The Director of Central Intelligence

Washington, D.C. 20505

Executive Registry
84-1399

27 March 1984

MEMORANDUM FOR: Chief, Technology Transfer
Task Force

FROM: Director of Central Intelligence

SUBJECT: Draft Remarks to Commonwealth Club, Silicon Valley

This seems a little thin. Can you give me anything more specific that would be interesting for some comments on technology transfer at Silicon Valley.

C

William J. Casey

B-301
XF P-306

DRAFT

DCI REMARKS TO

COMMONWEALTH CLUB

SILICON VALLEY

3 April 1984

DRAFT

When I was invited to address this distinguished group, which in a very real sense represents the mainstay of America's technological prowess, it occurred to me that your invitation could not have come at a more auspicious moment. Today, the Western democracies are faced with perhaps the most formidable military challenge they have ever encountered, the Soviet military machine. And, I regret to say, the U.S. contributes to the growing sophistication and lethality of that machine.

Some examples:

* The Soviets had our plans to the C-5A before it flew.

* The Soviet trucks which rolled into Afghanistan came from a plant outfitted with $1.5 billion of modern American and European machinery.

* The precise gyros and bearings in their SS-18 ICBM were designed by us.

* The radar in their AWACCs is ours.

* Their space shuttle is a virtual copy of ours.

* And the list goes on and on.

Over the past three years, the Intelligence Community has devoted substantial resources and countless hours of effort studying the impact of Western technology on Soviet military capabilities, trying to stem losses of our technology, and anticipating what we can expect from the Soviet collection effort in the future. I would like to share with you some of our findings.

The Russians have been trying to buy, borrow, or steal Western technology to upgrade the military capabilities from the time of Peter the Great in the early 18th century. Under Stalin, much of Soviet heavy industry was modernized through imports of Western technology.

Today, however, the Soviet technology acquisition program is far more massive, well coordinated, and precisely targeted than at any time in Russia's long history. The top Soviet leaders realized that, with rapid military technological change and Moscow's own technological backwardness, the Soviet Union must have ready access to Western innovations if their armed forces are to stay abreast of the qualitative improvements in our weapons. The Soviet military technology base is not weak. Quite the contrary, it is strong in most areas critical to future weapons development. But the Soviets do have

problems in R & D, in innovation. Current Soviet technology available for military applications is still several years behind the West, and it is this technology on which Soviet military systems for the 1980s and 1990s will be based.

Besides directly enhancing Soviet military capabilities, Western technology also serves another important purpose in Moscow's strategic calculations. Moscow has paid a high price for their military build-up. Technological progress in other key areas of their economy, particularly the consumer sector, has stagnated. By acquiring Western technology, Moscow hopes to bridge critical industrial gaps without disrupting domestic resource allocations favoring the military. This is an ancient and recurring pattern in Russian history: Each time military requirements began to overburden the economy, Russian leaders turned to the West for relief, and each time the West bailed them out of their economic difficulties.

I can encapsulate our intelligence findings on the implications of technology transfer in a single sentence: The ability of the Soviet military-industrial complex to acquire and assimilate Western technology far exceeds any previous estimates.

During the late-1970s, the Soviets got about 30,000 samples of Western production equipment, weapons and military components, and over 400,000 technical documents both classified and unclassified. The majority was of U.S. origin; with an increasing share of our technology obtained through Western Europe and Japan. This truly impressive take was acquired by both legal and illegal means, including espionage. We estimate that during this period, the KGB and its military equivalent, the GRU, and their surrogates among the East European Intelligence Services illegally stole about 70 percent of the technology most significant to Soviet military equipment and weapons programs.

This ill-gotten information or equipment directly contributed to several hundred Soviet military programs, such as:

* Strategic offensive missiles
* Strategic and tactical aircraft, including air defense interceptors
* Space and reconnaissance systems, and conventional ground and naval forces.

Ours or our allies' technology significantly enhanced the performance and quality of these systems. In some cases, a major weapon was deployed two to three years earlier because of our stolen brain-power.

Western dual-use technologies that have had the greatest impact on Soviet defense capabilities include: Microelectronics, Computing, Communications, Avionics, Electro-optics including lasers, Composite materials, and Numerically controlled machine tools.

I have been particularly eager to address this group because U.S. microelectronics production technology is the single most significant industrial technology acquired by the Soviets since the end of World War II. Silicon Valley and your firms are the primary target of Soviet and East European Intelligence Services. In the late 1970s alone, Moscow acquired several thousands of pieces of Western microelectronics equipment worth hundreds of millions of dollars in all of the major processing and production areas:

* Wafer preparation
* Circuit mask processing
* Device fabrication, and
* Assembly and test equipment, which they were most in need of.

With these gains, the Soviets have systematically built a modern microelectronics industry. For example, the Zelenograd Science Center, the Soviet equivalent of Silicon Valley, was equipped, literally from scratch, with Western technology. All Soviet monolithic integrated circuits are copies of U.S. designs. They even copied the imperfections contained in some of the U.S. samples!

As amusing as this anecdote might be, this situation is serious .

With Western equipment, the Soviets could meet 100 percent of their military microelectronics requirements. Currently the Soviet microelectronics technology lags some three to five years behind us and the Japanese. Ten years ago the gap was 10 to 12 years. Our technology has narrowed our own lead.

The Soviets have rapidly introduced monolithic IC's into a variety of land, sea, and air weapon systems, while the United States has been slower to introduce new microelectronics technology into its military systems. Consequently, the significant lead we formerly enjoyed in the application of military microelectronics has been reduced to

only two or three years. And the gap is narrowing. Our very high speed integrated circuits program might reverse this trend, but only if we do a better job of exploiting its military potential.

Just how do the Soviets get so much of our technology?

First of all, they comb through our open literature, buy through legal trade channels, religiously attend our scientific and technological conferences, and send students over here to study. Between 1970 and 1976, the Soviets purchased some $20 billion of Western equipment and machinery, some of which had potential military applications. In addition to exploiting all open, legal channels, they use espionage.

There are now several thousand Soviet Bloc collection officers at work primarily in the United States, Western Europe, and Japan. And as I stated before, your firms here in Silicon Valley are at the very top of their list. The Soviets especially pinpoint and target small, highly innovative companies in the computer and microelectronics field, not only because they are at the leading edge of the technologies that Moscow is most in need of, but also because such firms' security procedures are usually inadequate to protect against penetration by a determined, hostile intelligence service.

They also use sophisticated international diversion operations. We have identified some 300 firms operating from more than 30 countries engaged in such diversion schemes. And there are probably many more that remain unidentified. Most diversions occur by way of Western Europe, which is why we have made such a strong effort to enlist the help of our European allies in combating illegal trade activities.

The Soviets, over the past several years, have made a major push to acquire computers and software developed by key U.S. firms including IBM and Digital Equipment Corporation (DEC). Many of these acquisitions have been made through illegal traders.

You may recall that in late 1983 and early 1984, West German and Swedish Customs seized several of DEC's advanced VAX computers and 30 tons of related equipment that were being smuggled to the USSR by the notorious illegal trader, Richard Mueller. This was but the tip of the iceberg. Our evidence shows that much larger quantities of DEC computing and electronic equipment have been successfully diverted to the USSR.

They may use legal trade to pave the way for illegal trade. For example, they may send a Polish or East German acceptance engineer to a plant as part of a legal trade deal. But this engineer may have a hidden agenda to acquire additional information beyond his supposed access and to make contacts for future illegal exchanges. The KGB has been very successful using East Europeans as front men, for they are generally less suspicious.

Soviet dependence on the West for technological innovation is broad and deep. In the future, they will particularly need to buy or steal our innovation in information acquisition and information processing, technologies which will have a major impact on critical military systems. Soviet capabilities in information acquisition and processing will determine how successful they will be in detecting our future aircraft and cruise missiles, modern submarines, ballistic missile reentry vehicles, and how well the Soviet military performs in an electronic warfare environment. Their future near real-time targeting and command and control systems will also depend heavily on these technologies.

In microelectronics, the Soviets will need to considerably expand their material base to boost integrated circuit production. Thus, they will be anxious for

higher-precision Western equipment, particularly in packaging and printed circuit board production. We also expect them to target the emerging technologies related to very high-speed integrated circuits and very large scale integration.

The Soviet Union lags further behind the West --about 10 years--in computers than in any other field of advanced technology. Throughout the 1980's, they will probably try to acquire large-scale scientific computers such as the CRAY-1. Computers of this class offer significant improvements over Soviet models in weapons-systems design and simulation and in the processing of numerical data for many military applications. Other computer hardware targets will be: very dense random-access memory chips; high-capacity disk drives and packs; the so-called "superminicomputer" class of machines; and the latest in general purpose computer technology. The compelling attraction of computer networks also should spur great Soviet interest in acquiring network-control software and other programs related to such networking. (U)

The West must organize to protect its military, industrial, commercial, and scientific communities, keeping two objectives clearly in view. First, the West must seek to maintain its technological lead-time over the Soviets in vital design and manufacturing know-how. Second, manufacturing,

inspection, and, most importantly, automatic test equipment, which can alleviate acute Soviet deficiencies in military-related manufacturing areas, must be strictly controlled.

I cannot emphasize too strongly that protecting equipment is just as important as protecting manufacturing know-how. In this connection, the Defense Science Board report on export controls issued in 1976--the so-called Bucy (Buecee) report--is often held up as evidence that equipment sales divorced from the transfer of know-how have little long-term significance for the Soviets. This is not only a misinterpretation of the report's conclusions, but it simply cannot be supported by the wealth of evidence compiled by the Intelligence Community. That evidence indicates that equipment transfers, both large batch acquisitions and individual samples used for reverse engineering, far outstrip acquisitions of pure technology in quantity and in value to the Soviets.

Our ultimate goal, of course, must be to deny the Soviets access to technologies that will accelerate their military programs. Several positive steps have already been taken by the U.S., Western Europe, and Japan. The COCOM list has been expanded to include such items as electronic grade

silicon, composite materials, special feature robots, and large floating drydocks. In addition, an inventory of emerging technologies has been established to monitor Soviet attempts to acquire technologies with potential military application.

Western governments have also become more actively concerned about Soviet intelligence operations. As a result, there has been a major and successful crackdown against the KGB and GRU. In 1983, over 100 Soviets were expelled from 16 Western countries for espionage. This exceeds the combined total for 1980-82. About half those expelled were trying illegally to obtain scientific and technical data.

However, much remains to be done.

Efforts by the major Western countries to improve security against intelligence collection by visiting Soviet scientists, engineers, and trainees is making slow progress in most of the Western countries. This is due in part because Western scientists generally oppose tighter restrictions on the exchange of ideas and information with their Soviet Bloc counterparts. Furthermore, we need to develop a systematic program among the Western customs services aimed at preventing the illegal export of strategic technologies.

The Soviet appetite for our technology will continue to be voracious. They will continue to exploit the loopholes and weaknesses in Western export controls and policy differences among the COCOM countries, to acquire the technologies needed by their military programs for the 1990s and beyond.

I can assure you, however, that this effort is becoming more difficult and costly for them than at any time in the past. The stakes are high and the Soviets know it; they will devote whatever resources and manpower are required to fulfill their most critical military collection requirements. We in the West can do no less if we are to succeed in frustrating their efforts. All of us--government and private industry--will need to participate. Thank you.