive Number 2040.2 dated 17 January 1984, the following policy statement is provided: "It shall be DoD policy to treat defense-related technology as a valuable, limited national security resource, to be husbanded and invested in pursuit of national security objectives. Consistent with this policy and in recognition of the importance of international trade to a strong U. S. defense industrial base, the DoD shall apply export controls in a way that minimally interferes with the conduct of legitimate trade and scientific endeavor".<sup>2</sup>

Thus far, we have seen that the Soviets hope to improve their total force operational capabilities, to fill critical gaps in military technology, and to achieve major defense cost reductions and time savings through various methods of technology transfer from the West.

What are the implications for the U. S. military balance vis à vis the Soviets in the environment of rapid technology transfer? As many experts have pointed out, we have already entered the era in which we in the West find ourselves defending against our own technology. To continue this regimen is sheer folly. Staggering sums of money are spent annually on an enormous array of military hardware and intelligence gathering to "deter" the Soviets from launching a first strike against us or our allies. Both the U. S. and the U. S. S. R. are running high budget deficits that, if left unchecked, threaten to erode their economic strength and pave the way for the emergence of militarily weaker but economically stronger powers such as Japan and the nations of Western Europe.

American strategy for dealing with an adversary that boasts of a markedly superior force structure numerically, continues to emphasize a never ending quest for new and more effective weapons with higher lethality. This is a quest the United States must pursue because it cannot allow the Soviet Union, or any other

nation, to garner a technological advance that would upset the existing delicate balance of power. Presently, we do have a qualitative edge in most essential areas. The West possesses far superior economic strength and political cohesion. Continued research on the Strategic Defense Initiative is required to insure that the Soviets don't gain an advantage in this arena and to prepare for the potential battlefields of the 21st century. Stealth technology, which renders planes and possibly other weapons invisible to conventional radar detection, and thus invincible, is yet but another step in the seemingly never-ending search for a military edge.

Evidence of the need for a strong, well-implemented technology security program is clear from reading the 1985 report, "Soviet Acquisition of Militarily Significant Western Technology- An Update". According to the Soviets' own assessment, contained in that report, over 5000 of their military research projects benefit each year from technical documents and hardware obtained from the West. In Chapter VI we will examine export controls and other U. S. efforts which are designed to deny the Soviets possession of militarily-critical technology.

1. Richard Pipes, "How to Cope With the Soviet Threat", Commentary, August 1984, p. 28.

2. Department of Defense Directive Number 2040.2, "International Transfers of Technology, Goods, Services, and Munitions", p. 2.

## CHAPTER V

### SELECTED CASE STUDIES ON TECHNOLOGY TRANSFER

The volume of material available on instances of technology transfer from the West to the Soviet Union is staggering. Lenin declared that, "The capitalists will sell us the rope we need to hang them". After examining several score cases, greed-the profit motive-does indeed surface as the principle reason behind and entré point for the passing of militarily significant technology from the West to the Soviets. It is appalling that businessmen and individuals who commit espionage have seemingly placed the profit motive above the more cherished security of their respective nations. The following case studies vividly demonstrate the ease with which militarily significant technology transfer occurs and, by implication, the potential damage these acts inflict upon Western security:

#### **"Japanese Probe Diversion of Equipment to North Korea"**

Japanese authorities are investigating a series of diversions to North Korea of sensitive Western technologies, according to U. S. and Japanese sources. Several executives of an Osaka company have been indicted on charges of illegally selling sophisticated electronic equipment to North Korea. 100 advanced integrated circuits...were being shipped without licenses from the Ministry of International Trade and Industry. [This sale violates] the regulations of COCOM, the Coordinating Committee on Multilateral Trade and Export Controls, a Paris-based agency that oversees export policies of the United States and its allies.<sup>1</sup>

### **"Deals That Run Silent and Deep"**

Technology-starved Soviet engineers have long looked to the West to help solve their most pressing military problems, and with the help of the K.G.B. they have grown increasingly adept at bypassing even the strictest export controls. So no one was surprised three weeks ago [May 1987] when it was learned that some sophisticated propeller milling equipment, enabling the Soviet Union to make much quieter submarines, had slipped past the borders of Japan and Norway ending up in a Leningrad shipyard. The shock came last week when investigators probing the records of a respected Norwegian armaments maker, the state-owned Kongsberg Vapenfabrik, and a subsidiary of Japan's giant Toshiba Corporation began to find a trail of high-tech diversions involving sensitive equipment shipped out right under the noses of customs authorities. Senator Paul Sarbanes, Democrat of Maryland called [the illegal export]...**"one of the most egregious diversions of high technology in a decade"**. On Tuesday, the House passed by a vote of 415 to 1 an unusual amendment demanding that the State Department begin to negotiate "compensation" to the Navy, which claims it has lost a long lead in its ability to detect submarines. "We are paying a huge price for Toshiba's and Kongsberg's treachery", said Representative Duncan Hunter...who introduced the amendment.<sup>2</sup>

### **"L.A. Executive Denies Illegal Computer Sale"**

Walter Patzl, a target of the federal government's latest investigation into illegal technology shipments to the Soviet Union, is hardly the picture of a high-tech wizard. Austrian-born Patzl worked at the Los Angeles offices of the Austrian Trade Commission. In 1985, Patzl left the trade commission and opened Essex Marketing Corporation. By all accounts, Patzl spent the next few years helping foreign companies buy U. S.-made computers and other high-tech equipment. But earlier this week reports surfaced in Washington linking Essex to a government investigation into illegal shipments to the Soviet Union of a computer system that could help determine optimal targets for nuclear missiles. According to initial reports, the probe centers on an alleged shipment last Dec. 21 of a computer capable of simulating nuclear explosions. The shipment was originally intended for an engineering college in Zagreb, Yugoslavia. However, investigators report that it was diverted to the Soviet Union after heading first to East Berlin.<sup>3</sup>

**"Panelists Urge Vigilance to Prevent  
Technology Transfer to Soviets"**

The process of strengthening multilateral export controls will continue regardless of political changes in the Soviet Union or the United States or changes in the relations between them, according to U. S. officials responsible for technology security. Allan Wendt, the State Department's senior representative for strategic technology policy said, "Perhaps indeed we are facing a period of more stable relations with the Soviet Union, but if you look at the Soviet Union's military budget, there is no room for comfort...the significant problems [of Soviet technology theft] will remain".<sup>4</sup>

**"Soviets Obtain the Specifications for  
U. S. Stinger Missiles"**

The Soviet Union has obtained the specifications for the Stinger missile in the latest of a series of successful espionage activities aimed at acquiring the technology of U. S. anti-aircraft systems, Pentagon sources said yesterday. Through a military intelligence operation in Athens in 1984, the Soviets obtained microfiche containing basic data about the Stinger's design, **sparing themselves millions of dollars in developmental costs**, the sources said...The Afghan resistance is getting a very basic stripped-down model of the Stinger, one Pentagon official said. Administration officials also have confirmed that a number of Stingers supplied to the rebels have recently fallen into Iranian hands...Other U. S. missile technologies obtained by the Soviet Union include the Phoenix air-to-air missile, used by the F-14 fighter, and the Redeye missile, another surface-to-air weapon, the sources said...The Soviet Union is believed to have used technology from the Redeye to build the Grail, or SAM-7, used against U. S. helicopters in Vietnam from 1972 on and less effectively against Israeli jets by Soviet allies in the 1973 Middle East war.<sup>5</sup>

Obviously, the preceding examples of technology transfer from the U. S. to the Soviet Union are serious. Unfortunately, these cases represent only a small fraction of the number of instances in which this kind of transfer occurs.

1. James M. Dorsey, "Japanese Probe Diversion of Equipment to N. Korea," The Washington Times, 23 June 1987, p. 1.
2. David E. Sanger, "Deals That Run Silent and Deep", The New York Times, 21 June 1987, Section 4, p. 5.
3. Carl Lazzareschi, "L.A. Executive Denies Illegal Computer Sale", Los Angeles Times, 24 February 1988, p. IV9.
4. David Silverberg, "Panelists Urge Vigilance to Prevent Technology Transfer to Soviets", Defense News, 20 June 1988, p. 9.
5. James M. Dorsey, "Soviets Obtain the Specifications for U.S. Stinger Missiles", The Washington Times, 29 October 1987, p. 10.

## CHAPTER VI

### EFFORTS AT DETERRENCE

As long as the United States and its allies maintain comparatively open societies with free expression and exchange of ideas and products inter alios, the threat posed by the U.S.S.R. and its bloc nations having to do with their relentless pursuit of our technological discoveries, applications and innovations will remain alive, well and strident.

Preventing the diversions of high technology is as important to the free world's security as expanding our military capabilities. Our enforcement activities are directed at preventing losses of commodities and technologies that would harm U. S. national security and enhance our adversaries' military capabilities.<sup>1</sup>

In recognition of this menace, an organization was created, consisting of the U.S. and its allies, under the banner of Coordinating Committee for Multilateral Security Export Controls [COCOM]. The purpose of this organization is to oversee a multilateral system that serves as a vanguard against the transfer of strategic technology. COCOM, as a working modus, and in conjunction with the U. S. Department of Commerce, prescribes a Commodity Control List which has contained thereon component and end item products, the sale of which are prohibited/restricted to Soviet bloc nations. The National Security Agency assists Commerce in focusing attention and reviewing export requests of specified

products. Resulting policies that are developed provide doctrinal guidance and policy which prescribes those items which are prohibited for trade with proscribed nations.

Export licenses are required to be in the possession of the manufacturers and/or exporters of proscribed items. The U. S. Customs Service has nearly an impossible task of monitoring the shipment of end-items and component parts, both of which may contain embedded technology, out of the country. At best, Customs can only monitor a fraction of exported goods; but yet, over the years, this service has been able to prevent numerous prohibited items from leaving the United States.

Before the U.S. can foil Soviet endeavors directed at the acquisition of critical technologies, it is first necessary to determine what technologies or production processes might significantly contribute to Soviet military capabilities. To this end, fourteen technology target groups have been identified. They are:

•Automated Production and Control •Computer Technology  
•Directed Energy •Sensor Technology •Guidance and Navigation  
•Microelectronics/Semiconductors •Optics/Optoelectronics  
•Power Generation and Propulsion •Production and Manufacturing  
•Structural Materials •Genetic Engineering •Telecommunications  
Technology •Transportation Technologies •U.S. Weapon Work

Uniformity and consistency of regulating militarily significant restricted items from the above categorizations have been inadequate. For example, "the illegal sale of multi-axis milling machines by Toshiba Machine Company and Kongsberg Trading Company clearly demonstrates that there are gaps".<sup>3</sup> These western

firms, which held U.S. Defense contracts, violated the laws of their respective countries, and in so doing gave the Soviets the means to mass-fabrication capability for extremely quiet submarine propellers. Obviously, this episode will both cause the U.S. to expend many millions of dollars in researching methods to detect these expected quieter submarines as well as materially impact upon its national security. Mr. E. Allan Wendt, Senior Representative for Strategic Technology Policy, in remarks to the Royal Institute of International Affairs in London, remarked: "The resulting damage to our mutual security can only be repaired at great cost-a cost, I might add, that is far greater than the relatively trivial profits realized by the companies participating in these illegal sales or diversions."<sup>3</sup>

1. Paul Freedenberg, "The New Bureau of Export Administration, Business America, 29 February 1988, p. 4.

2. E. Allan Wendt, "Export Control Policy and COCOM", Department of State Bulletin, March 1988, p. 63.

3. Wendt, p. 64.

## CHAPTER VII

# CONCLUSIONS

Thus far, billions of dollars in research and development costs have been saved by the USSR and its bloc nations because of their ability to look over our technological shoulder. The net result of these "thefts" of western technology cause the United States to expend many millions of dollars defending against its own technology. As long as the profit motive exists as the bulwark of our capitalistic-entrepreneurial modus, the exporting of our technology base is likely to continue.

The United States and its allies are now more keenly aware of the high price that operating in the "clear", regarding technological innovations, have exacted in the past. The U.S. has embarked upon a vigorous multilateral program of alerting its allies to the dangers of this Soviet threat, which is both economic as well as military in nature. Member countries of COCOM are strengthening their resolve to resist these economic/national security encroachments by such actions as upgrading the legal basis for licensing and enforcement, mandating stiffer fines and penalties for violations and seeking longer statutes of limitation. It is believed that these countries are taking these steps not because of U.S. influence, but out of a more selfish motive: they have come to the conclusion that it is in their own national interest to do so.

The U.S. must continue to be vigilant in asserting its influence to staunch the flow of military-related technology, and if successful, this preemptive action will serve as an essential ingredient in the formula triad of the ways and means which buttress our national security interests and objectives.

## BIBLIOGRAPHY

1. Committee on Governmental Affairs, Soviet Acquisition of Military Significant Western Technology, An Update, September 1985, p. 1. Report on hearings before the Permanent Subcommittee on Investigations of the U.S. Senate, 97th Congress.
2. Department of Defense Directive Number 2040.2. "International Transfers of Technology, Goods, Services, and Munitions". p. 2.
3. Dorsey, James M. "Japanese Probe Diversion of Equipment to N. Korea". Washington Times, 23 June 1987, p. 1.
4. Dorsey, James M. "Soviets Obtain the Specifications for U.S. Stinger Missiles". The Washington Times, 29 October 1987, p. 10.
5. Goldberg, Marc D. "Rapping Ivan's Sticky Fingers", Proceedings. Vol. 114, p. 74.
6. Holland, John E., Jr. Transfer of High-Technology to the Soviet Union-A Predicament for the United States. p. 10.
7. Jones, Kathryn "CIA Official Expects Soviets to Step up Industrial Spying". Dallas Morning News, 17 February 1988.
8. Lazzareschi, Carla. "L.A. Executive Denies Illegal Computer Sale". Los Angeles Times, 24 February 1988, p. IV-9.
9. Linhares, A. B. Introduction, Directory of Federal Technology Transfer. Executive Office of the President, Federal Coordinating Council for Science, Engineering and Technology. p. v.
10. Office of the Undersecretary of Defense for Policy. Assessing the Effect of Technology Transfer on U.S./Western Security - A Defense Perspective-. February 1985, p. E-1.
11. Pipes, Richard. "How to Cope With the Soviet Threat". Commentary, August 1984, p. 28.
12. Sanger, David E. "Deals That Run Silent and Deep". New York Times, 21 June 1987, p. 5.
13. Silverberg, David. "Panelists Urge Vigilance to Prevent Technology Transfer to Soviets". Defense News, 20 June 1988, p. 9.
14. Weinberger, Caspar W. Report of Secretary of Defense to 99th Congress on the Technology Security Program, 1986, p. 10.
15. Wendt, E. Allan. "Export Control Policy and COCOM". Department of State Bulletin, March 1988, p. 63.